

# Kryptografické algoritmy využívané v bezpečnostní komunitě

Cryptographic Algorithms used in the Security Community

Stanislav Kovář

---

Bakalářská práce  
2012



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2011/2012

## **ZADÁNÍ BAKALÁŘSKÉ PRÁCE**

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Stanislav KOVÁŘ**  
Osobní číslo: **A09185**  
Studijní program: **B 3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Kryptografické algoritmy využívané v bezpečnostní komunitě**

Zásady pro vypracování:

1. Zpracujte literární rešerši na dané téma.
2. Stručně popište historický vývoj kryptologie.
3. Popište některé základní typy šifer.
4. Uvedte některé typy útoků na vybrané kryptografické algoritmy.
5. Provedte matematický rozbor algoritmu RSA včetně útoků na něj.
6. Uvedte nové trendy v oblasti kryptologie.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. ZELENKA, Josef. Ochrana dat: kryptologie. Vyd. 1. Hradec Králové: Gaudeamus, 2003, 198 s. ISBN 80-704-1737-4.
2. VONDRUŠKA, Pavel. Kryptologie, šifrování a tajná písma: kryptologie. 1. vyd. Praha: Albatros, 2006, 340 s. ISBN 80-000-1888-8.
3. PIPER, Fred, MURPHY, Sean. Kryptografie: kryptologie. 1. vyd. v českém jazyce. Překlad Pavel Mondschein. Praha: Dokořán, 2006, 157 s. ISBN 80-736-3074-5.
4. HANŽL, Tomáš, PELÁNEK, Radek, VÝBORNÝ, Ondřej. Šifry a hry s nimi: kolektivní outdoorové hry se šiframi. Vyd. 1. Překlad Pavel Mondschein. Praha: Portál, 2007, 198 s. ISBN 978-807-3671-969.
5. TILBORG, Henk C. Fundamentals of cryptology: a professional reference and interactive tutorial. Vyd. 1. Překlad Pavel Mondschein. Boston: Kluwer Academic Publishers, c2000, 490 s. ISBN 0792386752.

Vedoucí bakalářské práce: **Mgr. Jana Řezníčková, Ph.D.**

Ústav matematiky

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **25. května 2012**

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.  
*děkan*



doc. Mgr. Milan Adámek, Ph.D.  
*ředitel ústavu*

## **ABSTRAKT**

Student se seznámí s problematikou kryptografických algoritmů formou literární rešerše. V teoretické části práce se bude zabývat oblastmi použití kryptografických algoritmů v zabezpečení důvěryhodnosti dat, jako i zabezpečení integrity a autenticity. Přehlednou formou uvede základní typy šifer. Praktická část práce bude obsahovat typy útoků na kryptografické algoritmy. Student provede matematickou analýzu vybraných asymetrických šifrovacích algoritmů. V závěru práce uvede nové trendy v dané oblasti.

Klíčová slova: kryptografie, kryptoanalýza, klíč, otevřený text, asymetrické šifry, modulární aritmetika

## **ABSTRACT**

Student acquaints with the problems of cryptographic algorithms through literature searches. In the theoretical part of the thesis he will deals with areas of using and application of cryptographic algorithms to secure credibility of data, as well as the security of the integrity and authenticity. Student clearly gives basic types of ciphers. The practical part of the work includes types of attacks on cryptographic algorithms. The student performs a mathematical analysis of selected asymmetric encryption algorithms. In the conclusion in part there are indicated new trends in the area.

Keywords: cryptography, cryptanalysis, key, plaintext, asymmetric cypher, modular arithmetic

Touto cestou bych rád poděkoval vedoucí své bakalářské práce paní Mgr. Janě Řezníčkové Ph.D., za odborné rady, vedení a připomínky, které mi pomohly při vypracování této práce. Zároveň bych jí chtěl poděkovat za pozornost a trpělivost, kterou mi věnovala při tvorbě bakalářské práce.

**Prohlašuji, že**

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD</b> .....	<b>9</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>10</b>
<b>1 LITERÁRNÍ REŠERŠE</b> .....	<b>11</b>
1.1 ZÁKLADNÍ POJMY .....	11
1.2 HISTORIE .....	20
1.2.1 Starověk.....	20
1.2.1.1 Caesarova šifra.....	20
1.2.2 Středověk a raný novověk .....	22
1.2.2.1 Vigenèrova šifra.....	22
1.2.3 Dvacáté století.....	24
1.2.3.1 Playfairova šifra .....	25
1.2.4 Moderní kryptologie.....	27
1.2.4.1 Algoritmus RSA .....	27
<b>II PRAKTICKÁ ČÁST</b> .....	<b>29</b>
<b>2 KRYPTOANALÝZA</b> .....	<b>30</b>
2.1 FREKVENČNÍ ANALÝZA .....	31
2.1.1 Frekvenční analýza – Caesarova šifra .....	32
2.1.2 Frekvenční analýza – Vigenèrova šifra .....	33
2.1.3 Frekvenční analýza v programu Mathematica .....	42
2.2 KOEFICIENT KOINCIDENCE.....	44
2.2.1 Využití koeficientu koincidence.....	49
<b>3 ROZBOR ALGORITMU RSA</b> .....	<b>52</b>
3.1 TVORBA KLÍČŮ .....	52
3.2 POSTUP PŘI ŠIFROVÁNÍ A DEŠIFROVÁNÍ.....	54
3.3 ÚTOKY NA RSA ALGORITMUS .....	55
3.3.1 Útok se znalostí šifrovaného textu .....	56
3.3.2 Útok se společným modulem .....	57
3.3.3 Podpis podvrženého dokumentu .....	57
3.3.4 Záměna zpráv .....	58
<b>4 NOVÉ TRENDY</b> .....	<b>59</b>
4.1 AFINNÍ TRANSFORMACE .....	59
4.1.1 Afinní transformace v $\mathbb{R}$ .....	59
4.1.2 Afinní transformace v $\mathbb{R}^2$ .....	59
4.2 FRAKTÁLNÍ ŠIFROVÁNÍ .....	60
4.3 KVANTOVÁ KRYPTOGRAFIE.....	60
4.4 BIOTECHNOLOGIE VE STEGANOGRAFII .....	62
<b>ZÁVĚR</b> .....	<b>64</b>
<b>ZÁVĚR V ANGLIČTINĚ</b> .....	<b>65</b>

<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>66</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK .....</b>	<b>67</b>
<b>SEZNAM OBRÁZKŮ .....</b>	<b>68</b>
<b>SEZNAM TABULEK.....</b>	<b>70</b>
<b>SEZNAM PŘÍLOH.....</b>	<b>71</b>

## ÚVOD

Lidé už od svého počátku hledají způsob, jak zajistit bezpečný přenos informací, které jsou určeny pouze pro určitý okruh lidí, a jak tyto informace chránit před těmi, pro něž má jejich obsah zůstat nedostupný. V počátcích vzniku písma byl přenos zpráv jednoduchý, postupem času, kdy znalost psaní a čtení dosahovala vyšší a vyšší úrovně, se zdokonalovaly i metody ukrývání a přenosu zpráv tak, aby je byl schopen rozluštit pouze ten, komu byly určeny a nemohlo dojít k jejich prolomení. S objevem počítače začaly být jednodušší šifry nahrazovány složitějšími algoritmy, které zpočátku nebyly veřejně známy. Později začaly být tyto algoritmy sice zveřejňovány, ale k přenosu šifrovaných zpráv se začaly využívat tzv. klíče, které znali jen odesílatel a příjemce, takže přenos byl bezpečnější. Šifrování jedním klíčem bylo postupem nahrazováno složitějším šifrováním pomocí dvou klíčů. Odvětví kryptologie se neustále vyvíjí i v dnešní době.

Práce se skládá z teoretické a praktické části. V teoretické části jsou uvedeny základní pojmy, se kterými se čtenář setká v dalších kapitolách. Dále jsou stručně popsány nejdůležitější historické milníky, jež měly vliv na další vývoj kryptografie. Je uveden přehled některých historických i současných šifer.

Praktická část obsahuje některé typy útoků na kryptografické algoritmy, včetně ukázek jejich použití na vybraných příkladech. Hlavní pozornost je věnována frekvenční analýze a rozboru algoritmu RSA s uvedením možných útoků na něj. Poslední kapitola praktické části se zabývá novými trendy v oblasti kryptologie.

## **I. TEORETICKÁ ČÁST**

# 1 LITERÁRNÍ REŠERŠE

## 1.1 Základní pojmy

V této části je uveden přehled základních pojmů z oblasti kryptologie, včetně jejich významu. Pojmy jsou čerpány ze zdroje [1], není-li uvedeno jinak.

### **Kryptologie**

Kryptologie je věda zabývající se utajením obsahu zpráv nebo samotné existence zprávy. V minulosti bylo možné kryptologii nalézt v knihovnách v oddělení alchymie nebo hvězdopřevectví. Kryptologie nebyla dlouho uznána jako matematická věda a dlouho žila ve stínu matematiky a informatiky.

Kryptologie se dělí na kryptografii, kryptoanalýzu a steganografii.

### **Kryptografie**

Tato část kryptologie se zabývá matematickými metodami, které mají vztah k prvkům informační bezpečnosti jako je zajištění důvěrnosti zprávy, autentizace entit (ověření subjektu), integrity dat (neporušenosti) a původu dat (vlastnictví). Zkoumá také slabé a silné stránky i odolnosti vůči různým metodám útoku. V dřívějších dobách byla kryptografie chápána jako věda zabývající se navrhováním a používáním šifrovacích systémů. Jednalo se tedy o převedení informace do podoby, ve které zůstala daná informace skryta. Úkolem kryptografie bylo zajistit, aby zpráva byla nečitelná pro třetí neboli nepovolenou osobu, a to i v případě prozrazení přenosu informace. V tomto spočívá rozdíl mezi kryptografií a steganografií.

Kryptografové se zabývají návrhem, použitím a zkoumáním šifrovacích systémů a dalších aspektů informační bezpečnosti. Ve svých počátcích se kryptografie zabývala rozvojem algoritmů sloužících ke skrytí zprávy před nepovolenými osobami. V pozdějších letech došlo k rozšíření algoritmů (postup) tak, aby bylo možné jednoznačně určit odesílatele (identifikace) a ověření správnosti při přenosu zprávy příjemcem (autorizace).

### **Kryptoanalýza**

Kryptoanalýza je zaměřená na studium metod luštění šifrovacích systémů, jedná se tedy o opak kryptografie. Cílem kryptoanalýzy je získat ze zašifrované zprávy otevřený text nebo

alespoň část informací ze zprávy. Analyzuje odolnost (sílu) kryptografických systémů a snaží se do nich proniknout.

### **Steganografie**

Na rozdíl od kryptografie, steganografie má za cíl skrýt celou zprávu, a ne jen obsah zprávy. V případě steganografie může být zpráva napsána ve srozumitelné podobě, ale útočník (třetí osoba) nesmí vědět, že k přenosu zprávy došlo.

Steganografie je za plnohodnotnou disciplínu považována teprve krátce, v minulosti byla pro svou „jednoduchost“ kryptografie opomíjena. Nejznámějším příkladem steganografie je použití neviditelného inkoustu, v současné vyspělejší době využívá ke svým cílům složité matematické aparáty, stejně jako celá kryptologie.

### **Šifrový systém**

Šifrový systém, též šifrovací nebo kryptografický systém, může být jakýkoliv systém, jenž lze využít ke změně obsahu zprávy tak, aby se stala nečitelnou pro kohokoliv mimo příjemce zprávy.

### **Šifrování**

Šifrování (též zašifrování) nastane, pokud s použitím šifrového systému změním podobu nějakého textu.

### **Dešifrování**

Jedná se o opačný proces k šifrování, kdy se příjemce snaží získat původní otevřený text z šifrového textu. Dešifrování se provádí za pomoci domluvené kryptografické metody a znalosti příslušného klíče.

### **Šifrový text (šifrová zpráva)**

Jedná se o text, jenž byl zašifrován.

### **Otevřený text**

Jedná se o původní text ještě před zašifrováním.

### **Abeceda otevřeného textu / znak otevřeného textu**

Abeceda je množina znaků otevřeného textu. Znakem otevřeného textu může být jakékoliv písmenko, číslice, interpunkční znaménko atd., jež se může vyskytnout v otevřeném textu.

**Řetězec** je posloupnost různých po sobě následujících znaků. **Délka řetězce** značí počet znaků obsažených v řetězci.

### Šifrová abeceda

Šifrová abeceda (nebo také šifrové znaky), může být tvořena různými druhy znaků nebo obrázců. Znaky v šifrové abecedě tvoří řetězce nebo skupiny, které jsou zapisovány po pěti. Tento zvyk vznikl v 19. století, kdy se předávaly zprávy pomocí telegramu a platilo se za slovo. U většiny evropských jazyků je průměrná délka slova otevřeného textu 5 znaků, z důvodu poplatků bylo vyžadováno, aby byl šifrový text stejné délky.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9																
☺	☹	☀	♀	♂	♠	♣	♥	♦	♪	♫	▲	▶	▼	◀	←	↑	→	↓							
,	-	_	?	!	,																				

Tabulka 1: Příklady znaků šifrové abecedy

### Bigram (trigram, ...)

Za bigram je považována jakákoliv dvojice po sobě následujících písmen v textu. Za nejčastěji používaný bigram je považován TH z anglického textu. Trigram je obdobný jako bigram, jen s třemi po sobě jdoucími písmeny. Příkladem trigramu českého textu jsou například slova KTE. Neurčitý počet po sobě jdoucích písmen považujeme za polygram.

### Klamač

Jedná se o znak šifrové abecedy, který nemá v otevřeném textu žádný významový ekvivalent a nedešifruje se, resp. vynechává se. Důvod využívání klamače spočívá ve zvýšení bezpečnosti šifry. Především u statických útoků by mohlo na základě frekvence nebo analýzy bigramů dojít k odhalení znaků otevřeného textu.

### Mezinárodní abeceda

Tato abeceda je tvořena 26 písmeny a nepoužívá diakritiku. Za znaky mezinárodní abecedy jsou považována tato písmena:

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z.

Tuto abecedu lze rozšířit o mezeru a interpunkční znaménka. Abecedu otevřeného textu s využitím více písmen používaných v jiných jazycích je možné použít, ale při využití

šifrovacího zařízení by bylo nutno pro tento účel změnit jeho konstrukci. Z tohoto důvodu se používá jako abeceda otevřeného textu především mezinárodní abeceda.

### **Luštění**

Luštění je proces hledání otevřeného textu ze zašifrované zprávy. Luštěním se zabývají kryptoanalytici. Pokud se kryptoanalytikovi podaří vniknout do nějakého šifrového systému, říká se, že šifra byla zlomena nebo rozbita. Prolomení šifry znamená, že kryptoanalytik dokáže přečíst všechny zašifrované zprávy určitého šifrovacího systému. Tento jev nenastane vždy, zvláště u kvalitnějších systémů může dojít k rozluštění jen jedné konkrétní části zprávy, ale ne všech ostatních. Proniknutí do systému závisí na mnoha faktorech, jako je síla patřičného klíče, opakované používání klíče, délka šifrované zprávy apod.

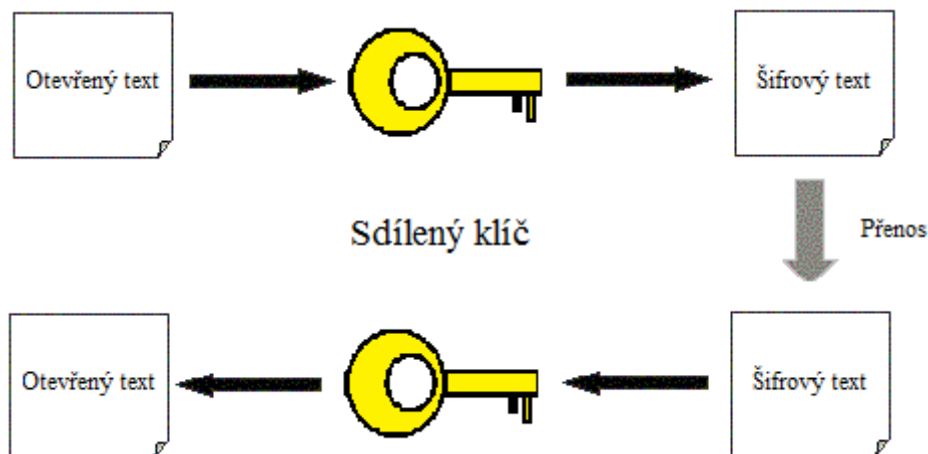
Cílem dešifrování a luštění je získat z šifrového textu patřičný otevřený text. I když se na první pohled zdá, že mezi těmito dvěma procesy není rozdíl, není to pravda. Dešifrování se používá v případě, že jsou známy všechny informace potřebné k převedení šifrového textu na otevřený text, ve většině případů jej provádí příjemce. Naopak luštění provádí třetí osoba, např. kryptoanalytik, která nemá k dispozici potřebné informace.

### **Klíč**

Klíč je parametr šifrového systému, který má vliv na šifrový text. Úkolem klíče je změnit obecný šifrovací algoritmus ve specifický postup šifrování.

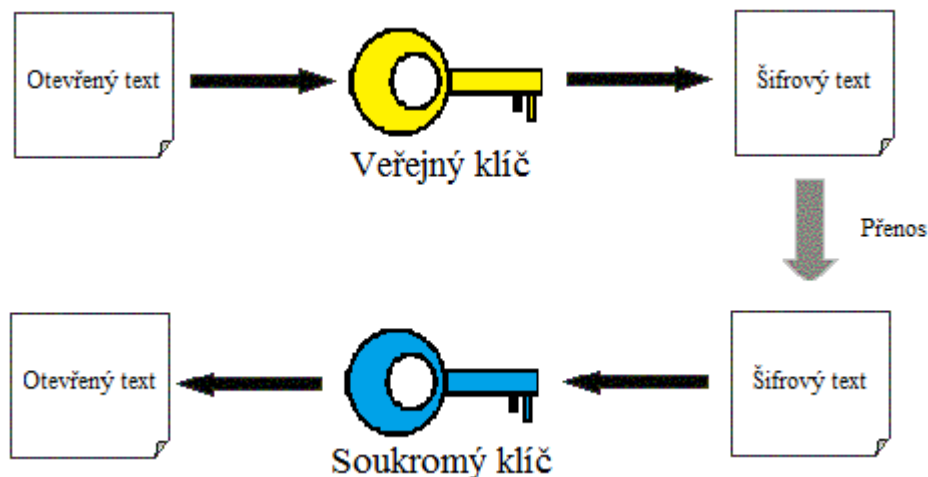
### **Symetrický šifrový systém**

Pojem symetrický šifrový systém se používá v případě, že je klíč pro šifrování a dešifrování stejný. Jsou méně výpočetně náročné. Klíč používaný v symetrickém šifrovém systému se nazývá *symetrický tajný klíč* nebo pouze *tajný klíč*. Mezi symetrické šifrové systémy patří např. Caesarova šifra, Vigenèrova šifra nebo DES.

Obrázek 1: *Symetrický šifrový systém*

### Asymetrický šifrový systém

Tento systém je založen na principu dvou klíčů. První klíč, tzv. veřejný klíč, slouží k zašifrování otevřeného textu, druhý klíč, tzv. soukromý klíč, k dešifrování šifrovaného textu zpět do původní podoby. Veřejný klíč může být znám všem osobám, neboť při dešifrování nebo luštění není potřeba. Dešifrovat šifrovaný text může jen vlastník soukromého klíče, čím větší množství klíčů, tím je bezpečnost šifrované zprávy vyšší. Příkladem asymetrického šifrového systému je RSA.

Obrázek 2: *Asymetrický šifrový systém*

### Modulární aritmetika

Protože se v kryptografii často pracuje s velkými čísly, využívá se při početních operacích s nimi tzv. modulární aritmetika. Je to aritmetika na množině celých čísel  $\mathbb{Z}$ , v níž se čísla

opakují po dosažení určité hodnoty  $m$ . Díky tomu pak lze pracovat s mnohem menšími čísly. Hodnota  $m$  se nazývá modul a značí se  $\text{mod}$ .

V modulární aritmetice se používají následující pojmy a jejich vlastnosti:

1. Celé číslo  $b$  dělí celé číslo  $a$ , jestliže existuje celé číslo  $k$  takové, že  $a = k \cdot b$ .
2. **Věta o dělení se zbytkem:** Jsou-li  $a, b$  celá čísla taková, že  $a \geq 0, b > 0$ , pak existuje právě jedna dvojice čísel  $q, r$  taková, že  $a = q \cdot b + r$ , kde  $q \geq 0, 0 \leq r < b$ .
3. **Největší společný dělitel:** Je největší společné číslo dvou celých čísel  $a, b$ , jímž jsou obě dělitelná beze zbytku.

### Euklidův algoritmus

Používá se k hledání největšího společného dělitele čísel. Princip je založen na následující úvaze. Pokud číslo  $n$  dělí čísla  $a$  i  $b$ , potom existují čísla  $a_1$  i  $b_1$  taková, že

$$a = n \cdot a_1$$

$$b = n \cdot b_1.$$

Tyto dva vztahy se nyní dosadí do výrazu  $a - x \cdot b$ :

$$a - (x \cdot b) = n \cdot a_1 - (x \cdot n \cdot b_1) = n \cdot [a_1 - (x \cdot b_1)],$$

z čehož plyne, že číslo  $n$  dělí  $a - x \cdot b$ .

Užitím předchozích úvah lze pak najít největšího společného dělitele  $n$  čísel  $a, b$ . Budeme předpokládat, že  $a > b$ . Potom podle věty o dělení se zbytkem platí:

$$a = (v \cdot b) + z,$$

kde  $v = \frac{a}{b}$  se zbytkem  $z$ . Největší společný dělitel  $n$  musí být dělitelný  $a, b$  i  $z$  a navíc,

největší společný dělitel čísel  $a, b$  je zároveň největším společným dělitelem  $b$  a  $z$ . Proto lze nahradit čísla  $a, b$  za podmínky  $b > z$  čísly  $b$  a  $z$ :

$$b = (v_1 \cdot z) + z_1,$$

$v_1 = \frac{b}{z}$  se zbytkem  $z_1$ . Ve výpočtech se pokračuje tak dlouho, dokud zbytek nebude roven

nule. Číslo  $v$  je potom největším společným dělitelem.

**Kongruence (shodnost)**

Dvě čísla  $a$ ,  $b$  se nazývají kongruentní podle  $\text{mod } m$ , jestliže rozdíl  $a - b$  je dělitelný číslem  $m$ . Kongruence se zapisuje ve tvaru

$$a \equiv b \pmod{m}.$$

To také znamená, že čísla  $a$  a  $b$  dávají po dělení číslem  $m$  stejný zbytek. Vztah  $a \equiv b \pmod{m}$  lze přepsat do tvaru

$$a = b + k \cdot m,$$

kde  $k \in \mathbb{Z}$ .

Příklad:

$$30 \equiv 12 \pmod{9}$$

$$30 = 12 + (2 \cdot 9), k=2$$

$$\frac{30}{9} = 3,333333$$

$$\frac{12}{9} = 1,333333.$$

**Zbytkové třídy**

Všechna celá čísla, která po dělení číslem  $m$  dávají stejný zbytek, zařazujeme do tzv. *zbytkové třídy modulo  $m$* . K danému číslu  $m$  pak existují zbytkové třídy odpovídající číslům  $0, 1, \dots, m-1$ . Množinu všech zbytkových tříd modulo  $m$  značíme  $\mathbb{Z}_m$ .

**Inverze**

Při matematických výpočtech je důležitá znalost inverze čísla, zvláště pak modulární inverze. Inverze se označuje symbolem  $^{-1}$ . Nejsnadněji se pojem inverze pochopí na příkladu. Příklad inverze:

$$n \cdot (n^{-1}) = n \cdot \frac{1}{n} = 1.$$

Inverze je v podstatě takové číslo, které po provedení algebraické operace (násobení, sčítání) s daným číslem musí dát číslo 1.

### Inverze mod $m$

Při hledání inverzí prvků v modulární aritmetice se vychází ze vztahu

$$1 \equiv a \cdot k \pmod{m}.$$

Tento vztah je možné přepsat jako

$$a^{-1} \equiv k \pmod{m}.$$

Pokud čísla  $a^{-1}$  a  $m$  nemají žádného společného dělitele, pak má inverze jen jediné řešení. Jestliže ovšem společného dělitele mají, potom rovnice  $a^{-1} \equiv k \pmod{m}$  nemá řešení. Když bude číslo  $m$  prvočíslem, potom všechna čísla v intervalu 1 až  $m-1$  budou mít jednu inverzi modulo  $m$ . V některých případech se pro výpočet modulo  $m$  využívá rozšířený Euklidův algoritmus (Kapitola 3.1).

### Prvočísla

Prvočísla hrají významnou roli především u algoritmů s veřejným klíčem. Dlouhá léta se matematikové snaží vymyslet algoritmus na testování, zda náhodně zvolené číslo je prvočíslo. Pro odhad počtu  $\pi(n)$  všech prvočísel menších než dané číslo  $n$  lze užít Gaussův vztah [3]:

$$\pi(n) = \frac{n}{\ln n}.$$

### Test prvočísel

Pro asymetrické šifrové systémy s velkými prvočísly se využívají testy na ověření prvočísel. Existují dvě metody ověření, zda se jedná o prvočíslo. První způsob je ověřování prvočísel s dostatečně velkou pravděpodobností (např. 99,9 % a více). Druhý způsob je pomocí faktorizace, tj. rozkladem čísel na součin prvočísel. Jedná se o složitou metodu a používá se především u útoků na šifry.

Na ověřování prvočísel s určitou pravděpodobností existuje několik možných testů, např. Rabin-Millerův test nebo Lehmanův test.

### Rabin-Millerův test (R-M test)

Kroky při testování  $p$  pomocí Rabin-Millerova testu:

- 1) zvolí se náhodné liché číslo  $p$  a následně se vypočítá  $b$  podle vztahu  $b = \frac{p-1}{2}$ ,

- 2) ověří se, zda je  $p$  dělitelné malými prvočísly,
- 3) určí se  $n$  tak, aby platilo  $p = 1 + (2^b \cdot n)$ ,
- 4) zvolí se náhodné číslo  $m$  tak, aby platilo  $m < p$ ,
- 5) položí se  $j=0$  a  $z \equiv m^n \pmod{p}$  :
  - a. pokud  $j=0$  a  $z=0$  (tzn.  $m^n$  je dělitelné  $p$ ) nebo  $z = p-1$ , pak  $p$  může být prvočíslo,
  - b. je-li  $j > 0$  a  $z=1$ , potom  $p$  není prvočíslo,
  - c. jestliže je  $j=j+1$  a zároveň je  $j < b$  a  $z \neq p-1$ , položí se  $z \equiv z^2 \pmod{p}$  a následně se provede návrat k předcházejícímu kroku; jestliže  $z = p-1$ , pak  $p$  je prvočíslo,
  - d. je-li  $j=b$  a  $z \neq p-1$ , potom  $p$  není prvočíslo,
- 6) číslo  $m$  platí v  $\frac{3}{4}$  případů, test se tedy obrátí na  $0,25^T$ , kde  $T$  je počet opakování výpočtu.

R-M test se několikrát opakuje s různými náhodnými čísly, aby se ověřila jeho správnost [3].

### Lehmanův test

Stejně jako u R-M testu, i u Lehmanova testu se bude testovat  $p$ , postup potom vypadá následovně:

- 1) zvolí se náhodné liché číslo  $p$ , vypočítá se  $b$  (stejně jako u R-M),
- 2) určí se, zda je dělitelné malými prvočísly,
- 3) zvolí se náhodné číslo  $m$  tak, aby platilo  $m < p$ ,
- 4) výpočet  $m^{(p-1)/2} \pmod{p}$ ,
- 5) jestliže  $m^{(p-1)/2} \not\equiv \pm 1 \pmod{p}$ , potom  $p$  není prvočíslo,
- 6) jestliže  $m^{(p-1)/2} \equiv \pm 1 \pmod{p}$ , pak  $p$  je pravděpodobně prvočíslem,
- 7) pokud se opakuje výpočet  $T$ -krát a ve výsledku se neustále střídá  $+1$  a  $-1$ , potom pravděpodobnost, že číslo není prvočíslem, je  $1:2^T$ .

## 1.2 Historie

V této části bakalářské práce jsou zmíněny některé historické milníky, jež měly vliv na vznik a vývoj kryptografie. Dále jsou zde detailně popsány některé historické šifry.

### 1.2.1 Starověk

Informace pro vypracování této části bakalářské práce byly použity z literatury [4], není-li uvedeno jinak.

Počátky kryptografie sahají daleko do historie. První zmínky souvisejí se vznikem písma, konkrétně mezopotámských a egyptských textů. V tehdejší době ovládalo znalosti písma jen několik vzdělců, proto se tedy šifrování využívalo jen zřídka. Za počátek šifrování lze považovat šifru ATBASH, která se objevila ve Starém zákoně. Princip spočíval v záměně konkrétního znaku abecedy za znak ve stejném pořadí z konce abecedy.

Daleko větší význam než šifrování měla v té době steganografie, která ke svému použití nevyžadovala vzdělání, ale především důvtip. Za zmínku stojí příběh Histiaia z roku 440 př. n. l. Tento muž nechal vyholit hlavu svému otroku a na ní napsat zprávu. Když otroku vlasy opět narostly, byl vyslán s touto zprávou.

Tento způsob posílání zpráv byl ovšem zdlouhavý a v mnoha případech, zvláště pak ve válečných situacích, nepřijatelný. Proto vznikaly z důvodu rychlejšího odesílání jiné metody maskování zpráv. Takovým příkladem je člen perského soudu Démerét, který ve Spatsko-perských válkách poslal do Sparty zprávu, kterou vyryl do dřevěné destičky a následně ji polil voskem, takže vypadala nepoužitá. Zpráva byla tak dokonale zamaskována, že ji nemohli rozluštit ani ve Spartě a přišli na ni náhodou.

Šifrování se využívalo především k vojenským a vládním účelům. Toho využívali zejména v Řecku a Římě při válečných taženích, kdy se používaly hlavně šifry substituční a transpozice. Nejznámější substituční šifrou této doby je Caesarova šifra, založena římským císařem Juliem Caesarem.

#### 1.2.1.1 Caesarova šifra

První zmínky o této jednoduché substituční šifře jsou popsány v knize Zápisky o válce galské. Princip této šifry je založen na posunu každého znaku textu o následující tři znaky, tedy například písmeno X bude Caesarovou šifrou nahrazeno za písmeno A. Tuto metodu

lze využít v případě posuvu o jakékoliv libovolné číslo v rozmezí od 1 do 25. Jakékoliv šifrování za pomoci posunu znaků v dnešní době označujeme jako Caesarovu šifru [2].

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tabulka 2: Příklad Caesarovy šifry s posunem o 3 znaky

V horním řádku tabulky jsou vypsané znaky mezinárodní abecedy, v dolním řádku jejich ekvivalenty v Caesarově šifře.

### Matematický zápis Caesarovy šifry při šifrování:

$$C_i(N) = n + k \bmod N,$$

kde  $C_i(N)$  je  $i$ -tý znak šifrovaného textu,  $n$  je znak otevřeného textu,  $k$  je posun a  $N$  je délka používané abecedy.

### Matematický zápis při dešifrování:

$$D_i(N) = m - k \bmod N$$

$C_i(N)$  značí  $i$ -tý znak otevřeného textu,  $m$  je znak šifrovaného textu,  $k$  je posun znaku a  $N$  délka abecedy.

Při konkrétním šifrování nebo dešifrování s posuvem o tři pozice by bylo  $k$  nahrazeno číslem 3.

Tato šifra je kvůli své jednoduchosti v dnešní době nepoužívaná. Ale ve středověku, zvláště ve válečných situacích, byla využívanou a výhodnou metodou při zasílání tajných zpráv.

Následující příklad ukazuje použití Caesarovy šifry s posunem o tři pozice v praxi. S využitím mezinárodní abecedy byla do anglického jazyku přeložena a následně zašifrována slova *Univerzita Tomáše Bati*.

**Otevřený text:** THOMAS BATA UNIVERSITY

**Zašifrovaný text:** WKRPDV EDWD XQLYHUVLWB.

Pro ověření správnosti lze otevřený text zašifrovat pomocí softwaru Wolfram Mathematica.

```
In[1]:= Encryption[text_, key_] :=  
  FromCharacterCode[Mod[ToCharacterCode[text] - 97 + key, 26] + 97]  
text = "thomasbatauniversity"  
key = 3;  
Encryption[text, key]  
Out[1]= wkrpdvedwdxqlyhuvlwb
```

Obrázek 3: Šifrování otevřeného textu Caesarovou šifrou programem Mathematica[6]

## 1.2.2 Středověk a raný novověk

Literatura použitá v následující části je stejná jako v části předešlé [4].

Toto historické období proslavil zejména vznik a rozvoj kryptoanalýzy na Předním východě. Pro kryptoanalytiku bylo zlomové 14. století, kdy byly objeveny první zmínky o řešení jednoduché substituční šifry. Řešení této šifry bylo založeno na frekvenční analýze, tedy na zkoumání počtu jednotlivých znaků v šifrovaném textu. Podrobněji je frekvenční analýza probrána v Kapitole 2.1.

Šifrování v této době nabývá na důležitosti, protože v době válek byla komunikace velmi důležitá, a proto bylo nutné šifry zdokonalit. Jedním z nejznámějších šifrových specialistů byl Francouz Antoine Rossignol, který vytvářel šifry i pro francouzského panovníka. Ve svých šifrách využíval především jednoduchá nahrazení, klamače nebo úmyslné komolení textu. Luštění těchto šifer nebylo moc náročné a brzy se začalo všeobecně využívat. Z toho důvodu byly vymyšleny bezpečnější šifrové systémy, ty se ovšem z důvodu složitosti příliš nevyužívaly. Nejvýznamnější šifrou této doby byla Vigenèrova šifra.

### 1.2.2.1 Vigenèrova šifra

Leon Battista Alberti jako první navrhl v roce 1466 složitější substituční algoritmus za pomoci hesla. Albertiho návrh spočíval v použití dvou nebo více abeced, které by se pravidelně střídaly. Ve svém objevu ovšem i přes obrovský význam dále nepokračoval. Tohoto návrhu využil ke konci 16. století francouzský diplomat Blaise de Vigenère, který ji chtěl využít pro svou práci a podle kterého nakonec dostala jméno. Vigenère Albertiho návrh ovšem upravil a využil většího počtu abeced, vytvořil tzv. Vigenèrův čtverec. Tento čtverec obsahuje v prvním řádku mezinárodní abecedu o délce 26 znaků. Každý následující řádek obsahuje tutéž abecedu s posuvem o jeden znak. Pro vyšší bezpečnost šifry

k abecedě s posunem využil klíč. Potom tedy k dešifrování Vigenèrovy šifry bylo třeba znát šifrový text i klíč.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Obrázek 4: Vigenèrův čtverec

První žlutě označený sloupec slouží k hledání znaků abecedy pro klíč použitý k šifrování, první žlutě označený řádek pro text.

#### Matematický zápis Vigenèrovy šifry při šifrování:

$$C_i \equiv D_i + K_i \pmod{N}$$

#### Matematický zápis Vigenèrovy šifry při dešifrování:

$$D_i \equiv C_i - K_i \pmod{N}$$

Kde  $C_i$  je  $i$ -tý znak šifrovaného textu,  $D_i$  je  $i$ -tý znak otevřeného textu,  $K_i$  je  $i$ -tý znak hesla textu,  $N$  označuje délku abecedy.

V případě šifrování i dešifrování je třeba počítat s tím, že délka hesla je menší než text, v takovém případě dochází k opakování hesla. Tento případ je názorně předveden v následujícím příkladu. Otevřený text je stejně jakou u Caesarovy šifry anglické slovo *Thomas Bata university*, jako klíč se použije slovo *BTSM*.

**Otevřený text:** THOMAS BATA UNIVERSITY

**Klíč:** BTSM.

Každý znak klíče se zapíše pod příslušný znak otevřeného textu, v případě krátkého klíče se znaky klíče opakují.

T H O M A S    B A T A    U N I V E R S I T Y  
B T S M B T    S M B T    S M B T S M B T S M

Následně se celý text zašifruje podle Vigenèrova čtverce uvedeného na předešlé straně.

**Zašifrovaný text:** UAGYBL TMUT MZJOWDTBLK

Ověření správnosti zašifrování otevřeného textu lze opět provést v programu Mathematica.

```
In[1]:= AddTwoLetters[a_, b_] :=
  FromCharCode[Mod[(ToCharCode[a] - 97) + (ToCharCode[b] - 97), 26] + 97]
text = "thomasbatauniversity";
key = "btsm";
ciphertext = "";
Do[
  ciphertext =
    ciphertext <> AddTwoLetters[StringTake[text, {i}],
      StringTake[key, {Mod[i - 1, StringLength[key]] + 1}],
      {i, 1, StringLength[text]}];
  ciphertext
Out[1]= uagybltmutmzjowdtblk
```

Obrázek 5: Šifrování otevřeného text Vigenèrovou šifrou v programu Mathematica [6]

Výhoda této šifry spočívá ve vyjádření jednoho znaku otevřeného textu více znaky šifrovaného textu, tudíž prolomení šifrovaného textu obyčejnou frekvenční analýzou odpadá. Je tedy vidět, že daná šifra byla na svou dobu velice složitá a pro své účely velice výhodná.

### 1.2.3 Dvacáté století

Literatura použitá pro vypracování této části je stejná jako v části předešlé [4].

Klíčovou roli v této době má vznik rádia a s tím spojený rozvoj komunikace, která byla daleko rychlejší. Z toho důvodu bylo nutné šifrovat rychle a bezpečně, zvláště pak při organizaci útoků měla rychlost dešifrování zprávy důležitou roli. V období válek byla kryptografie klíčem k úspěchu. Používaly se především kódové knihy, pomocí kterých se zprávy kodovaly. Nejpoužívanější šifry byly tzv. polní šifry, založené v 19. století. Polní šifry byly založeny na složitějších substitucích, jako například Playfairova šifra.

### 1.2.3.1 Playfairova šifra

Šifra byla vytvořena v roce 1854 britským vědcem Charlesem Wheatstonem, ovšem pojmenována byla po jeho příteli lordu Lyonu Playfairu, který jí proslavil prosazením ve vládě. Tím se šifra stala používanou nejen ve válečných, ale i v politických situacích. Tato šifra pracuje na principu šifrování otevřeného textu podle klíče, čímž znesnadní případné luštění šifrovaného textu třetí stranou.

Základem celé Playfairovy šifry je klíč, v tomto případě *BTSM*, vložený do tabulky o rozměrech 5x5. Zbytek volných políček se postupně doplní zbývajícími znaky abecedy, příklad je znázorněn v následující tabulce. Jelikož abeceda obsahuje 26 znaků a tabulka má jen 25 políček, je jeden znak abecedy vymazán, např. písmeno *Q* v českém jazyce nebo sloučeno s jiným písmenem, např. *I* s *J* v anglickém jazyce. V tomto případě došlo ke sloučení písmena *J* s *I* a zapisuje se jako písmeno *I*, jelikož šifrovaný text je v angličtině a četnost výskytu písmena *J* v anglickém jazyce je nejnižší.

B	T	S	M	A
C	D	E	F	G
H	I	K	L	N
O	P	Q	R	U
V	W	X	Y	Z

Tabulka 3: Klíč v tabulce s doplňujícími znaky

Nyní se otevřený text rozdělí na bigramy, tedy text *THOMAS BATA UNIVERSITY* bude následně vypadat: *TH OM AS BA TA UN IV ER SI TY*, v textu se nenachází žádné písmeno *J*, tudíž se nemusí nic nahrazovat. V případě, že je v textu lichý počet znaků, doplní se o jeden znak, např. písmeno *X* tak, aby počet znaků byl sudý. To se provádí i v případě, že se v textu nachází dva stejné znaky za sebou, aby nevzbuzovaly pozornost.

Po upravení textu se provede úprava tabulky s klíčem a následně je možno šifrovat otevřený text. Nejprve tabulku s klíčem rozšíříme o první sloupec a první řádek a oba umístíme na konec tabulky. Tabulka tedy bude vypadat následovně:

B	T	S	M	A	B
C	D	E	F	G	C
H	I	K	L	N	H
O	P	Q	R	U	O
V	W	X	Y	Z	V
B	T	S	M	A	

Tabulka 4: Rozšířená tabulka s klíčem

Po provedení této úpravy se přejde k samotnému šifrování, kdy se v tabulce hledají bigramy a k nimž se přiřadí podle tabulky jejich ekvivalenty v šifrové podobě. Pokud se oba znaky nachází v jednom sloupci nebo řádku, dochází k posunu znaku o jednu pozici vpravo, resp. o jednu pozici dolů. Znaky nenacházející se ve stejném sloupci nebo řádku se šifrují do kříže, podle pozice v textu. Takže šifrový ekvivalent bigramu *TH* v tabulce s rozšířeným klíčem bude *BI*. Stejně se postupuje i u dalších bigramů, tzn. *OM* je zašifrováno jako *RB*, *AS* jako *BM*, atd. Celý šifrovaný text tedy bude mít následující podobu: *BI RB BM TB SB ZU HW FQ TK MW*.

**Klíč:** BTSM

**Otevřený text:** TH OM AS BA TA UN IV ER SI TY

**Šifrovaný text:** BI RB BM TB SB ZU HW FQ TK MW.

Zlom pro kryptologii nastal v roce 1931, kdy se tvorbou a zdokonalováním šifer začali zabývat především matematikové. S technickým rozvojem došlo k mechanizaci šifrování. Nejznámějším příkladem mechanického šifrování je německá šifra Enigma, využívaná v druhé světové válce. Tato šifra hrála tehdy důležitou roli, neboť byla dlouhou dobu nerozluštitelná a poskytovala Německu výhodu nad nepřátelskými vojsky. Prolomení Enigmy bylo klíčovou událostí druhé světové války, protože tím spojenci získali výhodu nad nepřítelem a ukončili vleklou válku. Enigma nebyla jediná šifra využívaná v této válce, Japonsko používalo k šifrování mechanický přístroj Purple. USA se proslavilo především pseudošifrou Navajo, kterou tvořila slova indiánského jazyka, jenž se výrazně liší od ostatních jazyků. Tuto šifru kvůli odlišnosti jazyka nebylo možno rozšifrovat bez pomoci cizojazyčných dokumentů nebo jiných osob mluvících stejnou řečí. Slabým místem této šifry byli příslušníci indiánského kmene, kterým musela být poskytována ochrana, aby nemohla být šifra prolomena. Každý Navaj dostal speciální ochranu, která měla za úkol zabránit, aby Navajové padli do zajetí. V případě, že nebyla jiná možnost, měla ochranka příkaz svého svěřence zastřelit.

Významnou roli sehrála v této době především steganografie, ve které došlo k obrovskému pokroku. Už v 19. století začaly být zprávy zmenšovány do velikosti inkoustové skvrny. V pozdějších letech byla tato metoda Německem zdokonalena a zprávy se zmenšovaly do velikosti tečky. Toho se využívalo při psaní zpráv, kdy takto skryté zprávy nahrazovaly

tečky ve větech. Tato metoda měla všeobecný obdiv a v roce 1941 ji ředitel FBI J. Edgar Hoover označil za mistrovské dílo nepřítele.

#### 1.2.4 Moderní kryptologie

S rozvojem počítačů došlo i k vývoji a rozšíření v oblasti kryptologie. Za pomoci počítačů bylo možno šifrovat s přesností a bez omylů, což v dřívějších dobách nebylo možné. Kryptologie pozvolna proniká z vojenských a politických sektorů do všedního života. S novou politickou situací dochází k zveřejňování kryptografických publikací autorů z období válek. Jednou z prvních publikací je kniha Davida Kahna *The Codebreakers* z roku 1967. Kahnovou knihou se inspirovali Whitfield Diffie a Martin Hellman, ti na základě svých výzkumů a poznatků vydali vlastní článek, ve kterém představili svůj šifrovací algoritmus, založený na principu dvou různých klíčů (asymetrická šifra). Jejich nápad později matematicky realizovali Ron Rivest, Adi Shamir a Len Adleman. Tento algoritmus je v současné době znám jako RSA.

Největší kryptologický rozvoj nastal v USA, kde byl ovšem brzděn vládou. Zde byly šifrovací algoritmy tvořeny tak, aby byly vládní složky schopny prolomit každou šifru. Nejznámějším příkladem je standard DES, u něhož byla velikost klíče snížena z 64 bitů na 56 bitů, což byla hraniční možnost na překonání tehdejšími počítači.

V současné době šifrování prorazilo do mnoha oblastí, zvláště v bezpečnosti má nezastupitelné místo. Šifrování se využívá v komunikaci, jako například při posílání dat po Internetu, přenosu signálu z mobilních telefonů apod. V průmyslu komerční bezpečnosti se šifrování používá například v komunikaci s pultem centrální ochrany nebo jinými objekty, případně osobami, při přenosu dat nebo komunikace pomocí Wi-Fi, Bluetooth a jiných, u přístupových systémů apod.

##### 1.2.4.1 Algoritmus RSA

Tento způsob šifrování vznikl v roce 1977 jako náhrada za symetrické šifrové systémy, kdy k šifrování používal dvou klíčů, veřejného a soukromého. Asymetrická šifra pojmenovaná po autorech (Rivest-Shamir-Adelman) byla původně patentová šifra patřící Public Key Partners, později ale patent vypršel a RSA se začala hojně využívat ve všech oblastech. RSA se kvůli své vysoké bezpečnosti využívá i v dnešní době, např. v mobilních telefonech, bankomatech nebo v elektronických podpisech. Důvod vysoké spolehlivosti a

bezpečnosti algoritmu RSA spočívá v náročné faktorizaci. V současné době není znám algoritmus, pomocí něhož by šlo rozložit velmi vysoká čísla na dvě dostatečně velká prvočísla. Podrobný rozbor algoritmu RSA je uveden v Kapitole 3.

## **II. PRAKTICKÁ ČÁST**

## 2 KRYPTOANALÝZA

Informace v této kapitole jsou čerpány z literatury [3], není-li uvedeno jinak.

Se vznikem šifer přišla i snaha o jejich prolomení, především za účelem osobního obohacení. Jak již bylo napsáno v předešlých kapitolách, prolomení šifry hrálo v mnoha, především válečných konfliktech, klíčovou roli. Z toho důvodu odborníci z oboru kryptoanalýzy vytvářeli algoritmy na jejich vyluštění bez znalosti klíče. Při kryptoanalytickém útoku se využívá všech znalostí o šifrovaném textu, které má kryptoanalytik k dispozici. Což mohou být například:

### **Znalost otevřeného textu**

Předpokládá se, že kryptoanalytik ví, ve kterém jazyce je napsána zpráva, obsah zprávy nebo alespoň části zprávy.

### **Informace v otevřeném textu**

Těmi mohou být např. interpunkční znaménka, struktura slov, apod.

### **Znalosti o kryptosystému**

Kryptoanalytik má podrobné informace o použitém klíči, tj. délku, strukturu a způsob, jakým byl odvozen soukromý klíč od veřejného. Dále má znalosti o odolnosti daného kryptosystému a jiné informace.

### **Porušení kryptografických protokolů**

Zde spadá především opakované používání stejného hesla, především u Vernamovy šifry se jedná o jedinou možnost prolomení, jinak je nemožné ji prolomit.

### **Specifické znalosti**

Kryptoanalytik má znalosti o dostupnosti veřejného klíče, což mu umožňuje útok hrubou silou na šifrový text, např. generováním a porovnáváním náhodného textu s textem šifrovým.

Podle znalostí o otevřeném a šifrovaném textu existují následující kryptoanalytické útoky:

**Znalost pouze šifrového textu** (ciphertext only attack)

Kryptoanalytik pracuje pouze s částí šifrového textu, na kterém provádí patřičné procesy, jako je např. frekvenční analýza, pravděpodobnost, distribuce, apod. Pokud kryptosystém nedokáže odolat takovému typu útoku, není bezpečný.

**Částečná znalost přímého textu** (probably plaintext attack)

Kryptoanalytik má přibližné informace o zprávě, tj. důvod odeslání, čímž usnadní možný odhad o obsahu zprávy. Stejně jako u znalosti pouze šifrového textu, i zde musí používaný kryptosystém odolat útokům, jinak jej nelze považovat za bezpečný.

**Znalost přímého textu** (known plaintext attack)

V tomto případě má kryptoanalytik k dispozici část otevřeného textu a k němu jeho šifrový ekvivalent.

**Znalost zvoleného otevřeného textu** (chosen plaintext attack, adaptive chosen plaintext attack)

Jedná se o velmi používaný útok, kdy kryptoanalytik získá k libovolnému otevřenému textu text šifrovaný. Tento způsob se nazývá *útok hrubou silou*, kdy se využívá veřejného klíče.

V mnoha případech dochází k zveřejňování šifrovacích algoritmů mnohými autory, kteří tak zjišťují odolnost daného algoritmu a mohou jej případně zdokonalovat. Tento způsob byl zvolen např. k ověření odolnosti DES, kdy na reakci na prolomení vznikli zdokonalení nástupci, kteří nebyli dodnes prolomeni (IDEA, TripleDES). V této kapitole jsou popsány jen některé z možných kryptoanalytických útoků. K šifrování a následným ukázkám způsobu kryptoanalytických útoků byl použit úryvek textu z knihy Tonyho Howletta *Open source security tools: practical applications for security* [5] uvedený v Příloze I. Protože pro luštění je nejlepší mezinárodní abeceda, byl zvolen text v anglickém jazyce.

## 2.1 Frekvenční analýza

Tato metoda kryptografického útoku, někdy též známá jako statická analýza, pochází z 9. století, kdy ji světu předvedl Abú Jusúf Jaqúb ibn Ishád ibn as-Sabbáh ibn`omrán ibn Ismail al-Kindí. Podstatou frekvenční analýzy je porovnání frekvence výskytu znaků šifrovaného textu s frekvencí znaků daného jazyka. Nejúčinnějším útokem proti

monoalfabetickým šifrám (např. Caesarova šifra) je frekvenční analýza. S vyšším množstvím šifrovaného textu roste úspěšnost kryptoanalytického útoku statickou analýzou. V následující části bude frekvenční analýza předvedena na několika šifrách. Text zašifrovaný jednotlivými šiframi bude uveden v příloze za původním otevřeným textem. Jako klíč k šifrování otevřeného textu bylo použito slovo *ENCRYPTION*.

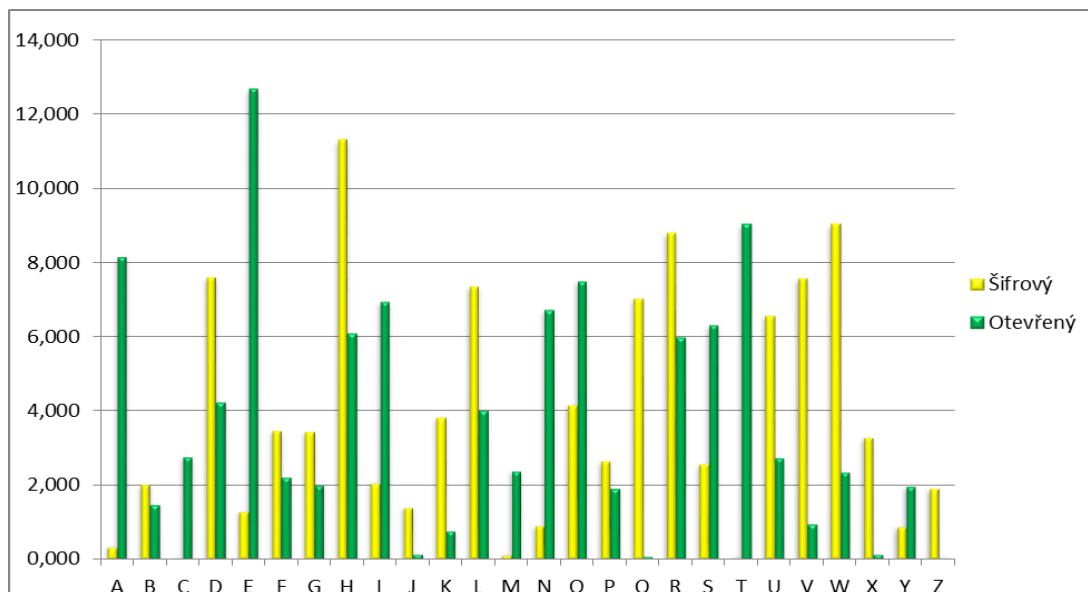
### 2.1.1 Frekvenční analýza – Caesarova šifra

Caesarova šifra (Kapitola 1.2.1.1) kvůli absenci klíče patří k nejjednodušším šifrám, tudíž se na ní frekvenční analýza provádí nejsnadněji. V tomto případě stačí určit ekvivalent k jednomu znaku a následující znaky se získají dešifrovacím postupem. V tabulce jsou uvedeny četnosti šifrovaného textu a výskyt jednotlivých znaků anglické abecedy.

	Četnost AJ [%]	Šifrovaný [%]
A	8,167	0,337
B	1,492	2,028
C	2,782	0,067
D	4,253	7,609
E	12,702	1,296
F	2,228	3,476
G	2,015	3,459
H	6,094	11,312
I	6,966	2,079
J	0,153	1,422
K	0,772	3,838
L	4,025	7,365
M	2,406	0,135
N	6,749	0,909
O	7,507	4,166
P	1,929	2,66
Q	0,095	7,045
R	5,987	8,812
S	6,327	2,584
T	9,056	0,084
U	2,758	6,582
V	0,978	7,592
W	2,36	9,056
X	0,15	3,283
Y	1,974	0,884
Z	0,074	1,919

Tabulka 5: Četnost výskytu znaků zašifrovaného textu Caesarovou šifrou a výskyt znaků v anglickém jazyce

Názorněji lze vidět výskyt znaků v následujícím grafu.



Obrázek 6: Graf četnosti výskytu znaků zašifrovaného textu Caesarovou šifrou a výskyt znaků v anglickém jazyce

Z grafu je vidět, že nejvyskytovanějším znakem šifrovaného textu je písmeno *H* a otevřeného textu písmeno *E*. Z toho lze soudit, že  $H=E$ . Důkazem je i fakt, že písmeno *E* posunuté o tři pozice vpravo odpovídá písmenu *H*, tudíž jsou splněny zásady pro šifrování, resp. dešifrování, pomocí Caesarovy šifry.

### 2.1.2 Frekvenční analýza – Vigenèrova šifra

Vigenèrovu šifru klasickou frekvenční analýzou rozluštit nelze, jelikož se k šifrování používá 26 různých abeced. Tím dochází k rovnoměrnému rozložení znaků, což neodpovídá rozložení znaků otevřeného textu, a proto je zapotřebí využít pokročilou frekvenční analýzu. Tuto pokročilou metodu vymyslel Charles Babage, který jako první roku 1845 za pomoci prvních počítačů Vigenèrovu šifru prolomil. Složitost luštění Vigenèrovy šifry spočívá ve velkém množství použitých abeced, tzn. jeden znak bude zašifrován více znaky. Z toho důvodu je četnost znaků vyrovnanější než u klasických monoalfabetických substitučních šifer. Luštění textu šifrovaného Vigenèrovou šifrou je náročné a zdlouhavé, proto se využívá především výpočetní techniky. V následující ukázce bude proveden útok na šifrový text zmíněný v Kapitole 2 s použitím příslušného klíče.

Při pokusu vyluštit šifrový text je nutné vyhledat skupinu znaků opakujících se vícekrát v celém šifrovém textu, tato skupina se někdy označuje *sekvence*. Sekvence by měla obsahovat co nejvíce znaků, nejméně ovšem čtyři.

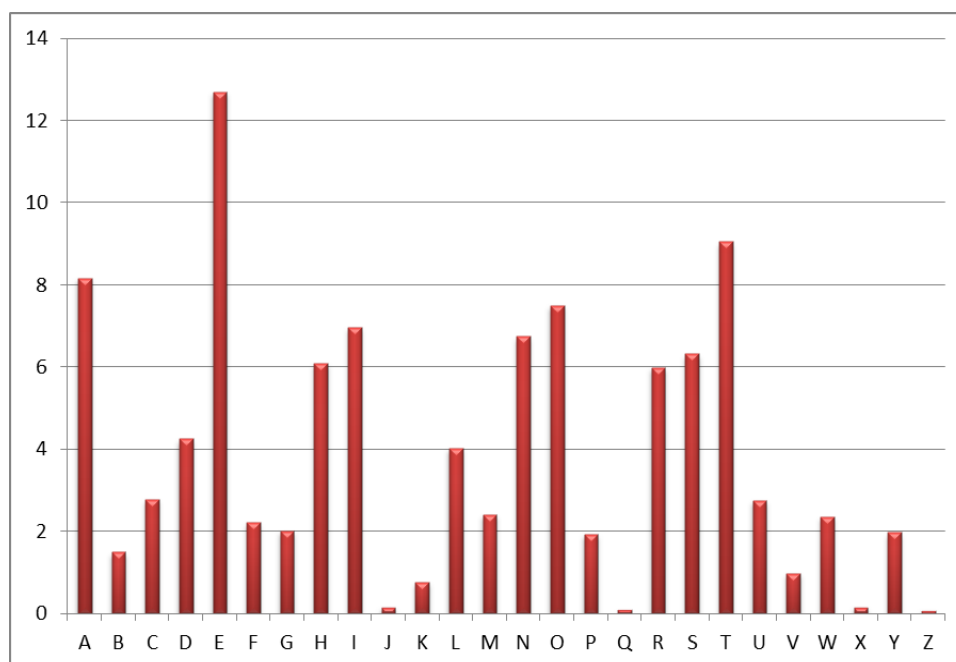
Opakovaná sekvence	Interval mezi opakováním	Délka klíče																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
T-E-G-W	9760	■	■		■	■			■	■							■				■
C-C-B-H-S-A-W-L-Q-L-K	770	■	■			■		■		■	■				■						
X-G-B-S	2630	■	■			■				■											
Q-G-O-S-B-M	1270	■	■			■				■											
V-B-I-I-Y-B-L	10400	■	■		■	■			■	■				■				■			■
Z-S-E-G	3860	■	■		■	■				■											■
E-Y-Q-T-V-C-F-X-L-V	770	■	■			■		■		■	■										
G-R-G-H-T-Z-R	130	■	■			■				■				■							

Tabulka 6: Údaje o opakovaných sekvencích

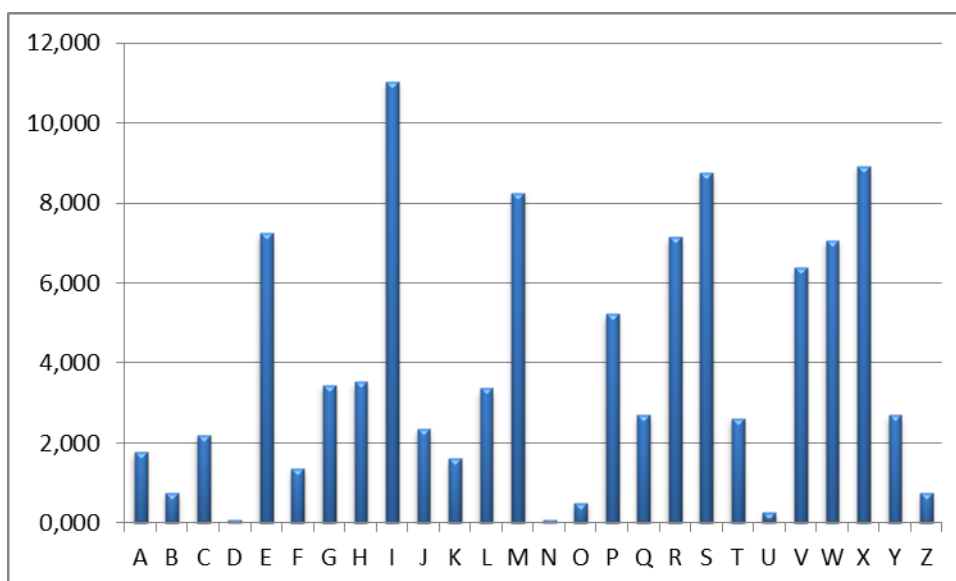
Tabulka názorně zobrazuje některé příklady opakovaných sekvencí ze zašifrovaného textu a údaje o nich, jako např. počet znaků mezi opakujícími se sekvencemi nebo možnou délku klíče. Při luštění Vigenèrovy šifry je nutné znát způsob šifrování i dešifrování (Kapitola 1.2.2.1). Hlavním cílem pokročilé frekvenční analýzy je zjištění klíče, s jehož pomocí je dešifrování textu snadné. Nejprve se musí zjistit délka klíče, v tomto případě se počítá s délkou klíče menší nebo rovnou dvaceti znakům. Délka se dá určit i za pomoci tzv. faktorů opakování. Jedná se o dělitele intervalu mezi opakováním, tzn. znaky *G-R-G-H-T-Z-R* se opakují po 130 znacích, takže faktory opakování potom budou čísla 1, 2, 5, 10, 13, 26, 65 a 130. Faktory musí být celočíselnými děliteli. V tomto případě, jak již bylo zmíněno výše, bude stačit uvažovat s délkou klíče do 20 znaků. Z tabulky lze zjistit, že nejčastěji se opakují délky o 1, 2, 5 a 10 znacích. O klíči s délkou jednoho znaku se neuvažuje, jelikož by se jednalo o klasickou monoalfabetickou šifru. Ze zbylých možných délek klíčů je nejpravděpodobnější nejdelší desetiznakový klíč.

Po určení možné délky klíče je třeba zjistit znaky klíče, ty se pro začátek zvolí jako písmena  $X_1, X_2$  až  $X_{10}$ , kdy  $X_1$  označuje první znak klíče,  $X_2$  druhý znak klíče atd. První znak otevřeného textu byl tedy šifrován písmenem  $X_1$ , druhý znak otevřeného textu písmenem  $X_2$ . Takto se postupuje až po desátý znak otevřeného textu, šifrovaný písmenem  $X_{10}$ , a poté se celý cyklus opakuje pro následujících deset znaků, např. jedenáctý znak bude šifrován opět prvním znakem klíče, tedy  $X_1$ . Pro každý znak označovaný písmeny  $X_1$  až  $X_{10}$  je použita jiná abeceda. Z toho vyplývá, že polyalfabetická šifra se skládá z deseti monoalfabetických šifer.  $X_1$  je definován abecedou s neznámým posuvem, která se skládá z 1., 11., 21., atd. znaku. Obdobným způsobem jsou definovány abecedy i pro  $X_2$  až  $X_{10}$ .

Následně se provede frekvenční analýza pro všech deset abeced a určí se znaky odpovídající jednotlivým písmenům.



Obrázek 7: Četnost výskytu jednotlivých znaků v anglickém jazyce



Obrázek 8: Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X_1$

Pro přehlednost jsou grafy zobrazeny jednotlivě. U těchto grafů se musí věnovat pozornost nejvýraznějším rysům, tj. např. zřetelné stoupání nebo klesání. Např. u prvního grafu (Obrázek 7) je nejvýraznější část u písmen R, S, T, po nichž následuje výrazný pokles až po písmeno Z. U grafu četnosti výskytu znaků definovaných písmenem  $X_1$  (Obrázek 8) by tomu mohla odpovídat část u písmen V, W, X, kde V, W, X je podobná R, S, T, a po obou

případech nastává výrazný pokles, v případě  $V$ ,  $W$ ,  $X$  až po písmeno  $E$ . To by znamenalo, že posun pro abecedu definovanou písmenem  $X_I$  je o 4 znaky, a proto by v tomto případě bylo  $X_I=E$ . Pro přehlednost je možno uvést tabulku pro všechna písmena  $X$ .

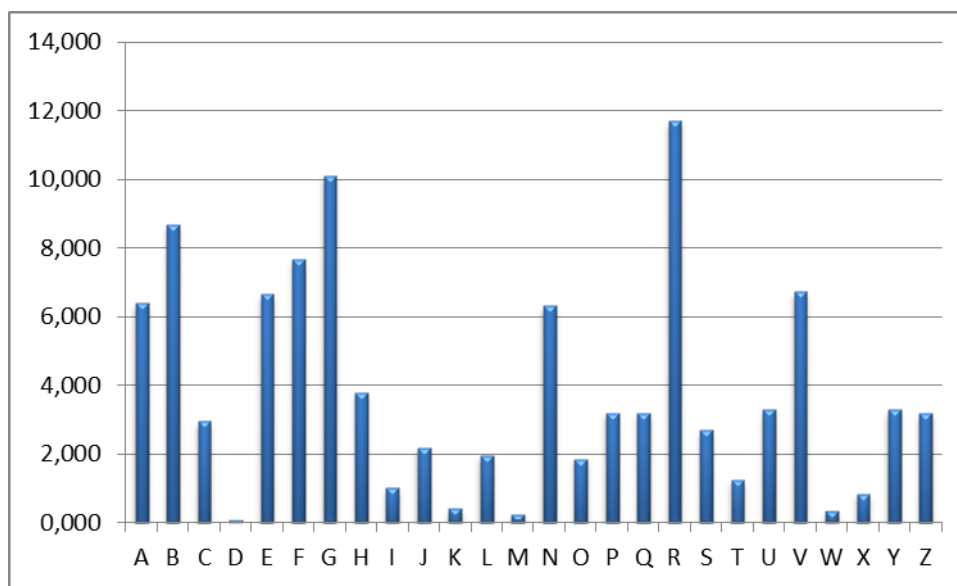
	Četnost v AJ	$X_1$	$X_2$	$X_3$	$X_4$	$X_5$	$X_6$	$X_7$	$X_8$	$X_9$	$X_{10}$
A	8,167	1,766	6,397	2,020	0,168	2,946	4,545	3,535	6,818	2,189	6,397
B	1,492	0,757	8,670	0,253	0,842	3,535	2,694	7,744	9,343	8,165	8,081
C	2,782	2,187	2,946	7,997	4,209	11,111	7,997	0,337	3,956	8,502	2,778
D	4,253	0,084	0,084	1,178	3,114	1,094	7,407	1,263	1,178	2,189	0,168
E	12,702	7,233	6,650	3,114	6,397	1,515	2,441	3,620	2,609	0,084	6,987
F	2,228	1,346	7,660	2,778	9,512	3,114	0,000	2,357	0,168	7,071	7,155
G	2,015	3,448	10,101	10,269	2,946	6,313	7,155	5,808	2,273	7,323	9,343
H	6,094	3,532	3,788	2,020	0,000	0,000	7,576	9,596	0,000	8,333	3,956
I	6,966	11,018	1,010	1,852	6,229	1,094	8,081	2,441	6,818	3,788	1,094
J	0,153	2,355	2,189	5,219	7,576	4,545	2,694	0,168	1,347	1,094	1,936
K	0,772	1,598	0,421	6,818	7,492	2,104	0,421	6,734	4,630	1,263	0,168
L	4,025	3,364	1,936	0,084	2,189	6,650	2,273	7,912	3,114	0,421	1,768
M	2,406	8,242	0,253	0,842	0,842	8,923	0,337	9,848	10,859	1,852	0,000
N	6,749	0,084	6,313	4,125	2,441	2,862	2,441	3,030	2,525	0,084	7,239
O	7,507	0,505	1,852	3,114	0,168	0,000	0,000	1,010	1,178	7,912	0,673
P	1,929	5,214	3,199	6,902	2,273	6,061	7,744	1,768	4,545	1,431	3,451
Q	0,095	2,691	3,199	10,101	0,000	10,185	1,094	0,168	7,239	2,946	4,040
R	5,987	7,149	11,700	2,609	8,081	9,933	3,956	1,599	0,000	3,620	10,859
S	6,327	8,747	2,694	0,084	0,926	3,451	4,125	0,000	0,673	11,532	1,936
T	9,056	2,607	1,263	6,397	3,788	0,673	12,037	7,492	2,862	2,020	1,178
U	2,758	0,252	3,283	6,650	3,367	1,094	2,104	1,768	2,525	1,347	4,882
V	0,978	6,392	6,734	9,175	11,785	0,253	1,431	3,283	8,586	3,620	6,987
W	2,36	7,065	0,337	3,283	1,852	1,936	3,451	3,283	8,586	7,912	0,253
X	0,15	8,915	0,842	0,758	1,768	0,000	6,987	11,953	2,020	0,000	0,589
Y	1,974	2,691	3,283	1,852	3,367	9,259	0,084	2,189	0,000	1,515	5,471
Z	0,074	0,757	3,199	0,505	8,670	1,347	0,926	1,094	6,145	3,788	2,609

Tabulka 7: Přehled četnosti výskytu znaků v anglickém jazyce a pro jednotlivá písmena  $X$

Jelikož nemusí být v mnoha případech odvození posuvu abecedy z grafu přesné, je možné odvodit posuv pro abecedy definované písmenem  $X$  z tabulky četnosti výskytu znaků. Z tabulky se pro názornost vybere písmeno abecedy s charakteristickou hodnotou četnosti výskytu. Může to být jakýkoliv znak, ovšem nejlépe se tato metoda uplatňuje na znacích s nevyšší nebo nejnižší hodnotou výskytu. Jedná se v podstatě o stejnou metodu jako je porovnávání hodnot z grafu, jen v přesnějším číselném vyjádření a méně graficky přívětivém. Vezme-li se opět příklad s určením posuvu abecedy definovanou písmenem  $X_I$ , potom nejlepší volbou pro určení je písmeno  $Z$ , jelikož má nejnižší hodnotu četnosti

výskytu ve sloupci četnosti v AJ. Hodnota písmene  $Z$  se porovnává s hodnotami ve sloupci  $X_1$ . Jelikož stejná hodnota se ve sloupci  $X_1$  nevyskytuje, je potřeba hledat hodnoty blízké hodnotě písmene  $Z$ . Nejbližší k hodnotě písmene  $Z$  má hodnota písmene  $D$ . Vzdálenost mezi písmeny  $Z$  a  $D$  jsou čtyři znaky, tzn. posuv abecedy definované písmenem  $X_1$  bude o 4 znaky a abeceda bude začínat písmenem  $E$  ( $X_1=E$ ). Tento způsob potvrdil správnost odvození znaku z grafu četnosti výskytu. Nemusí to být ale pokaždé stejně, v mnoha případech nejnížší hodnota četnosti v AJ neodpovídá nejnížší hodnotě znaku abecedy definované písmenem  $X$ . Ovšem jak již bylo řečeno, metoda pokročilé frekvenční analýzy je určena především pro výpočetní techniku, jelikož je značně náročná a při manuálním provádění i nepřesná.

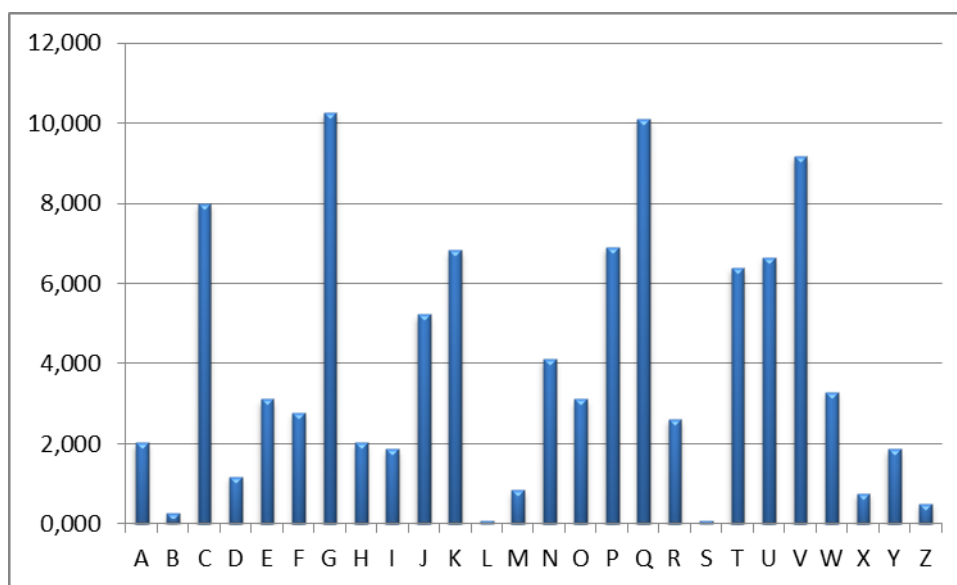
Tímto způsobem se zjišťují i další posuvy abecedy definované písmenou  $X$ . Při zjišťování posuvu definovaného písmenem  $X_2$  je možno opět využít jak tabulky, tak i grafu. Po porovnání grafů *Četnost výskytu jednotlivých znaků v anglickém jazyce* (Obrázek 7) a *Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X_2$*  (Obrázek 9) lze najít jistou shodu v části prvního grafu mezi písmeny  $S, T, U$  a druhého grafu mezi písmeny  $F, G, H$ , po kterých v obou případech následuje pokles po písmeno  $A$  resp.  $N$ . Z toho by se dalo soudit, že písmeno  $X_2$  definuje posuv abecedy o 13 znaků, potom tedy platí  $X_2=N$ . V tomto případě je hledání příslušných hodnot v tabulce zdlouhavé a nepřesné, proto se nevyplatí manuálně provádět.



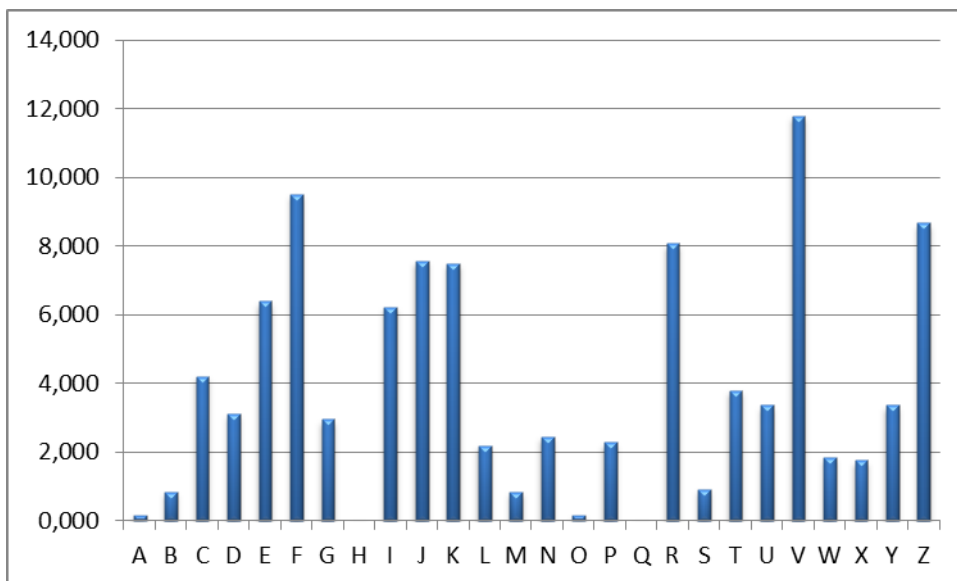
Obrázek 9: Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X_2$

Při hledání posunu abecedy definované písmenem  $X_3$  se opět využije tabulky a grafu. Porovnáním prvního grafu (Obrázek 7) a grafu *Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X_3$*  (Obrázek 10) a výběrem nejpodobnějších rysů obou grafů lze zjistit posunutí abecedy definované písmenem  $X_3=C$ , tzn. posuv je o dva znaky. To je možno vypočítat i z tabulky *Přehled četnosti výskytu znaků v anglickém jazyce a pro jednotlivá písmena  $X$*  (Tabulka 5), kde jsou značné poklesy a stoupání hodnot četnosti jednotlivých znaků.

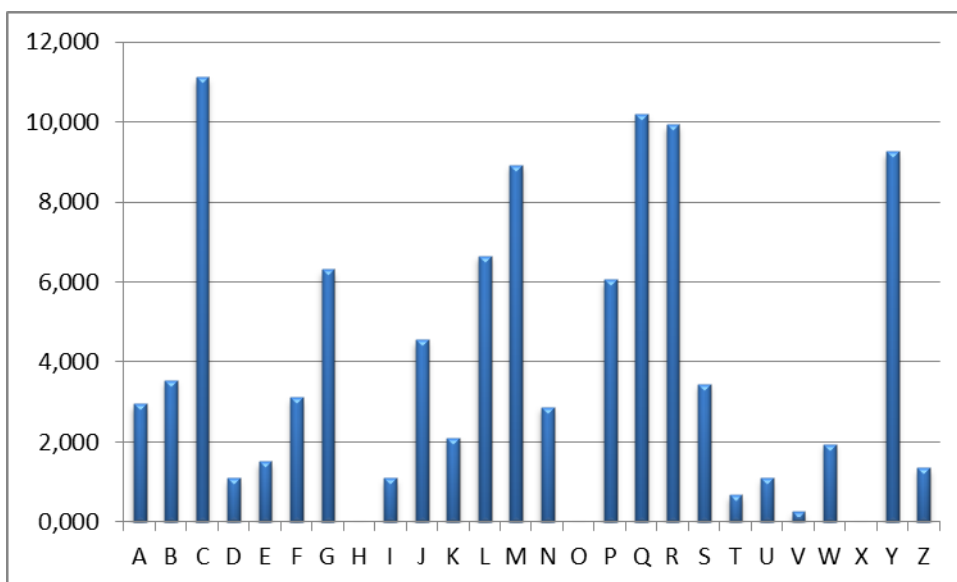
Tento postup se aplikuje i na zbývající písmena  $X$  definující posun abecedy. Opět je možné definovat hodnoty  $X$  pomocí tabulky nebo grafů



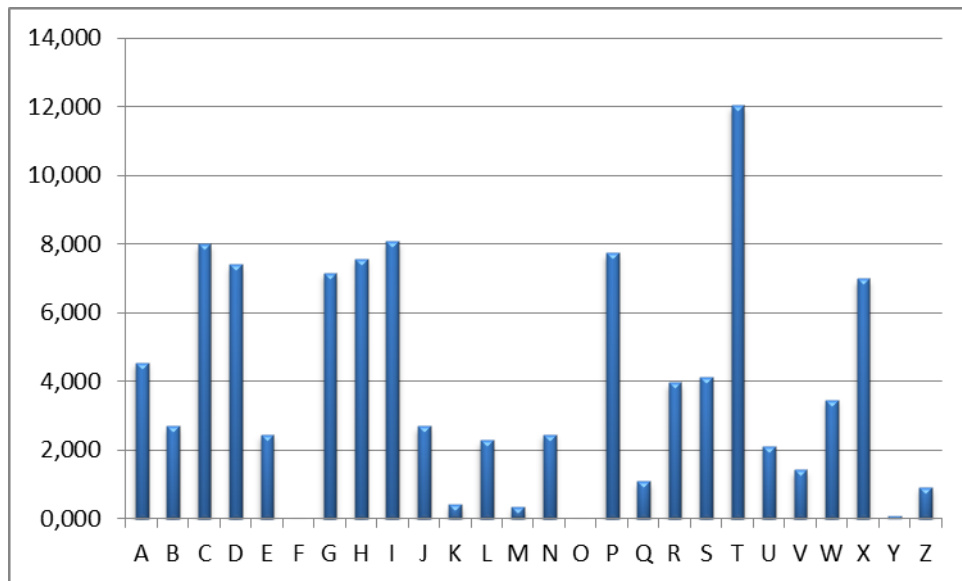
Obrázek 10: *Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X_3$*



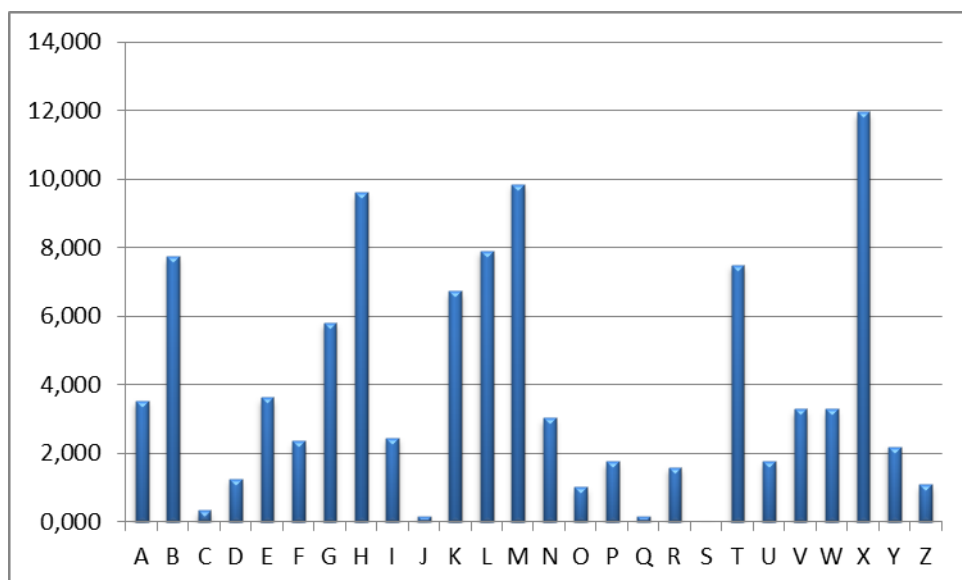
Obrázek 11: Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X_4$



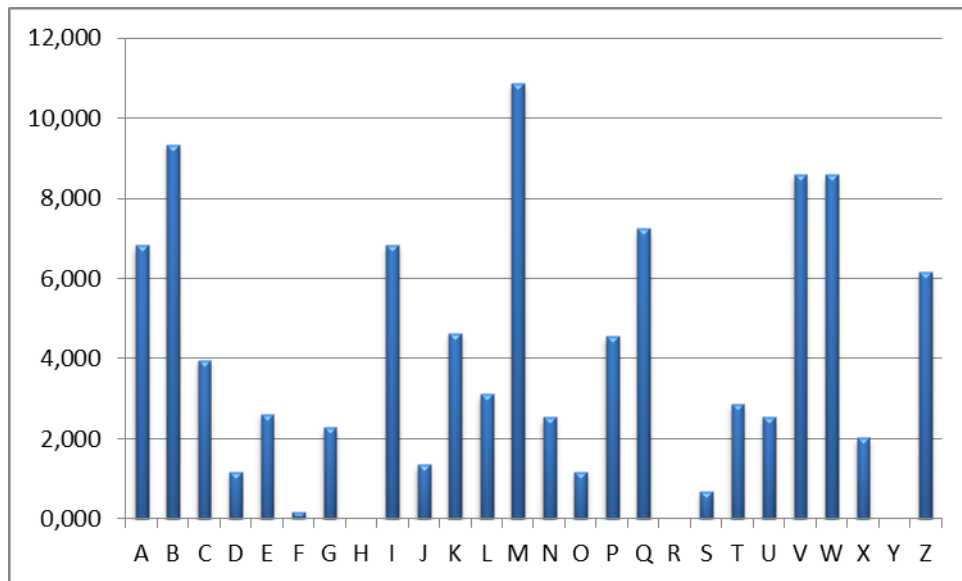
Obrázek 12: Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X_5$



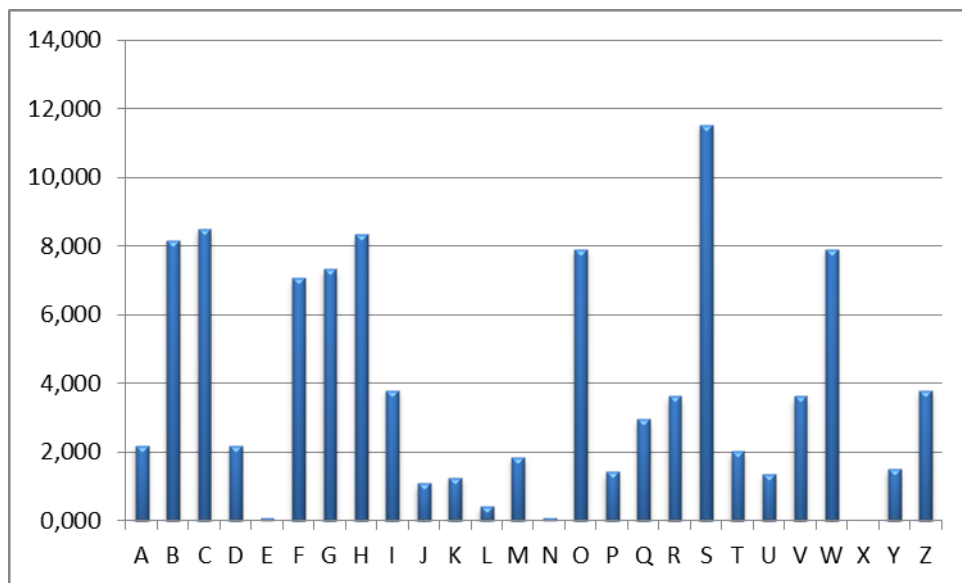
Obrázek 13: Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X_6$



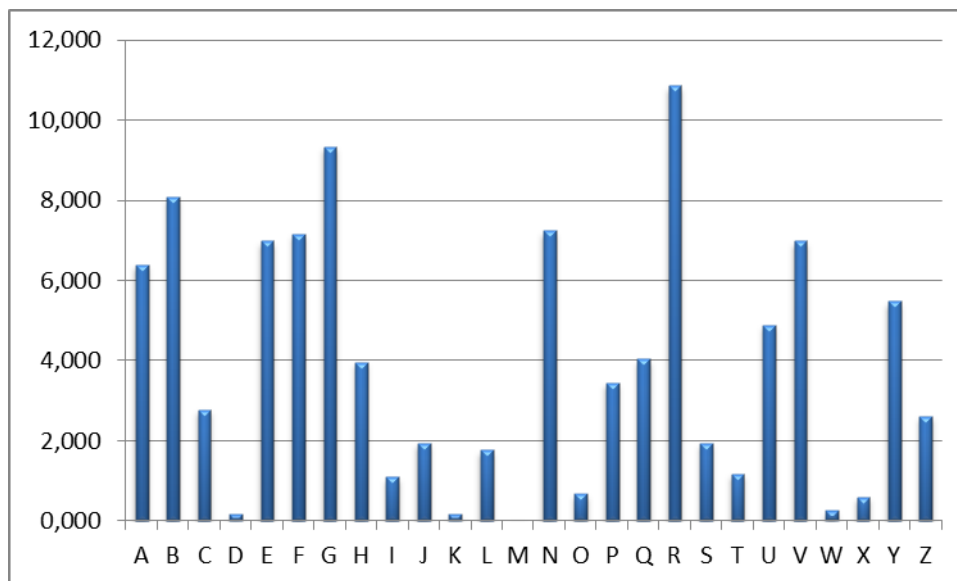
Obrázek 14: Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X_7$



Obrázek 15: Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X_8$



Obrázek 16: Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X_9$



Obrázek 17: Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X_{10}$

Pokud se zbývající grafy Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem  $X$  (Obrázek 11 - 17) srovnají s grafem Četnost výskytu jednotlivých znaků v anglickém jazyce, lze snadno zjistit zbývající hodnoty písmen  $X_4$  až  $X_{10}$ . Po srovnání tedy vyšla jednotlivá písmena  $X$  definující posuv v abecedě takto:

$X_4$  se posune o 17 znaků,  $X_5$  se posune o 24 znaků,  $X_6$  o 15 znaků,  $X_7$  o 19 znaků,  $X_8$  o 8 znaků,  $X_9$  o 14,  $X_{10}$  opět o 13 znaků.

Potom tedy platí, že  $X_4=R$ ,  $X_5=Y$ ,  $X_6=P$ ,  $X_7=T$ ,  $X_8=I$ ,  $X_9=O$ ,  $X_{10}=N$ . Po spojení všech písmen  $X$  tedy vychází celý klíč jako anglické slovo *ENCRYPTION*, což odpovídá klíči, který byl použit k šifrování otevřeného textu.

U těchto dvou příkladů bylo názorně vidět, že frekvenční analýza se hodí především pro jednoduché monoalfabetické substituční šifry. Kryptoanalýza pomocí pokročilé frekvenční analýzy vyžaduje velké množství výpočtů, které není člověk bez využití výpočetní techniky schopen v potřebném čase zpracovat.

### 2.1.3 Frekvenční analýza v programu Mathematica

Tato kapitola prakticky zpracovává frekvenční analýzu v programu Wolfram Mathematica. Frekvenční analýza je prováděna na textu šifrovaném Caesarovou šifrou uvedeném v Příloze PII.

```

In[1]:= Abeceda = {"A", "B", "C", "D", "E", "F", "G", "H", "I", "J", "K", "L", "M", "N", "O", "P", "Q",
  "R", "S", "T", "U", "V", "W", "X", "Y", "Z"};
LetterCountList = {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0};
SifrovýText = Import["C:\Documents and Settings\Standa\Desktop\Text.txt"];
SifrovýTextList = StringSplit[SifrovýText, ""];
For [i = 1, i ≤ Length[SifrovýTextList], i++, pos = Position[Abeceda, SifrovýTextList[[i]]];
  LetterCountList[[pos][[1]][[1]]] += 1]
LetterFreqList = LetterCountList;
FreqAnalysisList = LetterCountList;
For [i = 1, i ≤ 26, i++,
  LetterFreqList[[i]] = LetterCountList[[i]] * 100 / Length[SifrovýTextList];
  FreqAnalysisList[[i]] = StringJoin[ToString[Abeceda[[i]]], " = ", ToString[N[LetterFreqList[[i]], 3]],
    " %", "\n"]
]
N[LetterFreqList]
FreqAnalysisList

```

Obrázek 18: Výpočet frekvenční analýzy v programu Mathematica

Následující obrázek (Obrázek 19) obsahuje četnost výskytu znaků šifrového textu z Přílohy PII.

```

Out[2]= {A = 0.337 %
, B = 2.03 %
, C = 0.0673 %
, D = 7.61 %
, E = 1.30 %
, F = 3.47 %
, G = 3.46 %
, H = 11.3 %
, I = 2.08 %
, J = 1.42 %
, K = 3.84 %
, L = 7.36 %
, M = 0.135 %
, N = 0.909 %
, O = 4.16 %
, P = 2.66 %
, Q = 7.04 %
, R = 8.83 %
, S = 2.58 %
, T = 0.0841 %
, U = 6.58 %
, V = 7.59 %
, W = 9.05 %
, X = 3.28 %
, Y = 0.883 %
, Z = 1.92 %
}

```

Obrázek 19: Četnost znaků šifrového textu provedeném v programu Mathematica

## 2.2 Koeficient koincidence

Dalším způsobem luštění šifrového textu je metoda koeficientu (indexu) koincidence, pomocí které lze zjistit rozdíl mezi distribucí jednotlivých znaků šifrového textu a distribucí rovnoměrnou. Tento způsob luštění se využívá především jako doplněk u frekvenční analýzy. Při použití polyalfabetické substituční šifry se vypočítají hodnoty koeficientu koincidence, které jsou charakterizovány pro určitý jazyk, a počet použitých monoalfabetických substitucí. S rostoucím počtem monoalfabetických substitucí klesá koeficient koincidence na hodnotu  $1/n$ , kde  $n$  určuje počet znaků v dané abecedě [11].

Při realizaci výpočtu této metody se nejprve zvolí označení abecedy, v praxi označováno velkým písmenem  $A$ , v tomto případě se pro přehlednost ve výpočtech zvolí malé řecké písmeno  $\alpha$ . Následně se vypočítá pravděpodobnost výskytu určitého znaku v přímém textu (též nazývaná jako relativní frekvence), kdy se celkový počet výskytů určitého znaku podělí celkovým počtem všech znaků v textu. Relativní frekvence daného znaku se označuje  $p(\lambda)$ , šifrovaný text písmenem  $C$ . Výpočet relativní frekvence např. znaku  $A$  v mezinárodní abecedě, která obsahuje 26 znaků, vypadá následovně:

$$p(\lambda) = \frac{1}{26^2} + \frac{1}{26^2} + \frac{1}{26^2} + \dots + \frac{1}{26^2} = 26 \cdot \frac{1}{26^2} = \frac{1}{26},$$

$$p(\lambda) = \frac{1}{26} = 0,038461538. \quad (1)$$

Pokud se tento vzorec aplikuje např. na písmeno  $R$  z otevřeného textu uvedeného v příloze PI, lze vypočítat pravděpodobnost výskytu písmene  $R$  na určitém místě v textu:

$$p(\lambda) = \frac{782}{11881} = 0,065819.$$

S pomocí těchto základů, tedy relativní frekvence, lze vytvořit vzorec pro výpočet pravděpodobnosti výskytu náhodně zvoleného znaku abecedy na určitém místě v textu.

$$k = \sum_{i \in \alpha} \left( p_i - \frac{1}{26} \right).$$

Tento vzorec ovšem nelze použít pro monoalfabetickou šifru, jelikož po dosazení vyjde  $k=0$ , tzn. jedná se o dokonalou polyalfabetickou šifru. Výsledek výpočtu  $k$  po dosažení příslušných hodnot je uveden níže:

$$\sum_{i=1}^n p_i = \sum_{i=1}^{26} p_i = (0,07609 + 0,01296 + 0,03476 + 0,03459 + 0,11312 + 0,02079 + 0,01422 + 0,03838 + 0,07365 + 0,00135 + 0,00909 + 0,04166 + 0,02660 + 0,07045 + 0,08812 + 0,02584 + 0,084 + 0,06582 + 0,07592 + 0,09056 + 0,03283 + 0,00884 + 0,01919 + 0,00337 + 0,02028 + 0,0067),$$

$$p_i = 1,08918.$$

Pro ověření správnosti výpočtu s dosaženými četnostmi výskytu jednotlivých jazyků v angličtině byl výsledek ověřen v programu Mathematica.

```
In[1]:= p = {0.07609, 0.01296, 0.03476, 0.03459, 0.11312, 0.02079,
0.01422, 0.03838, 0.07365, 0.00135, 0.00909, 0.04166, 0.02660,
0.07045, 0.08812, 0.02584, 0.084, 0.06582, 0.07592, 0.09056,
0.03283, 0.00884, 0.01919, 0.00337, 0.02028, 0.0067}

k = Sum[p[[i]], {i, 1, 26}]

Out[1]= 1.08918
```

Obrázek 20: Výpočet pravděpodobnosti v programu Mathematica

Dokončení výpočtu pravděpodobnosti po dosažení zaokrouhlených hodnot:

$$k = 1 - 26 \cdot \frac{1}{26} = 1 - 1 = 0.$$

Z toho vyplývá, že vzorec musí být upraven tak, aby odpovídal i rovnoměrnému rozložení znaků v textu, jinak řečeno musí se obsah závorky umocnit na druhou. Pak tedy matematický zápis bude vypadat následovně:

$$k = \sum_{i \in \alpha} \left( p_i - \frac{1}{26} \right)^2 = \sum_{i \in \alpha} \left( p_i^2 - 2 \cdot \frac{1}{26} \cdot p_i + \left( \frac{1}{26} \right)^2 \right) = \sum_{i \in \alpha} p_i^2 - \frac{2}{26} \cdot \sum_{i \in \alpha} p_i + \sum_{i \in \alpha} \left( \frac{1}{26} \right)^2,$$

$$k = \sum_{i \in \alpha} p_i^2 - \frac{2}{26} + \frac{1}{26}.$$

Výsledný vzorec pro výpočet součtu kvadratických odchylek skutečných pravděpodobností výskytu znaků bude vypadat takto:

$$k = \sum_{i=1}^n p_i^2 - \frac{1}{26},$$

kde  $p_i^2$  značí pravděpodobnost výskytu náhodného znaku abecedy  $\alpha$  na určitém místě v otevřeném textu.

$$k = \sum_{i=1}^n p_i^2 - \frac{1}{26} = \sum_{i=1}^{26} p_i^2 - \frac{1}{26} = (0,07609^2 + 0,01296^2 + 0,03476^2 + 0,03459^2 + 0,11312^2 + 0,02079^2 + 0,01422^2 + 0,03838^2 + 0,07365^2 + 0,00135^2 + 0,00909^2 + 0,04166^2 + 0,02660^2 + 0,07045^2 + 0,08812^2 + 0,02584^2 + 0,084^2 + 0,06582^2 + 0,07592^2 + 0,09056^2 + 0,03283^2 + 0,00884^2 + 0,01919^2 + 0,00337^2 + 0,02028^2 + 0,0067^2) - \frac{1}{26},$$

$$k = 0,0334973.$$

Z toho plyne, že pravděpodobnost výskytu náhodně zvoleného znaku z otevřeného textu (Příloha PI) je 0,00335.

V programu Wolfram Mathematica bylo provedeno ověření správnosti předešlého výpočtu.

```
In[1]:= p = {0.07609, 0.01296, 0.03476, 0.03459, 0.11312, 0.02079,
           0.01422, 0.03838, 0.07365, 0.00135, 0.00909, 0.04166, 0.02660,
           0.07045, 0.08812, 0.02584, 0.084, 0.06582, 0.07592, 0.09056,
           0.03283, 0.00884, 0.01919, 0.00337, 0.02028, 0.0067}

k = Sum(p[[i]]^2, {i, 1, 26}) - (1/26)

Out[1]= 0.0334973
```

Obrázek 21: Výpočet  $k$  pomocí programu Mathematica

Při zjišťování koeficientu koincidence pro šifrovaný text se využívá stávajících znalostí. Nejprve se zjistí, kolikrát se znak  $\lambda$  objevuje v textu  $C$ , to se značí  $\lambda_i$ . Z těchto hodnot  $\lambda_i$  se vychází při zjišťování celkového počtu dvojic nacházejících se v textu  $C$  a označuje se velkým písmenem  $A$ . Výpočet vypadá následovně:

$$A = \frac{1}{2} \cdot \lambda_i \cdot (\lambda_i - 1).$$

Celkový počet všech znaků v textu  $C$  se označuje  $R$ . Z toho vyplývá, že výpočet všech dvojic nacházejících se v textu  $C$ , označující se velkým písmenem  $B$ , vypadá takto:

$$B = \frac{1}{2} \cdot R \cdot (R - 1).$$

Ze vzorců  $A$  a  $B$  se vychází při zjišťování indexu koincidence.

$$I(C) = \frac{A}{B} = \frac{\frac{1}{2} \cdot \lambda_i \cdot (\lambda_i - 1)}{\frac{1}{2} \cdot R \cdot (R - 1)}.$$

Pro zjištění výsledného vzorce pro výpočet indexu koincidence  $I(C)$  je nutné upravit čítelek  $A$  tak, aby došlo k součtu všech znaků v použité abecedě, tzn.  $\lambda_i$  bude zastupovat postupně počet znaků  $a$  až  $z$ . Potom tedy výsledný výpočet koeficientu koincidence bude:

$$I(C) = \frac{\frac{1}{2} \cdot \sum_{i=1}^n \lambda_i \cdot (\lambda_i - 1)}{\frac{1}{2} \cdot R \cdot (R - 1)} = \sum_{i=1}^n \frac{\lambda_i \cdot (\lambda_i - 1)}{R \cdot (R - 1)},$$

kde  $n$  označuje počet znaků abecedy v šifrovém textu, v mezinárodní abecedě je  $n=26$ , tzn.  $i \in \{1, 2, \dots, 26\}$ . Koeficient koincidence má přibližně stejnou hodnotu jako  $\sum_{i \in \alpha} p_i^2$ .

Při zjišťování hodnoty  $I(C)$  se dosadí hodnoty z šifrového textu zašifrovaného pomocí Vigenèrovy šifry uvedeného v Příloze PIII a následně se po krocích vypočítá. Výpočet hodnoty  $I(C)$  je uveden z důvodu názornosti po jednotlivých krocích.

$$A = \frac{1}{2} \cdot \sum_{i=1}^{26} \lambda_i \cdot (\lambda_i - 1) = 2952011,$$

$$B = \frac{1}{2} \cdot R \cdot (R - 1) = \frac{1}{2} \cdot 11881 \cdot (11881 - 1) = 70573140,$$

$$I(C) = \frac{A}{B} = \frac{2952011}{70573140} = 0,0418.$$

Na následujícím obrázku je vidět výpočet  $I(C)$  v programu Wolfram Mathematica.

```
In[1]:= λ = {437, 595, 618, 211, 483, 489, 772, 461, 516, 346, 376, 353,
          499, 370, 195, 506, 495, 707, 406, 479, 324, 692, 451, 402, 353, 345}
R = 11881
A =  $\frac{\sum_{i=1}^{26} \lambda[[i]] \times (\lambda[[i]] - 1)}{2}$ 
B =  $\frac{R \times (R - 1)}{2}$ 
k =  $\frac{A}{B}$  // N

Out[1]= 2952011
Out[2]= 70573140
Out[3]= 0.0418291
```

Obrázek 22: Výpočet indexu koincidence v programu Mathematica

Výsledek vypočtený ze vzorce  $I(C)$  přesně neodpovídá žádné abecedě, jak je vidět z následující tabulky. Je to způsobeno tím, že vybraný text není dostatečně dlouhý. Nejvíce se přibližuje náhodné hodnotě vypočtené podle vztahu (1), což by pro zvolený text odpovídalo.

Jazyk	Index koincidence
Angličtina	0,066895
Francouzština	0,074604
Němčina	0,076667
Ruština	0,056074
Slovenština	0,06027
Čeština	0,058258

Tabulka 8: *Koeficient koincidence pro národní abecedy*

Hodnoty uvedené v tabulkách se mohou v některých případech lišit, záleží na frekvenci jednotlivých znaků.

Hodnoty uvedené v tabulce (Tabulka 8) jsou počítány následujícím způsobem. Nejprve se určí četnost znaků ve zvolené abecedě (označeno malým  $c$ ), ta se určuje na základě výpočtů rozsáhlých textů. I v takových případech se mohou četnosti lišit. V tomto případě se zvolily neoficiální četnosti anglického jazyka ze zdroje [10]. Z toho důvodu nemusí vycházet hodnoty naprosto shodně s hodnotami v tabulce.

$$c = \sum_{i=1}^n p_i^2 = \sum_{i=1}^{26} p_i^2 = (0,08167^2 + 0,01492^2 + 0,02782^2 + 0,04253^2 + 0,12702^2 + 0,02228^2 + 0,02015^2 + 0,06094^2 + 0,06966^2 + 0,00153^2 + 0,00772^2 + 0,04025^2 + 0,02406^2 + 0,06749^2 + 0,07507^2 + 0,01929^2 + 0,00095^2 + 0,05987^2 + 0,06327^2 + 0,09056^2 + 0,02758^2 + 0,00978^2 + 0,02360^2 + 0,00150^2 + 0,01974^2 + 0,00074^2),$$

$$c = 0,0655.$$

Hodnota 0,0655 se blíží hodnotě uvedené v tabulce (Tabulka 8) pro anglický jazyk. Ověření správnosti výpočtu je možné ověřit v programu Mathematica.

```

In[1]:= p = {0.08167, 0.01492, 0.02782, 0.04253, 0.12702, 0.02228,
0.02015, 0.06094, 0.06966, 0.00153, 0.00772, 0.04025, 0.02406,
0.06749, 0.07507, 0.01929, 0.00095, 0.05987, 0.06327, 0.09056,
0.02758, 0.00978, 0.02360, 0.00150, 0.01974, 0.00074}

k = Sum[p[[i]]^2, {i, 1, 26}]

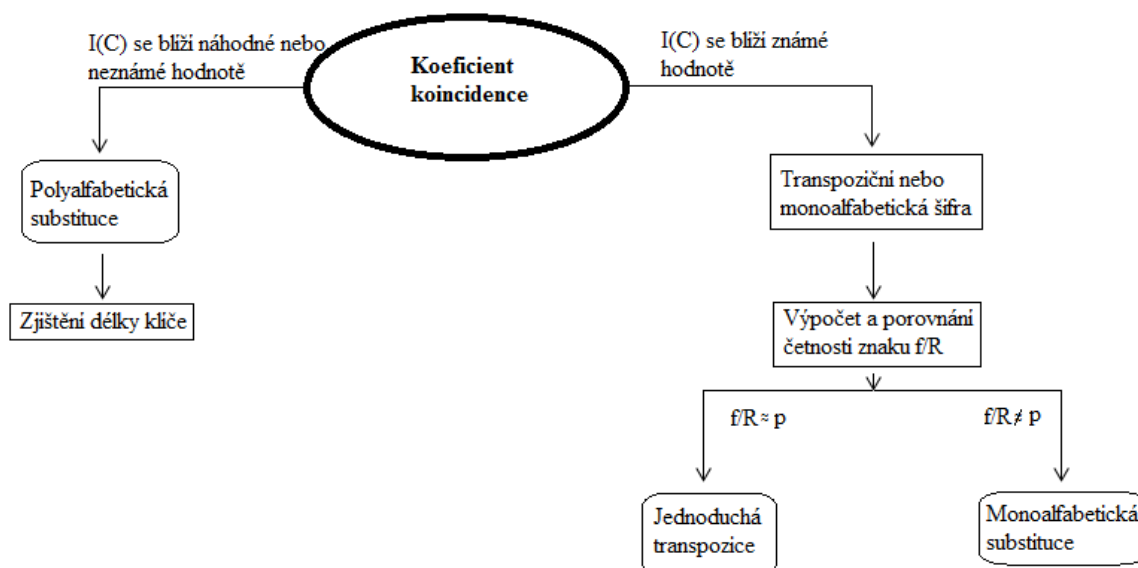
Out[1]:= 0.0654967

```

Obrázek 23: Výpočet četnosti v programu Mathematica

### 2.2.1 Využití koeficientu koincidence

V případě, že kryptoanalytik dostane do rukou zašifrovaný text neznámou šifrou, použije postup, který je uveden na Obrázku 24.



Obrázek 24: Využití koeficientu koincidence

Nejprve si vypočítá koeficient koincidence a ten porovnává s tabulkou známých abeced (Tabulka 8). V případě, že hodnota odpovídá nebo je přibližně stejná jako některá hodnota v tabulce, jedná se zpravidla o text zašifrovaný pomocí jednoduché transpozice nebo monoalfabetické substituce. Dále se postupuje porovnáním četností jednotlivých znaků s pravděpodobností výskytu určitého znaku v daném jazyce. Podle výsledků se rozhoduje, zda se jedná o transpozici nebo o monoalfabetickou šifru. Jestliže  $I(C)$  odpovídá náhodné hodnotě nebo neznámé hodnotě, pak jde o polyalfabetickou šifru, u jejíhož luštění je nutné nejprve zjistit klíč. Index koincidence závisí na délce šifrovaného textu; čím delší je text, tím se  $I(C)$  více mění.

Délku klíče lze odvodit za pomoci hrubého odhadu hodnoty  $I(C)$ . Tento odhad se označí malým písmenem  $e$ .

$$e = \left( \left( \frac{S-t}{t \cdot (S-1)} \right) \cdot k \right) + \left( \left( \frac{S \cdot (t-1)}{t \cdot (S-1)} \right) \cdot P \right),$$

kde  $S$  je délka šifrového textu,  $t$  označuje délku klíče, za  $k$  se dosadí hodnoty z Tabulky 8 pro určitou abecedu (v tomto případě anglickou) a  $P$  představuje hodnotu  $p(\lambda)$  pro mezinárodní abecedu, tedy 0,0385. Délka klíče se zadává od 1 do hodnoty, pro kterou se najde vhodný výsledek odpovídající hodnotě  $I(C)$  šifrového textu. V případě, že  $I(C)$  je blízké  $e$ , bude délka klíče rovna číslu dosazenému za  $t$ . Podobnost  $e$  s  $I(C)$  může nastat při více volbách klíče, stejně tak to vychází i u následujícího příkladu, kdy se použil šifrový text zašifrovaný polyalfabetickou Vigenèrovou šifrou uvedený v Příloze PIII. V tomto případě se  $e$  podobalo indexu koincidence ve třech případech, a to pro  $t=8$ ,  $t=9$  a  $t=10$ . Z toho by se dalo alespoň usoudit, že klíč musí mít délku minimálně 8 znaků.

$$e = \left( \left( \frac{11881-8}{8 \cdot (11881-1)} \right) \cdot 0,066895 \right) + \left( \left( \frac{11881 \cdot (8-1)}{8 \cdot (11881-1)} \right) \cdot 0,038 \right) = 0,0417,$$

$$e = \left( \left( \frac{11881-9}{9 \cdot (11881-1)} \right) \cdot 0,066895 \right) + \left( \left( \frac{11881 \cdot (9-1)}{9 \cdot (11881-1)} \right) \cdot 0,038 \right) = 0,0413,$$

$$e = \left( \left( \frac{11881-10}{10 \cdot (11881-1)} \right) \cdot 0,066895 \right) + \left( \left( \frac{11881 \cdot (10-1)}{10 \cdot (11881-1)} \right) \cdot 0,038 \right) = 0,0411.$$

Pro výpočet odhadu délky klíče se zvolil program Wolfram Mathematica, vzhledem k velkému množství možností délky klíče by bylo nevhodné provádět výpočet ručně. Teoreticky se uvažuje o délce klíče do 50 znaků, delší klíč se u této šifry většinou kvůli délce nepoužívá.

```
In[1]:= For[t = 1, t ≤ 10, t++; k = 0.066895; S = 11 881; P = 0.0385;  
Print[e = ((S - t) / (t * (S - 1))) * k + ((S * (t - 1)) / (t * (S - 1))) * P]]  
  
0.0526963  
0.0479634  
0.045597  
0.0441771  
0.0432305  
0.0425544  
0.0420473  
0.0416529  
0.0413373  
0.0410792
```

Obrázek 25: Využití koeficientu koincidence  $s \in \langle 1,10 \rangle$

Obrázek 25 názorně ukazuje, jak vycházejí hodnoty  $e$  pro jednotlivá  $t$ . Hodnoty se mohou z důvodů zaokrouhlování lišit od skutečných hodnot, rozdíl je ovšem v řádech desetitisícin.

### 3 ROZBOR ALGORITMU RSA

Teoretické informace o algoritmu RSA jsou uvedeny v Kapitole 1.2.4.1. Informace pro vypracování této části bakalářské práce byly použity z literatury [3], není-li uvedeno jinak.

#### 3.1 Tvorba klíčů

U této části se vychází ze znalosti asymetrického šifrového systému, popsaného v Kapitole 1.1, kdy jsou zapotřebí dva klíče, a to soukromý a veřejný. Základní vlastností klíče, stejně jako v jiných případech šifrování, je nepředvídatelnost, která zvyšuje bezpečnost hesla. Při tvorbě klíčů se nejprve zvolí dvě náhodná dostatečně velká prvočísla, označovaná  $p$  a  $q$ . Minimální velikost je většinou definována. Zda se jedná o prvočísla, se testuje např. R-M testem nebo Lehmanovým testem, popsanými v Kapitole 1.1.

$$n = p \cdot q, \quad (2)$$

$$m = (p - 1) \cdot (q - 1). \quad (3)$$

V dalším kroku se zvolí číslo  $r$  takové, že  $1 < r < m$  a  $r, m$  jsou nesoudělná, tj.  $D(r, m) = 1$ , kde  $D$  znamená největšího společného dělitele čísel  $r, m$ .

V následném kroku se využije znalostí Euklidova algoritmu, popsaného v Kapitole 1.1, kterým se jednoznačně určí číslo  $S$  takové, že:

$$1 < S < m,$$

$$r \cdot S \equiv 1 \pmod{m}.$$

Veřejný klíč v takovém případě má tvar  $(n, r)$ , soukromý je pak složen z čísel  $(n, S)$ . V tomto případě je  $n$  veřejné číslo, které se používá i u soukromého klíče. Z důvodů bezpečnosti není třeba se obávat zveřejnění  $n$ , jelikož nejsou veřejně známy hodnoty  $p$  a  $q$ . V současné době faktorizaci čísla  $n$  nelze provést v rozumném čase, což zajišťuje naprostou bezpečnost RSA algoritmu. Pokud by šlo provést faktorizaci v rozumném čase, tak by bylo možné provést pomocí Euklidova algoritmu výpočet soukromého klíče. Počet prvočísel lze zjistit podle zjednodušeného Gaussova vztahu [3]:

$$\pi(n) = \frac{n}{\ln n}.$$

Počet prvočísel závisí na intervalu, z kterého se prvočísla vybírají. Pokud počet prvočísel vyjde např. 100, je zhruba o 3 řády nižší než celkový počet prvočísel [3].

$$\pi(10^{100}) - \pi(10^{99}) = 3,9 \cdot 10^{97}.$$

Při tvorbě klíče se využívá generátor náhodných čísel, kterým se vyhledají náhodná stomístná prvočísla. Jestliže vyjde sudé číslo, je k němu automaticky přičtena jednička a testuje se, zda je číslo prvočíslo, pokud ne, pak je k náhodnému číslu přičtena dvojka a test probíhá odznovu. K testování se využívá Lehmanův test, R-M test (Kapitola 1.1) nebo jiné [3].

Nyní se provede praktická tvorba klíče podle výše uvedeného postupu. Odesílatel si zvolí za  $p$  a  $q$  hodnoty prvočísel 11 a 13, z nichž vypočítá hodnotu  $n$  podle výše uvedeného vzorce (2):

$$n = p \cdot q = 11 \cdot 13 = 143.$$

Z hodnot  $p$  a  $q$  se dále zjistí hodnota  $m$ , dle (3):

$$m = (p - 1) \cdot (q - 1) = (11 - 1) \cdot (13 - 1) = 120.$$

Nyní se zvolí číslo  $r$  podle stanovených podmínek, v tomto případě  $r=17$ . Při znalosti všech volitelných hodnot lze vypočítat hodnotu  $S$ :

$$\begin{aligned} r \cdot S &\equiv 1 \pmod{m}, \\ 17 \cdot S &\equiv 1 \pmod{120}. \end{aligned}$$

K vypočtení hodnoty  $S$  nestačí znalost obyčejného Euklidova algoritmu, ale je třeba využít jeho rozšířenou verzi, ke spočítání multiplikativní inverze. Je-li multiplikativní inverze k číslu 17 v  $\mathbb{Z}_{120}$ , pak výpočet čísla  $S$  bude vypadat následovně:

Vytvoří se rovnice pro čísla 120 a 17.

$$\begin{aligned} 120 &= 7 \cdot 17 + 1, \\ 17 &= 1 \cdot 17 + 0. \end{aligned}$$

Tyto rovnice lze napsat i jiným způsobem, a to pro zbytky po dělení.

$$1 = 1 \cdot 120 - 7 \cdot 17,$$

Tato rovnice je stejná jako rovnice  $1 = x \cdot a + y \cdot b$ . Z toho plyne, že  $x = 1$  a  $y = -7$ , tzn. že inverzí v  $\mathbb{Z}_{120}$  je číslo  $-7$ . Inverze k číslu  $17$  v  $\mathbb{Z}_{120}$  se vypočítá jako součet čísel  $-7$  a  $120$ , tj.

$$-7 + 120 = 113.$$

Inverze k číslu  $17$  v  $\mathbb{Z}_{120}$  tedy je číslo  $113$ , z toho plyne, že  $S = 113$ .

Jako důkaz správnosti se číslo  $113$  vloží do rovnice pro výpočet  $S$ :

$$\begin{aligned} r \cdot S &\equiv 1 \pmod{m}, \\ 17 \cdot 113 &\equiv 1 \pmod{120}, \\ 1921 &\equiv 1 \pmod{120}. \end{aligned}$$

Pokud se poslední řádek upraví na  $a = b + k \cdot n$  (Kapitola 1.1), pak výpočet bude pokračovat následovně:

$$\begin{aligned} 1921 &= 1 + 16 \cdot 120, \\ 1921 &= 1921. \end{aligned}$$

Levá strana rovnice je stejná jako strana pravá, z čehož plyne, že  $S = 113$  opravdu platí. Tímto postupem se stanovil veřejný klíč jako dvojice čísel  $(143, 17)$  a soukromý jako  $(143, 113)$ .

Z názorné ukázky vyplývá, že bezpečný klíč musí splňovat tato dvě kritéria:

- 1 Při rozkladu  $(p-1)$  a  $(q-1)$  musí minimálně jedna z hodnot  $p$  nebo  $q$  obsahovat velké prvočíslo.
- 2 Podíl  $p = \frac{p}{q}$  se nesmí blížit žádnému jednoduchému zlomku, jako je např.  $\frac{1}{2}, \frac{1}{3}, \frac{3}{8}$ .

### 3.2 Postup při šifrování a dešifrování

Prvním krokem při šifrování zprávy RSA algoritmem je převedení otevřeného textu na čísla, např. ASCII. Převedený text se rozdělí na bloky o určité délce  $d$ , pro kterou musí za předpokladu znalosti veřejného a soukromého klíče platit  $1 \leq d \leq m$ . V dalším kroku se musí zvolit šifrovací exponent  $x$ , který musí být nesoudělný s  $m$ , popsáno v části Tvorba klíče (Kapitola 3.1). V praxi se kvůli zkrácení šifrovací doby nejčastěji používá  $x=3$  nebo  $x=7$ , to ovšem znatelně prodlužuje čas potřebný k dešifrování šifrovaného textu. Uživatel, který šifruje a odesílá šifrovanou zprávu šifrovanou RSA algoritmem, zveřejní hodnoty  $m$  a

$x$ . V další kroku šifrování se určí ze vzorce  $t \cdot x \equiv 1 \pmod{(p-1) \cdot (q-1)}$  hodnota  $t$ , která vyhovuje kongruenci  $y \equiv d^x \pmod{m}$ . Šifrování se provádí podle vztahu

$$c \equiv o^r \pmod{m},$$

kde  $o$  představuje hodnotu otevřeného textu a musí platit, že  $0 \leq o \leq m-1$ ,  $c$  je šifrovaný text a  $r$  je náhodná hodnota používaná při výpočtu klíče (Kapitola 3.1). Dešifrování probíhá obdobným způsobem, kdy se místo  $r$  použije hodnota  $S$  (Kapitola 3.1) a dojde k vzájemné výměně znaků  $o$  a  $c$ . Vztah bude tedy vypadat takto:

$$o \equiv c^S \pmod{m}.$$

Pro názornost se využije příkladu se stanoveným klíčem, vypočítaného v Kapitole 3.1. Odesílatel použije veřejný klíč příjemce, což je  $(143,17)$ , a pro jednoduchost zašifruje jen číslo 53, tzn.  $o=53$ . Odesílatel tedy zašifruje otevřený text takto:

$$\begin{aligned} c &\equiv 53^{17} \pmod{143}, \\ c &\equiv 92. \end{aligned}$$

Číslo 53 bude tedy mít v šifrované podobě hodnotu 92. Tento šifrový znak pošle odesílatel příjemci, který jej rozšifruje pomocí svého soukromého klíče  $(143,113)$  následovně:

$$\begin{aligned} o &\equiv 92^{113} \pmod{143}, \\ o &= 53. \end{aligned}$$

Otevřený text odesílatele se shoduje s otevřeným textem příjemce, tzn. šifrování RSA algoritmem proběhlo úspěšně. Stejným způsobem by se šifrovalo i více znaků, jedná se ovšem o náročnější operace [3].

### 3.3 Útoky na RSA algoritmus

Informace o dané problematice byly čerpány z literatury [3], pokud není uvedeno jinak. Jak již bylo zmíněno v předešlých kapitolách o algoritmu RSA, je prolomení velice náročné z důvodu nesnadné faktorizace čísel, proto je v RSA v dnešní době považována za jednu z nejbezpečnějších šifer. I přesto ovšem existuje několik způsobů, jak RSA prolomit. V následující části budou uvedeny některé z nich.

### 3.3.1 Útok se znalostí šifrovaného textu

Při komunikaci příjemce s odesílatelem zachytí kryptoanalytik šifrovanou zprávu  $c$ . Pokud chce zjistit obsah šifrované zprávy, pak musí zjistit otevřený text  $o$ . Kryptoanalytik má k dispozici znalost veřejného klíče. V dalším kroku zvolí náhodné číslo  $e$ , pro které musí platit  $e < m$ . Se znalostí základních informací lze vypočítat hodnoty  $x$ ,  $y$ ,  $z$ :

$$\begin{aligned}x &= e^r \bmod m, \\y &= x \cdot c \bmod m, \\z &= e^{-1} \bmod m.\end{aligned}$$

Vztah  $x = e^r \bmod m$  lze také zapsat jako  $e = x^s \bmod m$ . Pokud se  $e = x^d \bmod m$  nechá podepsat soukromým klíčem  $y$ , pak vyjde:

$$v = y^s \bmod m.$$

V dalším kroku pro zjištění otevřeného textu  $o$  se vynásobí hodnoty  $v$  a  $z$ :

$$o = z \cdot v = e^{-1} \cdot y^s \bmod m.$$

Za  $y$  se dosadí  $y = x \cdot c \bmod m$  a rovnice se upraví takto:

$$o = e^{-1} \cdot x^s \cdot c^s \bmod m.$$

Následně se za  $x$  dosadí  $x = e^r \bmod m$ , tím dojde k vyrušení indexů  $r$  a  $S$ , protože vynásobením dají číslo 1.

$$o = e^{-1} \cdot e \cdot c^s \bmod m.$$

V posledním kroku se vztah  $o$  upraví do konečné podoby:

$$o = c^s \bmod m.$$

Analytik sice nezná soukromý klíč, ale přesto si může zprávu přečíst, jelikož při podpisu může dojít k dešifrování zprávy pokud je vhodně konstruovaná.

U útoku se znalostí podepsaného šifrovaného textu je názorně vidět, že volba kryptografického protokolu je velmi důležitá při šifrování, a neměly by se na něj tedy klást nižší nároky než na šifrovací algoritmus. Zamezení možnosti podepisování neznámých zpráv zajistí vyšší důvěryhodnost a integritu dané zprávy.

### 3.3.2 Útok se společným modulem

V některých případech dochází k realizaci algoritmu RSA pro modul  $m$  různými mocniteli  $r$  a  $S$ , tj. např.  $r_1, r_2, r_3$  atd. Takový text se tedy potom šifruje a dešifruje pro každé mocnitele  $r$  a  $S$  zvlášť:

$$\begin{aligned}c_1 &= o^{r_1} \bmod m, \\c_2 &= o^{r_2} \bmod m, \\c_3 &= o^{r_3} \bmod m.\end{aligned}$$

Takto by se pokračovalo dále. Vezmou-li se v úvahu předešlé dva příklady šifrování, a to  $c_1$  a  $c_2$ , potom kryptoanalytik má k dispozici dva různé  $c$  a  $r$  a jedno společné  $m$ . Jelikož  $c_1$  a  $c_2$  mají jen jednoho společného dělitele, a to konkrétně číslo jedna, pak je kryptoanalytik schopen pomocí rozšířeného Euklidova algoritmu najít takové  $\kappa$  a  $\mu$ , tak aby platilo  $\kappa \cdot r_1 + \mu \cdot r_2 = 1$  při  $\kappa < 0$ . Z toho lze spočítat otevřený text  $o$ :

$$o = (c_1^{-1})^{-\kappa} \cdot c_2^\mu = (a^{\kappa r_1} \bmod m) \cdot (a^{\mu r_2} \bmod m) = a^{\kappa r_1 + \mu r_2} \bmod m = a \bmod m.$$

### 3.3.3 Podpis podvrženého dokumentu

Tento způsob se zaměřuje na podepisování neověřených dokumentů. Jsou dva způsoby, jak v takovém případě postupovat.

#### Způsob první

Prvním krokem je označení znevážené zprávy a zprávy bez závad. Protože se vychází z druhé jmenované, označí se tato zpráva písmenem  $a$  a znevážená zpráva velkým písmenem  $A$ . Pokud chce osoba komunikující s příjemcem (nemusí to být odesílatel ale i útočník), podepsat zprávu, musí nejprve zvolit náhodnou hodnotu  $x$ , z níž vypočítá  $y = x^r \bmod m$ . Znalost  $y$  využije k výpočtu  $a = y \cdot A \bmod m$  a hodnotu  $a$  odešle k podpisu, z čehož se pak vypočte  $a^S \bmod m$ . Využitím všech dosavadních informací se vypočte podepsaná zpráva  $A$ :

$$A = ((a^S \cdot \bmod m) \cdot x^{-1} \bmod m) = ((y^S \cdot A^S \bmod m) \cdot x^{-1} \bmod m) = (x \cdot x^{-1} \cdot A^S) \bmod m.$$

#### Způsob druhý

Opět se v prvním kroku označí znevážená zpráva a obyčejná zpráva. Označení zůstane stejné jako v předešlém případě. Princip tohoto způsobu podepisování je v náhodném

zvolení dvou zpráv  $a_1$  a  $a_2$ , pro které musí platit  $A = (a_1 \cdot a_2) \bmod m$ . Obě zprávy  $a_1$  a  $a_2$  se pošlou k podpisu a následně se zjistí  $A$ :

$$A^s = (a_1^s \bmod m) \cdot a_2^s \bmod m.$$

### 3.3.4 Záměna zpráv

Při chybném postupu dojde k záměně  $a$  za  $A$ . Tedy nejprve odesílatel ( $X$ ) zašifruje text veřejným klíčem stanoveným kryptoanalytikem ( $Z$ ), poté jej digitálně podepíše. Zpráva od odesílatele potom bude mít tvar:

$$(a^{r_Z} \bmod m_Z) \cdot \bmod m_X.$$

Jestliže strana  $Z$  zná faktorizaci čísla  $m_Z$ , pak vypočítá hodnotu  $b$ , pro kterou platí:

$$A^b = a \bmod m_Z.$$

Po výpočtu  $A^b$  zjistí strana  $Z$  hodnotu  $x_{r_Z}$ , zveřejní jí jako nového mocnitele pro svůj veřejný klíč a zveřejní zaslání zprávy  $A$  šifrovanou tímto novým exponentem. Při správném postupu se provede nejprve digitální podpis, a až poté se zašifruje text klíčem strany  $Z$ . Zpráva bude mít tedy tvar:

$$(a^{s_X} \bmod m_X)^{r_Z} \bmod m_Z.$$

## 4 NOVÉ TRENDY

Oblast kryptologie je neustále se vyvíjející odvětví, neboť každá nově vytvořená šifra je vystavena velkému tlaku ze strany kryptoanalytiků, kteří se ji snaží prolomit. Z toho důvodu musí kryptologové vytvářet nové způsoby šifrování, které budou bezpečné a rychlé. Nebo vyvíjejí stávající šifrové systémy, příkladem je DES, po jehož prolomení vzniklo několik nových z DES vycházejících šifer. V současné době lze za nové trendy v kryptologii považovat fraktální kódování, neurofraktální šifrování nebo kvantovou kryptografii, která je mnohými odborníky považována za vrchol kryptografického vývoje. V této kapitole budou uvedeny jen některé z novinek v oblasti kryptologie.

### 4.1 Afinní transformace

Afinní transformace je součástí fraktálního kódování při převodu znaků do číselné podoby. V praxi se rozlišují dva způsoby využití afinní transformace. Informace k této části byly čerpány z [3].

#### 4.1.1 Afinní transformace v $\mathbb{R}$

Jedná se o funkci  $f: \mathbb{R} \rightarrow \mathbb{R}$ .

$$f(x) = a \cdot x + b,$$

pro každé  $x \in \mathbb{R}$ ;  $a, b \in \mathbb{R}$ . Interval  $J = (0,1)$  zobrazí funkci  $f$  na nový interval o délce  $|a|$ , to zapříčiní transformaci funkce  $f$  s měřítkem  $a$ . Bod 0 se přemístí do  $b$  a obraz  $f(J)$  potom bude ležet napravo nebo nalevo od bodu  $b$ , v závislosti na hodnotě  $a$ . Pokud tedy bude  $|a| > 1$ , potom se úsečka protahuje, pokud ale bude  $|a| < 1$ , pak se bude zkracovat. Otočení úsečky kolem počátku závisí na hodnotě  $a$ ; je-li  $a < 0$  pak se osa otočí o  $180^\circ$  a naopak. Celkový posuv závisí na hodnotě  $b$ ; jestliže  $b > 0$  pak se otočí doprava, v opačném případě doleva.

#### 4.1.2 Afinní transformace v $\mathbb{R}^2$

V tomto případě se jedná o dvoudimenzionální transformaci,  $g: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ , která má tvar:

$$g(x, y) = (a \cdot x + b \cdot y + c, d \cdot x + e \cdot y + f),$$

kde  $a, b, c, d, e, f \in \mathbb{R}$ ;  $[x, y] \in \mathbb{R}^2$ . Při výpočtech afinních transformací v  $\mathbb{R}^2$  se využívá matic, potom výpočet vypadá následovně:

$$g \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ d & e \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} c \\ f \end{pmatrix} = F \cdot x + Z,$$

kde  $F$  je deformační matice a  $Z$  translační sloupcový vektor. Matice

$$F = \begin{pmatrix} a & b \\ d & e \end{pmatrix}$$

určuje otočení, zmenšení nebo zkosení, vektor

$$Z = \begin{pmatrix} c \\ f \end{pmatrix}$$

zjišťuje, jak velký je lineární posuv [3].

## 4.2 Fraktální šifrování

Informace v této kapitole jsou čerpány z [3]. Při fraktálním šifrování se využívá výše popsaných afinních transformací (kapitola 4.1), které převedou písmena na čísla. Tato čísla se následně převedou do bitmapy. Při opakovaném postupu se vytvoří fraktální obraz, který přenáší danou zprávu. Při dešifrování fraktální šifry musí příjemce znát počet opakování postupu a afinní transformace použité při šifrování.

## 4.3 Kvantová kryptografie

Kvantová kryptografie je spojena s možností vzniku kvantových počítačů. Zatímco kvantové počítače budou sloužit jako prostředek kryptoanalytiků k prolomení všech možných stávajících šifer, kryptologové už vytvářejí svůj vlastní teoretický způsob, jak zajistit dokonalé zabezpečení pomocí této techniky. Kvantová kryptografie představuje možnost vytvoření neprolomitelné, a tím pádem naprosto bezpečné šifry. Základem kvantové kryptografie je kvantová teorie, která je zároveň podkladem pro kvantové počítače. S tímto nápadem přišel poprvé v 60. letech student Stephen Wiesner, který navrhl koncept kvantových peněz, které nešlo padělat. Návrh kvantových peněz pracuje s fotony a využívá jejich vlastností. Když foton putuje prostorem v určitém směru, má jistý úhel vibrací. Pokud budou stejným směrem putovat dva nebo více fotonů, pak bude jejich úhel vibrací rozdílný, jde o tzv. polarizaci fotonu. Některé fotony mohou vibrovat nahoru a

dolů, jiné zprava doleva a jiné všemi směry. Wiesner se ovšem ve své době i přes tento revoluční nápad nesetkal s pochopením, jediný, koho Wiesnerův nápad nadchl, byl geniální vědec Charles Bennett. Ten Wiesnerův návrh společně s Gillesem Brassardem aplikoval do oblasti kryptografie, kdy společně vytvořili teoreticky návrh kvantové kryptografie. Princip spočívá v odeslání fotonů odesílatele příjemci, který je detekuje. V praxi se počítá se dvěma možnostmi polarizace, a to rovnoběžné (též plus-schéma) a diagonální (x-schéma). Rovnoběžné schéma může být svisle nebo vodorovně polarizované a diagonální úhlopříčně zprava doleva nebo zleva doprava polarizované. Odesílatel poslal zprávu, která se skládá z 1 a 0. V plus-schématu bude svislá polarizace vyjádřena číslem 1 a vodorovná číslem 0, v x-schématu úhlopříčná zleva doprava číslem 1 a zprava doleva číslem 0. Pokud tedy příjemce nezná schéma, potom neví, jak přicházející foton detekovat. Pokud je přicházející foton rovnoběžný svislý a příjemce nebo útočník jej detekují diagonálním schématem, pak jim může a také nemusí, vyjít výsledek správně. Pokud zpráva projde jako diagonální zleva doprava, pak se označí číslem 1 a shoduje se s hodnotou svislé polarizace, jestliže ovšem vyjde, jako diagonální zprava doleva, pak vyjde 0 a hodnoty se neshodují. Chce-li např. odesílatel odeslat zprávu 1011 se schématem rovnoběžným, rovnoběžným, diagonálním a rovnoběžným, zvolí schéma rovnoběžné svisle, rovnoběžné vodorovně, diagonální zleva doprava a rovnoběžné svisle. Tímto způsobem pošle příjemci zprávu. Příjemce ovšem neví, jaké schéma odesílatel zvolil, a tak musí náhodně volit schéma. To zapříčiní, že příjemce uhodne jen polovinu schémat správně. Nyní odesílatel použije např. nezabezpečenou linku a zavolá příjemci. Tímto způsobem není snížena bezpečnost zprávy, jelikož útočník při odposlouchávání uhodl jen polovinu schémat jako příjemce. Navíc se jejich schémata liší, protože nehádají zpravidla totožně. Odesílatel a příjemce si telefonicky ověří, která schémata příjemce uhodl, a ty, které neuhodl, se ignorují. Z těch, které jsou společné pro obě strany, se vytvoří jednorázová tabulka, čímž naprosto znemožní útočníkovi úspěšně zachytit zprávu. Dalším velkým přínosem kvantové kryptografie, mimo její vysokou bezpečnost, je možnost odhalení odposlouchání zprávy útočníkem. Odhalení spočívá v tom, že každý foton po změření špatným detektorem změní svou polarizaci, tzn. útočník při zachytávání špatným detektorem změní polarizaci fotonu odesílatele a příjemci potom přijde foton s jinou polarizací, než s jakou byl odeslán. Po odeslání příjemce opět komunikuje s odesílatelem a zjistí, které fotony uhodl příjemce správně. Pokud odpovídá i schéma u náhodných čísel v příchozí zprávě, pak je komunikace bezpečná. Jestliže ovšem

čísla neodpovídají, potom je komunikace nezabezpečená a musí se začít nová na jiném kanále [7].

Po teoretické stránce je kvantová kryptografie dokonalá, ovšem realizace, zvláště na dlouhé vzdálenosti, je v současné době neproveditelná. Bennett se svým studentem Johnem Smolinem v roce 1988 realizovali první kvantový přenos, ovšem jen na vzdálenost 30 cm. Ale tímto pokusem dokázali, že kvantovou kryptografii lze realizovat. Inspirovali tím další kryptologické instituty, které se začaly výrobou systému kvantové kryptografie zabývat. Nejprve se uvažovalo o šíření fotonů vzduchem, ale protože foton není ideální pro dlouhé cestování a molekuly vzduchu mohou změnit molekuly vzduchu, muselo se od této možnosti ustoupit. V roce 1995 na ženevské univerzitě bylo využito pro přenos fotonů optické vlákno a provedl se přenos na vzdálenost 23 km. Přenos přes optické vlákno byl sice úspěšný, ale pro realizaci kvantové kryptografie v globálním měřítku je nutné se neomezovat délkou vlákna, proto se opět začalo experimentovat se vzduchem. V současné době se pracuje s možností přenosu přes satelity. Pokud se realizace kvantové kryptografie v globálním měřítku uskuteční, mohlo by to znamenat naprosté bezpečí soukromí. Ovšem stejně jako v minulosti i zde teprve čas ukáže, zda to tak opravdu bude, protože kryptoanalytikové si zatím poradili se všemi nástrahami kryptologů [7].

#### 4.4 Biotechnologie ve steganografii

V posledních několika měsících se pozornost kryptologů upnula především na steganografii, kde dochází k velkým pokrokům v utajování zpráv pomocí neviditelných inkoustů. Na konci roku 2011 přišli vědci z Tuftsovy univerzity s novou možností skrývat zprávy před nežádoucími osobami pomocí bakterií. Konkrétně se jedná o *Escherichia coli*, bakterii nacházející se běžně v žaludeční mikroflóře. Tento princip steganografie, nazývaný infoBiologie, spočívá v přenesení živých organismů na nitrocelulózovou membránu, která vypadá jako obyčejný papír. Bakterie jsou upraveny, aby na sebe vázaly barevné proteiny, které jsou viditelné jen pod UV zářením. Jednotlivé znaky textu jsou tvořeny kombinací barevných proteinů. Výhodou infoBiologie je možnost upravit zobrazení textu až po určitém časovém intervalu. Zprávě psané touto formou se říká Steganography by Printed Arrays of Microbes, zkráceně SPAM. Proces psaní zprávy probíhá tak, že nejprve se bakterie s barevnou bílkovinou umístí do Petriho misky se vzorem kódu. Petriho miska je vybavena agarem, což je médium, které umožní bakteriím vyvinout se a vyrůst. Když

bakterie vyrostou, tak se v přesném pořadí vytisknou na membránu. Taková zpráva je velmi stabilní a trvanlivá. Příjemce po příchodu této zprávy musí nejprve opět vrátit *Escherichia coli* zpět do Petriho misky s agarem a následně si je prohlédnout pod UV světlem. Aby zprávu mohl ovšem přečíst, musí znát tzv. barevný klíč. Tento klíč určuje, jaké složení jednotlivých barev zastupuje jaký znak. Např. zelená a červená spolu mohou značit znak S. Profesor David Walt, který se svým týmem vymyslel tento způsob skrytí textu, experimentoval dále a upravil *Escherichia coli*. Vytvořil v ní fluorescentní geny, které dokáží odolat antibiotikům. Pokud se tedy na Petriho misku s agarem použije vhodné antibiotikum ve správném množství, bude zpráva viditelná. Tento způsob by zajistil bezpečnost zprávy, protože útočník neznající dané antibiotikum a jeho dávku nemůže zprávu přečíst. Tím ale Walt nekončí, v současné době se pracuje na možnosti ovlivnit bakterie teplotou nebo jinými látkami, čímž by bakterie ztrácely své fluorescentní vlastnosti a časem by se ztrácely, což by odstranilo i samotnou zprávu. Princip infoBiologie není v současné době dostatečně známý veřejnosti, jelikož se jedná o novinku v oblasti steganografie. Tohoto principu ovšem využívají jiní vědci, zvláště v USA, a už vyvíjí možnost nahrazení *Escherichia coli* stabilnějšími látkami, jako např. kvasinkami nebo sporotvornými bakteriemi [9].

## ZÁVĚR

Cílem bakalářské práce bylo seznámit se s problematikou kryptografických algoritmů formou literární rešerše doplněnou autorem o detailní rozbor v jednotlivých kapitolách.

V úvodní části práce byly uvedeny základní pojmy v oblasti kryptologie, které jsou důležité pro pochopení dalších kapitol v této práci. Stručně byl popsán historický vývoj kryptologie od nejstarších dob až po současnost. Rovněž byly uvedeny nejznámější historické šifry, např. Caesarova šifra, Vigenèrova šifra či Playfairiova šifra. Z těch současných šifer autor zmínil zejména algoritmus RSA, který patří mezi asymetrické šifrové systémy. Tento algoritmus pak byl podrobně popsán v praktické části z matematického hlediska, s využitím modulární aritmetiky.

Praktická část byla věnována útokům na vybrané šifrové algoritmy, pro názornost autor vybral ukázky útoků na Caesarovu a Vigenèrovu šifru, které patří mezi ty nejjednodušší. Byla použita frekvenční analýza, která patří mezi nejpoužívanější metody luštění šifer. Nakonec byl proveden podrobný rozbor útoků na výše zmiňovaný algoritmus RSA.

Poslední kapitola bakalářské práce byla věnována některým novým trendům v oblasti kryptologie, např. kvantová kryptografie či biotechnologie.

Na závěr bych rád podotkl, že práce byla psána tak, aby byla srozumitelná zejména pro čtenáře, kteří nemají mnoho znalostí z oblasti kryptologie. Hlavně byl kladen důraz na co nejnázornější a nejpodrobnější vysvětlení principů kryptologie. Věřím, že jim přinese užitek.

## ZÁVĚR V ANGLIČTINĚ

The purpose of this bachelor thesis was to acquaint with cryptographic algorithms by literature search form, expanded by author with more detailed descriptions in each chapter.

In the introduction part there were given basic concepts of cryptography which are important to better understanding following parts of the thesis. Historical development of cryptography was briefly described. Best known historical ciphers were given as well, e. g. Caesar cipher, Vigenère cipher, Playfair cipher etc. From present ciphers, author mentioned RSA algorithm by few words in this chapter, detailed mathematical description was given in the practical part of the thesis.

The practical part of the thesis was devoted to attacks on selected algorithms, namely Caesar cipher and Vigenère cipher because of their simplicity and their easier description. It was chosen a frequency analysis which is one of the most used methods of decoding a cipher text. Finally, there was given detailed analysis of attacks on the RSA algorithm mentioned above.

The last part of the thesis is devoted to new trends in the field of cryptology, for example a quantum cryptography and a biotechnology.

In the end, I would like to remark that the thesis was written in order to be understandable mainly for the beginners of studying cryptology. Especially the emphasis was placed on the most revealing and detailed explanation of the principles of cryptology. I believe the thesis brings benefit to them.

**SEZNAM POUŽITÉ LITERATURY**

- [1] VONDRUŠKA, Pavel; BUCHALOVÁ, Bára. *Kryptologie, šifrování a tajná písma*. 1. vyd. Praha : Albatros, 2006. 340 s. ISBN 80-00-01888-8.
- [2] PIPER, F; MURPHY, Sean. *Kryptografie*. 1. vyd. v českém jazyce. Praha : Dokořán, 2006. 157 s. ISBN 80-7363-074-5.
- [3] ZELENKA, Josef, et al. *Ochrana dat kryptologie*. Hradec Králové : Gaudeamus, 2003. 500 s. ISBN 80-7041-737-4.
- [4] HANŽL, Tomáš. *Šifry a hry s nimi*. Vyd.1. Praha: Portál, 2007. ISBN 978-80-7367-196-9
- [5] HOWLETT, Tony. *Open source security tools: practical applications for security*. Upper Saddle River, NJ: Prentice Hall, c2005, 578 s. ISBN 03-211-9443-8.
- [6] TILBORG, Henk C. TILBORG. *Fundamentals of cryptology: a professional reference and interactive tutorial*. Vyd.1. Překlad Pavel Mondschein. Boston: Kluwer Academic Publishers, c2000, 490 s. ISBN 07-923-8675-2.
- [7] SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii*. 2. vyd. v čes. jaz. Překlad Petr Koubský, Dita Eckhardtová. Praha: Dokořán, 2009, 382 s. Aliter, sv. 9. ISBN 978-802-5701-447.
- [8] *Crypto-world: Informační sešit GCUCMP* [online]. 2010 [cit. 2012-05-14]. ISSN 1801-2140. Dostupné z: [http://crypto-world.info/casop12/crypto04\\_10.pdf](http://crypto-world.info/casop12/crypto04_10.pdf).
- [9] *Bakterie jako špionážní pomůcka? Ano!. 21. století: Revue objevů, vědy, techniky a lidí* [online]. Praha: RF HOBBY spol. s r.o, 2011, č. 2 [cit. 2012-05-17]. ISSN 1214-1097. Dostupné z: <http://21stoleti.cz/blog/2012/01/20/bakterie-jako-spionazni-pomucka-ano/>.
- [10] *Četnost znaků v anglickém textu. Algoritmy.net* [online]. 2011 [cit. 2012-05-06]. Dostupné z: <http://www.algoritmy.net/article/43/Cetnost-znaku-AJ>.
- [11] *Security.uhk* [online]. 2005 [cit. 2012-03-24]. Dostupné z: <http://security.uhk.cz/page.aspx>.

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

$\in$	patří
$\mathbb{R}$	množina všech reálných čísel
$f: \mathbb{R} \rightarrow \mathbb{R}$	zobrazení množiny reálných čísel do množiny reálných čísel
$\mathbb{R}^2$	množina všech uspořádaných dvojic reálných čísel $[x, y]$
$g: \mathbb{R}^2 \rightarrow \mathbb{R}^2$	zobrazení množiny $\mathbb{R}^2$ do množiny $\mathbb{R}^2$
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{Z}_m$	množina všech zbytkových tříd modulo $m$
AJ	anglický jazyk
DES	Data Encryption Standard
FBI	Federal Bureau of Investigation
IDEA	International Data Encryption Algorithm
mod	modulo
R–M test	Rabin–Millerův test
RSA	Rivest-Shamir-Adelman

## SEZNAM OBRÁZKŮ

Obrázek 1: <i>Symetrický šifrový systém</i> .....	15
Obrázek 2: <i>Asymetrický šifrový systém</i> .....	15
Obrázek 3: <i>Šifrování otevřeného textu Caesarovou šifrou programem Mathematica</i> .....	22
Obrázek 4: <i>Vigenèrův čtverec</i> .....	23
Obrázek 5: <i>Šifrování otevřeného text Vigenèrovou šifrou v programu Mathematica</i> .....	24
Obrázek 6: <i>Graf četnosti výskytu znaků zašifrovaného textu Caesarovou šifrou a výskyt znaků v anglickém jazyce</i> .....	33
Obrázek 7: <i>Četnost výskytu jednotlivých znaků v anglickém jazyce</i> .....	35
Obrázek 8: <i>Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem <math>X_1</math></i> .....	35
Obrázek 9: <i>Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem <math>X_2</math></i> .....	37
Obrázek 10: <i>Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem <math>X_3</math></i> .....	38
Obrázek 11: <i>Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem <math>X_4</math></i> .....	39
Obrázek 12: <i>Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem <math>X_5</math></i> .....	39
Obrázek 13: <i>Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem <math>X_6</math></i> .....	40
Obrázek 14: <i>Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem <math>X_7</math></i> .....	40
Obrázek 15: <i>Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem <math>X_8</math></i> .....	41
Obrázek 16: <i>Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem <math>X_9</math></i> .....	41
Obrázek 17: <i>Četnost výskytu jednotlivých znaků pro abecedu definovanou písmenem <math>X_{10}</math></i> .....	42
Obrázek 18: <i>Výpočet frekvenční analýzy v programu Mathematica</i> .....	43
Obrázek 19: <i>Četnost znaků šifrovaného textu provedeném v programu Mathematica</i> .....	43
Obrázek 20: <i>Výpočet pravděpodobnosti v programu Mathematica</i> .....	45

---

Obrázek 21: <i>Výpočet <math>k</math> pomocí programu Mathematica</i> .....	46
Obrázek 22: <i>Výpočet indexu koincidence v programu Mathematica</i> .....	47
Obrázek 23: <i>Výpočet četnosti v programu Mathematica</i> .....	49
Obrázek 24: <i>Využití koeficientu koincidence</i> .....	49
Obrázek 25: <i>Využití koeficientu koincidence s <math>t \in \langle 1,10 \rangle</math></i> .....	51

**SEZNAM TABULEK**

Tabulka 1: <i>Příklady znaků šifrové abecedy</i> .....	13
Tabulka 2: <i>Příklad Caesarovy šifry s posunem o 3 znaky</i> .....	21
Tabulka 3: <i>Klíč v tabulce s doplňujícími znaky</i> .....	25
Tabulka 4: <i>Rozšířená tabulka s klíčem</i> .....	25
Tabulka 5: <i>Četnost výskytu znaků zašifrovaného textu Caesarovou šifrou a výskyt znaků v anglickém jazyce</i> .....	32
Tabulka 6: <i>Údaje o opakovaných sekvencích</i> .....	34
Tabulka 7: <i>Přehled četnosti výskytu znaků v anglickém jazyce a pro jednotlivá písmena X</i> .....	36
Tabulka 8: <i>Koeficient koincidence pro národní abecedy</i> .....	48

**SEZNAM PŘÍLOH**

Příloha P I: Otevřený text.....	13
Příloha P II: Caesarova šifra – šifrovaný text .....	21
Příloha P III: Vigenèrova šifra – šifrovaný text .....	25
Příloha P IV: Play-fairova šifra – šifrovaný text.....	25

## **PŘÍLOHA P I: OTEVŘENÝ TEXT**

Text z přílohy PI byl převzat ze zdroje [5].

### Preface

Open source software is such an integral part of the Internet that it is safe to say that the Internet wouldn't exist as we know it today without it. The Internet never would have grown as fast and as dynamically as it did without open source programs such as BIND, which controls the domain name system; Sendmail, which powers most e-mail servers; INN, which runs many news servers; Major Domo, which runs many of the thousands of mailing lists on the Internet; and of course the popular Apache Web server. One thing for sure is that the Internet is a lot cheaper due to open source software. For that, you can thank the Free Software Foundation, BSD UNIX, Linux and Linus Torvalds, and the thousands of nameless programmers who put their hard work and sweat into the programs that run today's Internet. While open source programs cover just about every aspect of computer software from complete operating systems and games to word processors and databases—this book primarily deals with tools used in computer security. In the security field, there are programs that address every possible angle of IT security. There are open source firewalls, intrusion detection systems, vulnerability scanners, forensic tools, and cutting-edge programs for areas such as wireless communications. There are usually multiple choices in each category of mature, stable programs that compare favorably with commercial products. I have tried to choose the best of breed in each major area of information security (in my opinion, of course!). I present them in a detailed manner, showing you not just how to install and run them but also how to use them in your everyday work to have a more secure network. Using the open source software described in this book, you can secure your enterprise from both internal and external security threats with a minimal cost and maximum benefit for both the company and you personally. I believe combining the concepts of information security with open source software offers one of the most powerful tools for securing your company's infrastructure, and by extension the entire Internet. It is common knowledge that large-scale virus infections and worms are able to spread because many systems are improperly secured. I believe that by educating the rank-and-file system managers and giving them the tools to get the job done, we can make the Internet more secure, one network at a time.

## Audience

The audience for this book is intended to be the average network or system administrator whose job duties are not specifically security and who has at least several years of experience. This is not to say that security gurus won't get anything out of this book; there might be areas or tools discussed that are new to you. And likewise, someone just getting into IT will learn quite a bit by installing and using these tools. The concepts discussed and techniques used assume a minimal level of computer and network proficiency. There is also a broad group of readers that is often overlooked by the many open source books. These are the Windows system administrators. The info-security elite often has a certain disdain for Windows-only administrators, and little has been written on quality open source software for Windows. However, the fact remains that Windows servers make up the lion's share of the Internet infrastructure, and ignoring this is doing a disservice to them and the security community at large. While overall the book is still tilted towards Linux/UNIX because most open source programs are still Linux/UNIX-only, I have tried to put Windows-based security tools in every chapter. I've also included helpful hints and full explanations for those who have never run a UNIX machine.

## Contents

This book covers most of the major areas of information security and the open source tools you can use to help secure them. The chapters are designed around the major disciplines of information security and key concepts are covered in each chapter. The tools included on the book's CD-ROM allow for a lab-like environment that everyone can participate in. All you need is a PC and this book's CD-ROM to start using the tools described herein. This book also contains some quick tutorials on basic network terminology and concepts. I have found that while many technicians are well-schooled in their particular platforms or applications, they often lack an understanding of the network protocols and how they work together to get your information from point A to point B. Understanding these concepts are vital to securing your network and implementing these tools properly. So while this book may seem slanted towards the network side of security, most of the threats are coming from there these days, so this is the best place to start. Coverage of each security tool is prefaced by a summary of the tool, contact information, and various resources for support and more information. While I give a fairly detailed look at the tools covered, whole books can and have been written on many of the programs discussed. These resources give you options for

further research. Helpful and sometimes humorous tips and tricks and tangents are used to accent or emphasize an area of particular importance. These are introduced by Flamey the Tech, our helpful yet sometimes acerbic mascot who is there to help and inform the newbies as well as keeping the more technical readers interested in sections where we actually make some minor modifications to the program code. He resembles the denizens you may encounter in the open source world. In exploring the open source world, you will meet many diverse, brilliant, and sometimes bizarre personalities (you have to be at least a little bent to spend as much unpaid time on these programs as some of us do). Knowing the proper etiquette and protocol will get you a lot farther and with fewer flames. On a more serious note, many of the tools in this book can be destructive or malicious if used in the wrong ways. You can unintentionally break the law if you use these tools in an uninformed or careless manner (for example, accidentally scanning IP addresses that aren't yours with safe mode off). Flamey will always pipe up to warn you when this is a possibility.

#### Open Source Security Tool Index

Immediately following this Preface is a listing of all the tools and the pages where they are covered. This way you can skip all the background and go straight to installing the tools if you want.

#### Chapter 1: Information Security and Open Source Software

This chapter offers an introduction to the world of information security and open source software. The current state of computer security is discussed along with a brief history of the open source movement.

#### Chapter 2: Operating System Tools

This chapter covers the importance of setting up your security tool system as securely as possible. A tool for hardening Linux systems is discussed as well as considerations for hardening Windows systems. Several operating system-level tools are reviewed too. These basic tools are like a security administrator's screwdriver and will be used again and again throughout the course of this book and your job.

#### Chapter 3: Firewalls

The basics of TCP/IP communications and how firewalls work are covered here before jumping into installing and setting up your own open source firewall.

#### Chapter 4: Port Scanners

This chapter delves deeper into the TCP/IP stack, especially the application layer and ports. It describes the installation and uses for a port scanner, which builds up to the next chapter.

#### Chapter 5: Vulnerability Scanners

This chapter details a tool that uses some of the earlier technology such as port scanning, but takes it a step further and actually tests the security of the open ports found. This security Swiss army knife will scan your whole network and give you a detailed report on any security holes that it finds.

#### Chapter 6: Network Sniffers

This chapter primarily deals with the lower levels of the OSI model and how to capture raw data off the wire. Many of the later tools use this basic technology, and it shows how sniffers can be used to diagnose all kinds of network issues in addition to tracking down security problems.

#### Chapter 7: Intrusion Detection Systems

A tool that uses the sniffer technology introduced in the previous chapter is used here to build a network intrusion detection system. Installation, maintenance, and optimal use are also discussed.

#### Chapter 8: Analysis and Management Tools

This chapter examines how to keep track of security data and log it efficiently for later review. It also looks at tools that help you analyze the security data and put it in a more usable format.

#### Chapter 9: Encryption Tools

Sending sensitive data over the Internet is a big concern these days, yet it is becoming more and more of a requirement. These tools will help you encrypt your communications and files with strong encryption as well as create IPsec VPNs.

#### Chapter 10: Wireless Tools

Wireless networks are becoming quite popular and the tools in this chapter will help you make sure that any wireless networks your company uses are secure and that there aren't wireless LANs you don't know about.

## Chapter 11: Forensic Tools

The tools discussed in this chapter will help you investigate past break-ins and how to properly collect digital evidence.

## Chapter 12: More On Open Source Software

Finally, this chapter will give you resources for finding out more about open source software. Various key Web sites, mailing lists, and other Internet-based resources are identified. Also, I give a number of ways to become more involved in the open source movement if you so desire.

## Appendix A: Common Open Source Licenses

Contains the two main open source licenses, the GPL and BSD software licenses.

## Appendix B: Basic Linux/UNIX Commands

Contains basic navigation and file manipulation commands for those new to UNIX and Linux.

## Appendix C: Well-Known TCP/IP Port Numbers

Contains a listing of all the known port numbers as per IANA. Note that this section is not intended to be comprehensive and is subject to constant update. Please check the IANA Web site for the most current information.

## Appendix D: General Permission and Waiver Form

Contains a template for getting permission to scan a third-party network (one that is not your own). This is intended to be used as an example only and is not intended as a legal document.

## Appendix E: Nessus Plug-ins

Contains a partial listing of plug-ins for the Nessus Vulnerability Scanner discussed in Chapter 5. This listing will not be the most current since the plug-ins are updated daily. The Nessus Web site should be consulted for plug-ins added after January 12, 2004.

## CD-ROM Contents and Organization

The CD-ROM that accompanies this book has most of the open source security tools on it for easy access and installation. The disk is organized into directories labeled by tool. If

there are separate files for Windows and Linux, they will be in their own directories. The directory “Misc” has various drivers and other documentation such as RFCs that will be of general use through your reading.

### Using the Tools

Whenever possible, the tools in this book are provided in RedHat Package Manager (RPM) format. Of course, you don't have to be running RedHat Linux to use RPM. The RedHat folks originally designed it, but now it comes with most Linux versions. The RedHat Package Manager automates the installation process of a program and makes sure you have all the supporting programs and so forth. It is similar to a Windows installation process where you are guided through the process graphically and prompted where necessary. Using the RPM is almost always preferable to doing a manual installation. When you need to set custom install parameters or if a RPM file is not available for your distribution, I describe how to install the program manually. If the RPM file is provided, simply download the file or copy it from the CD-ROM that comes with this book and click on it. Your version of RPM will take care of the rest. If you use any of the other variations of UNIX (BSD, Solaris, HP/UX, and so on), they will probably work with the tools in this book, but the installation instructions may be different. You can run most of the tools in this book on alternative versions of UNIX or Linux. Staying within the Linux family will certainly make compatibility more likely with the actual tools on the CD-ROM. If you have to download a different version of the program, some of the features discussed may not be supported. But if you are a Solaris aficionado or believe that BSD is the only way to go, feel free to use it as your security workstation. Just be aware that the instructions in this book were designed for a specific implementation and you may have to do some additional homework to get it to work. The platforms supported are listed at the beginning of each tool description.

### Reference Installation

Most of the tools in this book were tested and reviewed on the following platforms:

- Mandrake Linux 9.1 on a HP Vectra series PC and a Compaq Presario laptop.
- Windows XP Pro and Windows 2000 Pro on a Compaq Prosignia series desktop and Compaq Armada laptop.

### Input or Variables

In code and command examples, italics are used to designate user input. The words in italics should be replaced with the variables or values specific to your installation. Operating system-level commands appear like this: `ssh -l login hostname`. Due to page size limits, code lines that wrap are indented with a small indent. I hope you enjoy and learn from this book. There are many, many more tools that I couldn't include due to space limitations, and I apologize in advance if I didn't include your favorite tool. I had room to cover only my favorites and tried to pick the best of breed in each category. I'm sure some will differ with my choices; feel free to e-mail me at [tony@howlett.org](mailto:tony@howlett.org), and perhaps those will make it into a future edition.

### Acknowledgments

This book wouldn't be possible without the tireless efforts of programmers all around the world, making great open source software. I'd name a few but would certainly leave too many out. Thanks for your great software! I'd like to thank my business partner, Glenn Kramer, for assisting with proofing this book (as well as minding the business while I was busy trying to make deadlines) and my Nessus Command Center (NCC) project mates, Brian Credeur, Lorell Hathcock, and Matt Sisk. Finally, my love and gratitude goes to my lovely wife, Cynthia, and daughters, Carina and Alanna, who sacrificed countless hours without husband and daddy to make this book happen

## PŘÍLOHA P II: CAESAROVA ŠIFRA – ŠIFROVANÝ TEXT

SUHIDFHRSHQVRXUFHVRIWZDUHLVVXFKDQLQWHJUDOSDUWRIWKHLQW  
HUQHWWKDWLVLVVDIHWRVDBWKDWWKHLQWHUQHWRXOGQWHALV  
WDVZHNQRZLWWRGDBZLWKRXLWVKHLQWHUQHWRQHYHUZRKXOGKDY  
HJURZQDVIDVWDQGDVGBQDPLFDOOBDVLWGLGZLWKRXWRSHQVRXUFHS  
URJUDPVVXFKDVELQGZKLFKFRQWUROVWKHGRPDLOQDPHVBVWHPVHQG  
PDLOZKLFKSRZHUVPRVWHPDLOVHUYHUVLQQZKLFKUXQVPDQBQHZVVH  
UYHUVPMRUGRPRZKLFKUXQVPDQBRIWKHWKRXVDQGVRIPLDOLQJOLV  
WVRQWKHLQWHUQHWDQGRIFRXUVHWKHSRSXODUDSDFKHZHEVHUYHU  
RQHWKLQJIRUVXUHLVWKDWWKHLQWHUQHWWLVDORWFKHDSHUGXHWR  
RSHQVRXUFHVRIWZDUHIRUWKDWBRXFDQWKDQNKHIUHHVRIWZDUHIR  
XQGDWLRQEVGXQLAOLQXADQGOLQXVWRUYDOGVDOGWKHWKRXVDQG  
VRIQDPHOHVVSURJUDPPHUVZKRSXWVKHLUKDUGZRUNDQGVZHDWLQW  
RWKHSURJUDPVWKDWUXQWRGDBVLQWHUQHWWZKLOHRSHQVRXUFHSUR  
JUDPVFRYHUMXVWDERXWHYHUBDVSHFWRIFRPSXWHUVRIWZDUHIURPFR  
PSOHWRSHUDWLQJVBVWHPVDQGDJPHVWRZRUGSURFHVVRUVDQGGDW  
DEDVHVWKLVERRNSULPDULOVBGHDOVZLWKWRROVXVHGLQFRPSXWHUV  
HFXULWBLQWKHVHFXULWBILHOGWKHUHDUHSURJUDPVWKDWGGUHV  
VHYHUBSRVLEOHDQJOHRILWVHFXULWBWKHUHDUHRSHQVRXUFHILUH  
ZDOOVLQWUXVLRQGHWHFWLRQVBVWHPVYXOQHUDELOLWBVFDQQHUVI  
RUHQVLFWRROVDQGFXXWLQJHGJHSURJUDPVIRUDUHDVVXFKDVZLUHOH  
VFRPPXQLFDWLRQVWKHUHDUHXVXDOOBXPOWLSOHFKRLFHVQLQHDFKF  
DWHJRUBRIPDWXUHVWDEOHSURJUDPVWKDWFRPSDUHIDYRUDEOBZLWK  
FRPPHUFLOSURGXFWVLKDYHWULHGWRFRKRRVHWKHEHVWRIEUHHGLQ  
HDFKPDMRUDUHDRILQIRUPDWLRQVHFXULWBLQPBRSLQLRQRIFRXUVHLS  
UHVHQWVKHPLQDGHWDLOHGPDQQHUVKRZLQJBRXQRWMXVWKRZWRLO  
VWDOODQGUXQWKHPEXWDOVRKRZRXXVHWKHPLQBRXUHYHUBGDBZR  
UNWRKDYHDPRUHVHFXUHQHWRUNXVLQJWKHRSHQVRXUFHVRIWZDUH  
GHVFULEHGLQWKLVERRNBRXFDQVHFXUHBRXUHQUHUSULVHIURPERWK  
LQWHUQDODQGHAWHUQDOVHFXULWBWKUHDWVZLWKDPLQLPDOFRVW  
DQGPDALPXPEHQHILWIRUERWKWKHFRPSDQBDQGBRXSHUVRQDOOBLEHO  
LHYHFRPELQLQJWKHFRQFHSWVRILQIRUPDWLRQVHFXULWBZLWKRSHQV

RXUFHVRIWZDUHRIIHUVRQHRIWKHPRVWSRZHUIXOWRROVIRUVHFXULQJ  
BRXUFRPSDQBVLIUDVWUXFWXUHDQGEHBHAWHQVLRQWKHHQWLUHLQ  
WHUQHHLWLWVFRPPRQNQRZOHGJHWKDWODUJHVFDHXYLUXVLQIHFWR  
QVDQGZRUPVDUHDEOHWVRSUHDGEHFDXVHPDQBVVWHPVDUHLPSURSH  
UOBVHFXUHGLEHOLHYHWKDWEBHGXFIDLQJWKHUDQNDQGILOHVBVWH  
PPDQDJHUVDQGLYLQJWKHPWKHWRRVWRJHWWKHMREGRQHZHFDQPD  
NHWKHLQWHUQHWPVPRUHVHFXUHRQHQHWRZUNDWDWLPHDXGLHQFHWK  
HDXGLHQFHIRUWKLVERRNLVLQWHQGHGWREHWKHDYHUDJHQRHWZRNR  
UVBVWHPDGPLQLVWUDWRUZKRVMREGXWLHVDUHQRWVSHFLILFDOOB  
VHFXULWBDQGGZKRKDVWVWVHGHVWVHYHUBHBUVRHASHULHQFHWKL  
VLVQRWWRVDBWKDWVHFXULWBJXUXVZRQWJHWDQBWKLQJRXWRIWKL  
VERRNWKHUHPLJKWEHVDUHDVURUWRROVGLVFXVVHGWKDWDUHQHZWRB  
RXDQGGOLNHZLVHVRPHRQHMXVWJHWWLQJLQWRLWZLOOHDUQTXLWH  
DELWEBLQVWDOOLQJDQGXVLQJWKHVHWRROVWKHFRQFHSWVGLVFXVV  
HGDQGWVHFKQLTXHVXVHGDVVPXPHDPLQLPDOOHYHORIFRPSXWHUDQGGQH  
WZRUNSURILFLHQFBWKHUHLVDOVRDEURDGJURXSRIUHDGHUVWKDWLV  
RIWHQRYHUORRNHGEBWKHPDQBRSHQVRXUFHERRNVWKHVHVDUHWKHZL  
QGRZVVBVWHPDGPLQLVWUDWRUVWKHLQIRVHFXULWBHOLWHRIWHQK  
DVDFHUWDLQGLVGLQIRUZLQGRZVRQOBDGPLQLVWUDWRUVDQGGOLWW  
OHKDVVHQQZULWWHQRTXDOLWBRSHQVRXUFHVRIWZDUHIRUZLQGRZV  
KRZHYHUWKHIDFWUHPDLQVWKDWZLQGRZVVHUYHUVDPNHXSWKHOLR  
QVVKDUHRIWKHLQWHUQHHLWLIUDVWUXFWXUHDQGLJQRULQJWKLVLVGL  
RLQJDGLVVHUYLFWHWRWKHPDQGWKHVHFXULWBFRPPXQLWBDWODUJHZ  
KLOHRYHUDOOWKHERRNLVVWLOWLOWHGWZRZDUGVOLQXAXQLAEHFD  
XVHPRVWRSHQVRXUFHSURJUDPVDUHVWLOOOLQXAXQLARQOBLKDYHW  
ULHGWRSXWZLQGRZVEDVHGVHFXULWBWRROVLQHYHUBFKDSWHULYHD  
OVLQFOXGHGKHOSIXOKLQWVDQGXOOHASODQDWLRQVIRUWKRZHVKR  
KDYHQHYHUUXQDXQLAPDFKLQHFQRQWHQWVWKLVERRNFRYHUVPVWRRI  
WKHPDMRUDUHDVRIHQIRUPDWLRQVHFXULWBDQGWKHRSHQVRXUFHWR  
ROVBRXFDQXVHWRKHOSVHFXUHWKHPWKHFKDSWHUVDUHGHLVJQHGD  
URXQGKHPDMRUGLVFLSOLQHVRILQIRUPDWLRQVHFXULWBDQGNHBF  
QFHSWVDUHFYHUHGLQHDFKFKDSWHUWKHWRRVLRQFOXGHGRQWKHE  
RRNVFGURPDOORZIRUDODEOLNHHQYLURQPHQWVKDWWHYHUBRQHFDQS



XSWRZDUQBRXZKHQWKLVLVDSRVVLELOLWBRSHQVRXUFHVHFXULWBW  
RROLQGHALPPHGLDWHOBIROORZLQJWKLVSUHIDFHLVDOLVWLQJRIDOOW  
KHWRROVDQGWKHSDJHVZKHUHWKHBUDHFRYHUHGWKLZDBBRXFDQV  
NLSDOOWKHEDFNJURXQGDQGGJRVWUDLJKWWRLQVWDOOLQJWKHWRROV  
LIBRXZDQWFKDSWHULQIRUPDWLRQVHFXULWBDQGRSHQVRXUFHVRIWZ  
DUHWKLVFKDSWHURIIHUVLQWURGXFWLRQWRWVKHZRUGRILQIRUPD  
WLRQVHFXULWBDQGRSHQVRXUFHVRIWZDUHWKHFUHQWVWDWHRIF  
RPSXWHUVHFXULWBLVGLVFXVVHGDORQJZLWKDEULHIKLVWRUBRIWKH  
RSHQVRXUFHPRYHPHQWFKDSWHURSHUDWLQJVBVWHPWRROVWKLVKD  
SWHUFYHUVWVKHLPSRUWDQFHRIVHWWLQJXSBRXUVHFXULWBWRROVB  
VWHPDVVHFXUHOBVSRVVLEOHDWRROIRUKDUGHQLQJOLQXAVBVWHP  
VLVGLVFXVVHGDVZHOOVFRQVLGHUDWLRQVIRUKDUGHQLQJZLQGRZV  
VBVWHPVVHYHUDORSHUDWLQJVBVWHPHYHOWRROVDUHUHYLHZHGW  
RRWKHVHEDVLFWRROVDUHOLNHDVHFXULWBDGPLQLVWUDWRUVVUFU  
ZGULYHUDQGZLOOEHVHGDJDLQDQGDJDLQWKURXJKRXWWKHFRXUVH  
RIWKLVERRNDQGBRXUMREFKDSWHUILUHZDOOVWKHEDVLFVRIWFSLFR  
PPXQLFDWLRQVDQGGKRZILUHZDOOVZRUNDUHFRYHUHGKHUHEHIRUHMXP  
SLQJLQWRLQVWDOOLQJDQGVHWWLQJXSBRXURZQRSHQVRXUFHILUHZDO  
OFKDSWHUSRUWVFDQQHUVWKLVKDSWHUGHOYHVGHHSHULQWRWKH  
WFSLSVWDFNHVSHFLDOOBWKHDSSOLFDWLRQODBHUDQGSRUWVLWGHV  
FULEHVWVKHLQVWDOODWLRQDQGXVHVIRUDSRUWVFDQQHUZKLFKEXLO  
GVXSWRWKHAWFKDSWHUFKDSWHUYXOQHUDELOLWBVFDQQHUVWK  
LVFKDSWHUGHWDLOVDWRROWKDWXVHVVRPHRIWKHHDUOLHUWHFKQR  
ORJBVXFKDVSRUWVFDQQQLQJEXWWDNHVLWDVWHSIXUWKHUDQGDVFX  
DOOBWHVWVWVKHVHFXULWBRIWKHRSHQSRUWVIRXQGWKLVVHFXULWB  
VZLVVDUPBNQLIHZLOOVFDQBRXUZKROHQHWZRUNDQGLYHBRXDGHWD  
LOHGUHSRUWRQDQBVHFXULWBKROHVWKDWLWILQGVFKDSWHUQHWZR  
UNVQLIIHUVWKLVKDSWHUSULPDULOVBGHDOVZLWKWKHORZHUOHYHOV  
RIWKHRVLPRGHODQGGKRZWRFDVXUHUDZGDWDRIIWKHZLUHPDQBRIWK  
HODWHUWRROVXVHWKLVEDVLFVHFKQRORJBDQGLWVKRZVKRZVQLIIHU  
VFDQEHXVHGWRGLDJQRVHDOONLQGVRIQHWZRUNLVVXHVLQDGGGLWLR  
QWRWUDFNLQJGRZQVHFXULWBASUREOHPVFKDSWHULQWUXVLRQGHWHF  
WLRQVBVWHPVDWRROWKDWXVHVWVKHVQLIIHUWHFKQRORJBLQWURGX

FHGLQWKHSUHYLRXVFKDSWHULVXVHGKHUHWREXLOGDQHWZRUNLQW  
UXVLRQGHWHFWLRQVBVWHPLQVWDOODWLRQPDLQWHQDQFHDQGRSWL  
PDOXVHDOHDOVRGLVFXVVHGFKDSWHUDQDOBVLVDQGPDQDJHPHQWWR  
ROVWKL VFKDSWHUHADPLQHVKRZWRNHHSWUDFNRIVHFXULWBGDWDD  
QGORJLWHIILFLHQWOBIRUODWHUUHYLHZLWDOVRORRNVDWWRROVWK  
DWKHOSBRXDQDOBCHWKHVHFXULWBGDWDDQGSXWLWLQDPRUHXVDEO  
HIRUPDWFKDSWHUHQFUBSWLRQWRROVVHQGLQJVHQVLWLYHGDWDRYH  
UWKHLQWHUQHVLVDELJFRQFHUQWKHVHGDBVBHWLWLVEHFRPLQJPRU  
HDQGPURHRIDUHTXLUHPHQWVKHVHWRROVZLOOKHOSBRXHQFUBSWBR  
XUFRPPXQLFDWLRQVDQGILOHVZLWKVWURQJHQFUBSWLRQDVZHOODVF  
UHDWHL SVHFYSQVFKDSWHUZLUHOHVVRROVZLUHOHVQHWZRUNVD  
UHEHFRPLQJTXLWHSRSXODUDQGWKHWRRVLQWKL VFKDSWHUZLOOKH  
OSBRXPDNHVXUHWKDWDBZLUHOHVQHWZRUNVBRXUFRPSDQBXVHVD  
UHVHFXUHDQGWKDWKWHUHDUHQWZLUHOHVODQVBRXGRQWNQRZDE  
RXWFKDSWHUIRUHQVLFWRROVWKHWRROVGLVFXVVHGLQWKL VFKDSW  
HUZLOOKHOSBRXLQYHVWLJDWHSVWEUHDNLQVDQGKRZRSURSHUOB  
FROOHFWGLJLWDOHYLGHQFHFKDSWHUPRUHRQRSHQVRXUFHVRIWZDUHI  
LQDOOBWKL VFKDSWHUZLOOJLYHBRXUHVRXUFHVIRUQLQGLQJRXWPRUH  
DERXWRSHQVRXUFHVRIWZDUHYDULRXVNBZHEVLWHVDPDLOLQJOLVWV  
DQGRWKHULQWHUQHWEDEVHGUHVVRXUFHVDUHLGHQWLILHGDOVRLJLYH  
DQXPEHURIZDBVWREHFRPHPRUHLQYROYHGLQWKHRSHQVRXUFHPRYHPH  
QWLIBRXVRGHVLUHDSSHQGLADFRPPRQRSHQVRXUFHOLFHQVHVFRQWDL  
QVWKHWZRPDLQRSHQVRXUFHOLFHQVHVWKHJSODQGEVGVRIWZDUHOLF  
HQVHV DSSHQGLAEEDVLFOLQXAXQLAFRPPDQGVFRQWDLQVEDVLFQDYLJ  
DWLRQDQGILOHPDQLSXODWLRQFRPPDQGVIRUWKR VHQHZWRXQLADQGO  
LQXADSSHQGLAFZHOONQRZQWFSLSRUWQXPEHUVFRQWDLQVDOLVWLQ  
JRIDOOWKHNQRZQSRUWQXPEHUVDVSHULDQDQRWHWKDWWKLVVHFWL  
RQLVQRWLQWHQGHGWREHFRPSUHKKHVLYHDQGLVXEMHFWWRFRQVW  
DQWXSGDWHSOHDVHFKHFNWKHLDQDZHEVLWHIRUWKHPRVWFXUUHQW  
LQIRUPDWLRQDSSHQGLAGJHQHUDOSHUPLVVLQRQDQGDZLYHUIRUPFRQW  
DLQVDWHP SODWHIRUJHWWLQJSHUPLVVLQRQWRVFDQDWKLU GSDUWBQH  
WZRUNRQH WKDWLVQRWBRXURZQWKLVLVLQWHQGHGWREH XVHGDVDDQ  
HADPSOHRQOBDQGLVQRWLQWHQGHGDVDOHJDOGRFXPHQWDSSHQGLAH

QHVVXVSOXJLQVFRQWDLQVDSUWLDLQVWLVWLQJRISOXJLQVIRUWKHQHV  
VXVYXOQHUELOLWBVFDQHQUGLVFXVVHGLQFKDSWHUWKLVLQVWLQJ  
ZLOOQRWEHWKHPRVWFXUUHQWVLQFHWKHSOXJLQVDUHXSGDWHGGDL  
OBWKHQHVXVZHEVLWHVKRXOGEHFRQVXOWHGIRUSOXJLQVDGGHGDI  
WHUMDQXDUBFGURPFRQWHQWVDQGRUJDQLCDWLRQWKHFGURPWKDW  
DFFRPSDQLHVWKLVERRNKDVPRVWRIWKHRSHQVRXUFHVHFXULWBWRO  
VRQLWIRUHDVBDFFHVVDQGLQVWDOODWLRQWKHGLVNLVRUJDQLCHGL  
QWRGLUHFWRULHVODEHOHGEBWRROLIWKHUHDUHVHSDUDWHILOHVIR  
UZLQGRZVDQGOLOXAWKHBZLOOEHLQWKHLURZQGLUHFWRULHVWKHGL  
UHFWRUBPLVFKDVYDULRXVGULYHUVDQGRWKHUGRFXPHQWDWLRQVXF  
KDVUIFVWKDWZLOOEHRIJHQHUDOXVHWKURXJKBRXUHDGLQJXVLQJW  
KHWRROVZKHQHYHUSRVVLEOHWKHWRROVLQWKLVERRNDUHSURYLGH  
GLQUHGKDWSDFNDJHPDQDJHUUSPIRUPDWIRFXUVHBRXGRQWKDYHWRE  
HUXQQLOJUHGKDWOLQXAWRXVHUSPWKHUHGKDWIRONVRULJLQDOOBG  
HVLJQHGLWEXWQRZLWFRPHVZLWKPRVWOLQXAYHUVLRQVWKHUHGK  
WSDFNDJHPDQDJHUDXWRPDWHVWKLQVWDOODWLRQSURFHVVZRIDSURJ  
UDPDQGPDNHVXUHBRXKDYHDOOWKHVXSSRUWLQJSURJUDPVDQGVIR  
UWKLWLVLPLODUWRDZLQGRZVLQVWDOODWLRQSURFHVVZKHUHBXRD  
UHJXLGHGWKURXJKWKHSURFHVVJUDSKLFDQOBDQGSURPSWHGZKHUHQ  
HFHVVDUBXVLQJWKHUSPLVDOPRVWDOZDBVSUHIHUEOHWRGRLQJDPD  
QXDOLQVWDOODWLRQZKHQBRXQHGGWRVHWFVWRPLQVWDOOSDUDP  
HWHUVRULIDUSPILOHLVQRWDYDLODEOHIRUBRXUGLVWULEXWLRQLGH  
VFULEHKRZWRQLQVWDOOWKHSURJUDPPDQXDOOBLIWKHUSPILOHLVSURY  
LGHGVLPSOBGRZQORDGWKHILOHRUFRSBLWIURPWKHFGURPWKDWFRPH  
VZLWKWKLVERRNDQGFOLFNRQLWBRXUYHUVLRQRIUSPZLOOWDNHFDUH  
RIWKHUHVWLIBRXXVHDQBRIWKHRWKHUYDULDWLRQVRIXQLAEVGVROD  
ULVKSXADQGVRRQWKHBZLOOSUREDEOBZRUNZLWKWKHWRROVLQWKL  
ERRNEXWWKHLQVWDOODWLRQLQVWUXFWLRQVPDBEHGLIHHUHQWBRXF  
DQUXQPRVWRIWKHWRROVLQWKLVERRNRQDOWHUQDWLYHYHUVLRQVR  
IXQLARUOLQXAVWDBLQJZLWKLQWKHOLQXAIIDPLOBZLOOFHUWDLQOBPD  
NHFRPSDWLELOLWBPRUHOLNHOBZLWKWKHDFWXDOWRROVRQWKHFGU  
RPLIBRXXKDYHWRGRZQORDGDGLIHHUHQWYHUVLRQRIWKHSURJUDPVRPHR  
IWKHIHDWXUHVGLVFXVVHGPDBQRWEHVXSSRUWHGEXWLIBRDXDUHDVR



### **PŘÍLOHA P III: VIGENÈROVA ŠIFRA – ŠIFROVANÝ TEXT**

TEGWYRXWDRRFQLPRXAC SXJ C IC X L A I P L N P Z L I X O F N P C C I R D Y B V R M A V V P C  
X B H U E G K J G I L I T R X B U R W I A I H G L R K E R T K V S G A B W C B C M M L V W G C J U T D V C J M  
G V F B P R E W G L B W K G I M P S V R G G I L T M V S I E Y F S A W P O I T T F U C T A T N W G C E B P L L  
M A E Z K T Y A E G O F M G F Z B L B B V B Y G Q G C C L W I E G R R I M V K I A F W H E Y Y H U Q B Q A U  
K T F R H V H E S Y U K F T W W A N M A P R K T L G G G I Z U V L S F I W Y A U K T F E H E S E W Z Q J R T F  
I W Y W R T M C G L Q B A A U K T F G N V G Z E A A E C L L A S E Z R T J K P C W F Q S Z Q N F X V P F H R F  
O R L N H N H U I G J F S H T V R F S S O R G A B V U Y M F V J M C M P S V R G G I L T M I B Q S S E F S G L M  
H U I C Q G S A T Z O C E P J V U T U A S E Z R T F L T M P W A K S Q I Q J K M W F X U C K R W X Q B G I E P  
V R X L I Z B X P J V Y E X Z R H I G Q F N T G A C H V P G J M U M E O E I S Q I R W T B M B Y P C E R W T V Y  
G L R H I C T L W T G A N T V D D N V R N X V Q E Z H W C B V B Y K E S M T V R Y M A W J R D K D O Y H  
F C E B I A M H U S H U R L S L W T A E Z G C C H L X F B K E C D K T K A K U S C W K R W X Q F U E E F N M  
G D I B Q W J G R R X G B C G L R R I M V K I A F X U C K P J G B C Q E L U Z L I X Z B R X J J Z J T H X S A W B  
W I A T I Z C T V N O J A D O M F W Y F V R Z D N B S I I E A R Q E X K H B J P Q D N J M M F F S S V N Y G X N  
F B Q P Q D N A X B S B T R T R R X G O G L W G G D Q P G L U N Q R U K M L H Z R C V B E V Q H H Z G N R  
Q F R R P U I G R W G J Z Q Q H W Y C V V O R P X E G R R E Y U N G I A B C B P F W J C S B V Q B Q C W K C  
G L M Q H V V V P G C M P S F I P W I G I R N W R P Q V Y C G X I F R T E Q X P P F A H U E G C U B G X A G R  
Z R T P N D L A W O P R C E E A X W T V X F G T S G B B M G L R T V Y G X W D R R F Q L P R X N W E I J C C  
J H B V H E Y F K F L S X B S P X V Q E Q N L B S Z W I W C L T K I P V P V P Q R T V B R V F H F P T G A W P  
X B Q C Q P G L Q H X G K E E T W O S C V B I I Y B L N C E E E G R Q H N K V N W J K I C A X A G P S Z O L L  
X V I H V S A U K F T K M O E I H U L Y A E G A H P G K G J T V P C V G R U Z L T T K V P E G G X M G R W T  
Z E G W I C H M I P Y I C T F E G T U G G L N V T M B I I F R J N X F P P U T M J M G J T M B F M F P M N N G P D  
W C Q G W V J R T T M Z W R H G Q T F D H A S G L R D V Q I H N P E I R F Z L T T K V Z E W Q I Y G X I C S M  
A H F P B T B W B R F G T S G B B M V R Z A F N X G Q C A S S E F S G L M W C V R U V L I M P S Z M A C U C  
I T Q Z R H Z C E L T K A V B A V P X W D N V C G N H U K F D P B C V R F V R J A T V R E Y A V Y C B U C H  
N P F Q Y M L M W I F I G J V K X G G C H V R X V P N W I M J S E M K M W T D S N Q B T V Q T V C F R R R V  
N M G D C G V R T V Y C D I M B F S H T T C H H N H J E E G U C H V Z W O I Q K E R W B A P B S X A F S R T  
V G R G H T V W D N Z S A X R T G P X L M T E S Z D F R W B V H R V A C C Y C W M L G I E P R J H X K I E M  
G A K F G X I H F A V V Y Y B B V W Z E Y E F Q I T V R Z E K K D S B U M B R J V V W M G U W H U X U G T  
M B I I B L E A F P M J I M F F S A C C J N B J S Y M R X V A D F J W A M A I K F T V W B P I C V J M U B V T B V  
Z C K G D G A S P Y E K K W L B B V B T R P J M J K K S F S S V N Y G X W T S I E U F L T H N H U I Z Q J R E H  
E S E J H N K M D E A T B V F G T S G B V U L S H T T M B I I B L W V P W P P L B F H G G W I C P G L P L I K V

VLHBWBGLRGERXKMWAXRTECIBBWFGBODMCDVCJPRFXCIAIHYYEIVQRTT  
SIMEWJGCYMQGMBPJYCWECEQFCICPUTSGSFRICPWJSPEHUVKPGGGLWGG  
DQPKMWZTEQGCGEGRGHTVBXUMZVIIGKFP MJMRHHERRXGOHUIECEIPGL  
TVPRUPQIXUANRNIVPHTVRTMIKEEIAMAGLRVFMALBCTIGVYCYHJRBRRYV  
APGUOXIGJVGCMMAIGOFPTLMQHVRQECCXBKBVXCKYIBUSNYQKVLRXB  
VREHFZCCVMTBVGJZQQHWYVWVPKCCWMRGSOGKFTT DSEETGECIPWFXSE  
UPQIXUOQQVPZQIKIHBVJFQTCWPQYGKVQPKMBBXFRVAXYQQNPYAJCRN  
ZWGCNPUUWHPOFEGNVYHMASIIECCWTTZGBJRZGCGMBPIGJZQXLVCGXB  
URWIAIHFIPWIGIROIEYFYFLIZMHNRLVYGCZWIGSSVYGHUWCXXUGICBBOV  
GFRCICPLWFGSBNJBXLKIFWRFKFP MIFRRRYKMNHCOAHYKBCLBASFSZGFL  
TCCGGKRVKGCZQBGSVVNGAETSNVASLGIXIPVXOAZLHMIZYMAIRLSNAWA  
KGJVQTMWCYWGJVADGKSCXFFZQRNAGRHNPURTPBVBVUHGJSHXLOFWHO  
VYBBVWZEYNVTTEWTPSZRLRTKIBQRRVNMGD XFBJVEZCCVGHUIEGZQPEA  
CNFEQRBVKWICSSTVYSXZGGLNVZQDYBSASIGIJDHSSQFLVYCBTVMBTRPJ  
MJKKSOSBMJRWXASNVRVYCLBVRBAFUPQIXUOQQVPZQIKIHBVFVYCXGNC  
FIPWIGIRMZVXRQWRTGPOFEPGIRPBVRVWQCZLUHZKVRQQNQDGMTNHZKE  
GHMZOGSEURLSEQHGPRJRQXMBJV VVKCCHVEHEYKKWDIMBFSHTTCHHN  
HJEEGWMGPQBQSJU YMLXDSEXUGWYRMZSZEVPJRWTBKVRQQNQHXZJRVF  
ORITNXHUIYKFLHLPOEIBHKFTBVHRVAGKGCYZOFXEWTRJKMOAHVIEMGB  
VUGLVUZQSHQBTEQKJQTKDWPIGQKFTFIBQXUGJCRNZWGC P QDKJGQHLEG  
NRPVXE VPRQMC GTTZGLRDFMZBAGGMYNKGAMMRGSJCIBHEQBHBHPZV  
QXKOHWROFQIHXS AWBWIATIZCTVNOJYGXAHVPYNZLJQCBVBBPCWXA IJR  
XEKVB IHXIGAVPUMLLJOFIQUVAJKQHLXBQCQXGMJRVLEYYEMMFVZ RCCQ  
DBVQYYQGUFTEXTHPUKERHTVRSYYNVVEEIBNXVQEQUHZHUSFGNFDA IJR  
RRXVPGNVOHRVZDYRAQBRGBPKCCMAHUMFDFMZVWJR VFOFQIHNHUIZCA  
MGTZSNWBHZLUHZANXVQEQT VCFVXLCEBIAMCCIAUFGVMHBSYUPMJVIB  
HWRVFFTEXGRGHTVRWXUHUIPJR NIXZGNVRFVQXZVSQEEQLLSMPSZEWQI  
BXLKWCPVPVQDYQBSSEORRXHVGRGHTZRNTVRXILEFLRXXHFEEGTMKXZS  
QMAGRAWVPOCXRTKFTMWCYWVPTJJWMRBRGJVZDHSGPHEQDYAEWKSSE  
CCYQEYRIAXZPDGUSAXGJRR TOMFLSAGTYCIIFGMPKGYIXQBNPYAFSCXM  
RVWNRTYCWBV VWOQFIHVLFBQGQJRPKBIFMAIKFTMWCYWQGJAGBJSQLR  
TVGCMPWFFBQBYALWQBRGCZLHLWARUHKT IINBCEMNNJMCUIGVGAGKU  
DKSHRVZKEMAHOMNRQEFLRXXHFMUCMCUHC BQXUCKUWBTSZEA AKCRA

VWPMNPJYGXESYPFEYMDEMVRGJVGGIIFGMPWCYGITOGJBDQDKIDCPV  
ERRXHVGLRAFDIXVZNGXCESCWFFFXNPUGCZWTGLRPVRLHZYCVBVFAD  
EAOAHUQNRWXGKBVXVFETMPSEXBIVRNHCFVRSQIKPMQCAJEQDNDBVHN  
XBRFGCMJIAHRTJRPGLWAKGJVQTVWBPICVJYGXDWGEYVFQTVCFVRTAFS  
GGMHJSEMRLSBUDYIZGERXGOHUIFGKMDEADESCGIJNLWKUMYGKFXLJCB  
OZCPQTXUGYEAUVBIHEOEHFVYCCXBKBVXUZBTHNGRGHTZRNFVGGSSVY  
CIAZSNXFCICRHUWAKSTFKIAMFRXUGJCSTGGFSGJZQXLBVRFUKNATKSGS  
FVRPIVWJRNVNIVMUXIQUWRELPXMGHBSYKJNGXNOPIQDPYHNUANVLQWR  
WXBCBPPQERPVBWAJBTDYIBWBNRQXRPXHCGEIFQLPRXATBVFVGNDKBO  
AHZQICXGNCEQNVZMCPWPYIVIZTTTNOVVYAUCITQZRHYQFIPMBVRXBQC  
QRHDSEIQYYMAXJCBOFERLPGLVNZRDVCCPZWGXRPFBLTVMBJGJVNGHOF  
NQFFZQRNAGRHGJVQTKMGBYEEVQVBDSLHQGRXHVGSSSEHLPIAMFEIFGR  
PRAPSYTSWCYCWACZIGKDCHACABVBWJR XIAOAHGTZAZLIBQXNPXCCMA  
OEIHUVBIHIQPIAVFPTFXVNWBVYCTZSNSSRRPIBKIYEEKDNDKBOAGRVC  
HXIFRMAVIMSNKSQFLHCYBXGHUIGGTFDNZVRPCHLJNXBGBQRVZKTLIQRV  
OKTKPLKCGAUQZQIAMFRXBJVJETVRVRSQIKIAMBRAOKVQPLESYPNUBCTI  
QBTXUGDMGXBSPLAKTYAKMOQIEUZLIXZSFXRFZLHXKHVSAUNFTKMKREP  
VLYAEGANORUFKTFQBBVZQUGUBKOGMBPJRDMPSCVBIIYBVWRRRLRTVQTF  
JZRWGVJBTGQNRRAFSBTGSAGBWERTKQBGLRQGCCLWIEGRYFPAWQBRB  
CNFPXGOHUIBRVLHHCFFPIJQISRWIJMYNDCTMUOACQKMCGLMPEMYNZYC  
MIBQWBOVRXFMGOMMCIPTIMFFSACCGIBMGLSHJRTTMWPREYGRQITTWG  
XYGSCCMBCFTRPUYHFCQUYARRGSMQARSAVYCHXXFBKECDQPLACZIBHL  
QSHSBBAVPXRWXXFBTRTVRXJCSGXRCEBEKWHBGBNNGAEOSGCBWRJDM  
NOEXUGIYCWEWGLSGNCGYTOZIFQEYBHZSFIEKFSHGWHRQNPPMUMPSGSB  
NJGCMPPWFFBQBAPGJSQIFVISRMQJRSEORJXVQCHWVHLQTWQBGLRYIMCZE  
OLWLQLAPGCBVRGGERXHVOYPLDICPDBVRPNYZDNHCIFIGJVQTMWCYWVP  
RLJGQBSSEOVBDKKOEIYGJQBTVBRVSQICMTUDYINETGSXVHNPYAJAPGVW  
AKVRRBSKMGFIFVYYITZSAXLQLPHPQHUNHVKDWMCSJSNRKKTREWYPNN  
NYNLXWCIIHRKMLTZBLSHYCCMPWFMFCGMHLQPVVPMEXVGBYEEVQT  
VCFVXLVFMABVRRBVODCSBIHRPLHFJAHEWAKGJZQEKMNTNGRKJYABAHV  
RTQWYAEBVRXBQCQPGLHUICCXCHPPSEIGJVWPKMQBZRTVBIAQGJELAFSR  
TVGXMCCCJIAMPNGXIIMJGLOAHTQJRGTTQUUXGQZLHMIZYMAIKFTMWCYW  
VHPMJPIBGGUCGRTKQBSSEORRXHVGRGHTZRNTVRBTRPJMJKKSFSVNYGX

BVVWPJRNIXZCSJRTJYCBVHESQWTRXHVHVBXUGNMGELCSMAHFPBTBWBRF  
GTSGBBMNRQQGCCLWIEGRUFDIPIFRXUGTSGKMBGWGCKCDYKCZTHVVPH  
XKIEMGAZQSBAQHWFGUYAHVUJMGJRZGBMTUMFVFPNHNHUIBRVLHHC FPI  
ZQMCBXVHPLNRKCGHXSEEGKEEHRAHRQGQFJHMPWFGUCGRTKKCIIEUKFT  
BUDBVGCEATHNGRXGKEEJIGCHVFGTSGBBMGSBNJWHMMANWFGTSGXTM  
NWCQJQXUTSNXBQCDDKPOEHRPZLVEQBHBFAJRTFAWFHVUTSHLMRNWJG  
CJPLKCAWVFPMPQCAWSQIFPKLSAMAINGCWWKFWLUKCBLASIIECCMEXZ  
OGMAIJWHMMA YIIGCRDHTGNVRTVTXXESQXBQKFTLMPNWVEKMDEAOEY  
KBCPLMQHVVPYVSFQBVGTRRDKAGPVRYPXOMFNRQYZJAUMIFIQCXYX  
GIBQETCZLIAZCHKUQLRIAMQBYEUV MUMPWFFBQBYCWGCHVWQSAWTXH  
RVSKICLTTZFXUGSYHBKGBJGEGGEVWAZYAKTYIBWBFEAFYMLYQFRANNC  
QLHZYNVREFTTKMRUIEGSCUHZSWYZRZLVBVHBM AUKYAEQBTEAFJCMQB  
TYCAFSGHEBBTRPJMJKSSMEGNYAEKVNTGGINDKBGPEAPVPHMPWFGUCG  
RTKLSYZRUUCTIMFVRGQKFTMKDVT FVRAZXADRGVCCJNMPSNTCNZAPMQ  
CAPNAVPPGLDBV GUZRSXAQEMOGRWXQBFXNNCYIBWBNRQWJCHYWFNT  
BTKQRTVBRVJZAWUCWYHFWGRDMPSAIKVTFPIBSEGUCGRTKDIYRRTRZX  
EQHLWPCELTKAHUMFEYYEMMFQIGCZJHTBCBPGJRRJLMGFSZGFDIAMS NV  
YKVPIXKVASYQXWHNKVNWCQIRHVIBAMAISSIMIYRWVVRQIXXTHVGJVPP  
GLOPXHCCJNMMGGWGVQTVCFVXLQWRWXWDRRCQIRHYWIAHGJZQH XKI  
EMGAJUXLAOEQLMEGUXEWYPFERLNHCFJLBNVLTMECEONPUEXOMMBYNF  
VRPBTSQVRRFPIHVOACFGTSGBBMUSYGJRWTBWGJVPUQRAIDGIEPURLHZY  
FRVHWCGLBVVWPJRNIXZDEMZCIGARLSNPFYZRWMP SYSJGIJTOMZFSSVYC  
DLQABHRNRLSAWKGSPCGRJKMFNAQCKYDYNHUIJKICBTVMBJGVJPM MF  
SBNJSHXBVVWOCJGRMMQURBNFENTVRVXFJFUHAWKFRVHWCGLKOA FRW  
JCSMWRVETPFQTTTTZXMAFJMUGMHJSEMZQHNMGVRNFUGIBWBGSGTRAZB  
VUQSJPJCRNZWGCCTFZAXUGPLNRKCGBVHEYFKFLSXBS PXVQEQLBSZWN  
VFMAMPOGYFGJRWXABVJSGIRTVBBPBIPGCMZCQYPGUGCMPSCVRXZMJL  
KVNTGGIGHNASQLRTVRDUCWYHNPVRLHZYVRGTLQXHVRRXREKGDGAMF  
XROZLHMIZYEGKFLBTQBGIACEATTVRBTGKDYANASNVRCCQDWQGPYFUV  
BRAIDGIECEYARAWFEAFDYCTOSZIAVKMDEAHUMFEYYEMMFRBNOZLT LPC  
JXBMVCEMZOPBHJCRNZWGCQCKYPGLZBKVVVDUBKWRRGNPDDKTOGIE  
TVTXXEWGEYUFJDHSGNXGQFJHMPOGLRNGWDNIBNPLBVRWXASPYEKKWS  
TBONRQRLRXMQBNQBTVSHTJZRJBTDYIVPOCXRTVLRKGDGMBPKMDEAGR

RQKEEHXVGXVXVBPMICIEVYCXGBSERRVZQPUQUPSAEVPMPFSFIQCPQN  
XBWGMFDVADFQBTQBTVYCWUCEIBHRPTJCWEIZGERIAMGRXBQCQLBTZUI  
YRPMJXVQECCVPMJKKCZQHPZAPMQCAWNPUDXEMGJMJJRGHVURRPTPNI  
BWBNWJGCJPLKFREGGZNHXKJCRFEYYEMMFJMEGCCHLBCBPFYZPTEMGFR  
RVNMGDAOEIOGTMBBVUDYVVVNDICZNVNPURWXBCBPFKERWBAQUECVV  
PLBTZUIYRPMJFIYRWHTVRWTBOACJKICAXAGAIGYFPZLGHVQDNPPGGIFIF  
CICHXKIEINPURWTBHUIEGRPTGBKVVRNVQHEIBFCBWUMCMSBBANDFSIVP  
OCXRTWMGXVGVGGQFJHMPSGSBNJBXLKIFWRFZLIAQGPLNRKCGPQZYLNRN  
GWDNQBIIFVZEPMDNWDICPDQBFEAFYMLMWDESCGIJNVWZYIPVUGVB  
BOYIUKUCCVMQUECVVPBHZSBRBRVLHHCFFIFQWRLTZSSMACCJNMPWFGU  
CGRTKEWYPTKMCNHCFRWBWIALNCEJVPUGCZWIGQBTVYQHCHBTRPJM  
KKSFSVNYGXDOEMBWIJITRESOWVVVQBTQZVRTNZQILIBQSGJVPXGBSERR  
VSYHXLFRWBWIALIFRMQGERXYQSQEYUFGVBDSNRHOSCGHNKNCVFVZT  
VWARQBTVGCOWZIIQKERWXWDRRFQLPRXUCIIZGERXYGCHWBFVQXKMO  
CTRPUGMTKCZQBPFGACHVPGCGRXVGRWPQERPBGGLRVNMBTQBBTRP  
JMJKKSYMPGEQTLBVRKCNRLSUARFSSVNYGXTWPIAUVQPIXSAHVZSZPLQQ  
YMAWOSCBFQBQZCEBHVWBGEVPJZPLQQAIEKXYIBWBNRQHZJTFIBVTHNR  
RXHVQBQZCEBHYWFGLBUVLTPBCHRZRLSEQBHBNRGCCWQLPARNCICHE  
BGGCKGNDKBBHQOGIQRHVHMAURJXLBWAKBHRJAMPSXRBYENDKBBHQ  
OGIQPLXSEMNPRLDMMHUEGVYGHLMQGMBPZQCHBWAXRPUCSMWPRGBO  
GPTAMBFMIGRLSBAGHFWGTRIHKCAWGCERJILOGICNVYHXKVRGXVYCXTV  
OJIOUZRTYWFGLROFQIVCFEIAVZLUHZANXVQEYEIMBQMKFCCXZOYTRTD  
GHLQCAEAFNYXOMFSSEOTMCMIAWNVVKEEIHJRJBTXCIMQBTTRTDGHLQ  
CAXBUTYCTBVVVQRRPIRVSGABTBMCXBNXVUEMIRWIESJPKFXLQGVRRG  
EBTWBCOIHUVBPLIBRBNNOGJTHVZLEAFZQCHBWAXRPUCSTAOYITCCBDVCA  
RRGCGNTGLWKIAGJQLXZHKVPJADGBOVRFCCGYGMQOYPVUKGCZWTCPHIZ  
LHYWFGLRPVQHNAJHPAGIYQBTWGCFERLCXZRVPWPWJQTWQBPLNRKCGMP  
WFPVUKGCZEWYPAQKZTMPSSZSFVTSKGMBGWVPTCIAMDYYTKEQPKMICHN  
VVBSTQZLXUGECHLCGJIOUZRTLPCHPQDVADGAIYXRFWMGITITMAURBSXL  
OSXRTAYCNIFLGQTFKRHVHRRGURLSHZUNRVBRXHVHUIPFIMBMPOGEPEF  
KETVWRWGJZQQHWYUEFOFQIHNHUIBRVLHHCFFIFGTSGBBMGSBNJMCBBT  
BVRCJWPVKSFWNPUCLBOYPNVZMCMPSQMFZQDKOOAMMGUGCMWRV  
VREKMGBMGYEOGCCSUGHBSYKWRWXZSNVRUVNPKIHRJVNVQUHZKVRQ

QNPGLZVRHZKFTREWYPOGZLIAMWESJPUGGXXKHBVVGJRWXLWEIPVFPNF  
QGPLNUMYGBWIFHEKMCGLIBQSGJVPSHKIZIAVRRXHVGHGUCJPUVAHUEG  
YZJAUMCSKRVPPECGRXUTFSVAGCHVEGRBXGOIFMAIKFTMWCYWJJVLTO  
MFCSFUZZAXBVRXBQCQXGBVVWOQFIPKMDESİKUCSBVFRHUCKNPVSOTIZ  
CEYVXZFCQSQIKPMWTPSHTJCNHCRBRGJRTTMWPRVHPEGCZZSQLNVC GCN  
FHB YFGINBMPSEIQJRRUHTYFSEKXGCTTZLHRUZECXLWGFHVEMLBQBQRU  
NGIAUCFX YKESMOMFFMBPJRWXZSQLNVGYRDIURQNPRET KIIGSZCKCHMPS  
VRFVRJATBWB RCTFATLACSECTFEGTUOAHZCBCHLCFR CBWYYKXIZYXUGJ  
SEIWFGMAIGPDZZOZWNPUQDYWFGLVVZQHBUWYEEVFYLBVRBAFKEQITZ  
NXVQENGHKSFWJJVPTRWINVRILGSXLHUVBWXFIAMDESPGJQVKIDUMPCCJ  
NTVRCVBOGRTWEVRVRPVATLAOECHUZLVMPSETZKJYAFWGG EYYRWHIZS  
SIECSJTMWRBMAIRKPGCOYMAUKYAEIHVSAYYCCRWIAIRFKMHXBQHWGQ  
DGCLBOYPCCIYBXBSEWBTZDPKXASMYGZQCHBOIEVNRZAXNCECBWIBXLB  
FVFHVZMCBLSFGEKSCWHEHBMAUKYAEBVRTEQXPPFUOAYNNCWXYBVRV  
COWGAXQGCVBXZBTWAWZTYAUMLGTCNHGJV DXEMCEGBRPGIYZCZXUGT  
BGHUHUEGEFKTLEWGLGJZQQHWYNRQECGRDWBVXLQLPKXZGVSAQWPEF  
EWYPGCBCRTZSBJGJVPTLBWSCBWLQTTVMBJGJVMIAMFIEEKRRXHVBGJHP  
ZVQLLGBPNTZQWICLNRQUFMCMPSLAVNCNGHJOOPLYFPZPQHUXUGKMDE  
AWAXUKJZDHS PHXGJVGC LBOYPNVZMCBVGGVHEKGDGAANCOGUGUYMF  
RRGAFSRTVFHRZQJRDYBVRXBQCQXGBVVWOQFIDGIZGIEPRRXOMJRVFKFL  
HHNIAMKQIJXGCLFXNAZLVPQHUMAVY CABVIKJNOZJNPQZYGR TKYXGTMZ  
EXGTMBIHVFVNZRNFWRPVMVJNPQHUXUGRAINIZGSBNJMCMPSPHEQDGU  
RWIUEIGKMSHEBYSNFRBXYNSEIAVMCGLQCASSVYCEKWUEEZUFKTHNHUI  
SGRRJKMGQMFELQHXLANCAQKZTL CDCSEVVBQNBWSCBWRPTTACYEEKJY  
UBKWBRNFFMGUMZVIIGKFP MJGQMFVYCDGTMJELVFEDYMSYJEGVRDNAS  
VXNUPMJKASPYEKKWLHZYFXNVZMCCCGGFR CNYGXBVN XGJVGC LBFHGG  
KFLHBVHUMFDFMZPMFRHRUZECXLTBVNUGCRBNWPMZRCCBXVHNXVQEY  
CWGCHQNA YYKXBCQSFQDCPWLWGMBPRJWHUSJSEMKMVXBWGXB YFPZM  
PSCP NVWGMFAGHTCQIRTWIFRPVUKCSTBHUIOGXGCGQBTSSGRAWMWCYH  
RUTPXIBWBREGWCGXVQRMAUKYAEIHVSAOFQIHNHUIGQFJHBVHUMFDFM  
ZPMFRXRUKCSTVREI IKVUTWWBGLRHFJAHEWAKCNRRUHZA FQNPUPPDMZ  
VRHZFLPAXJRGGRQTKQSFTPCEBPVWACEDRICH TZWBPNRKM EPQBQSJUO  
NEKWOAHJKEBDPADESBRADFXODTEQJGVGQOFIEKVQSXAYGSCCEBRHUD

NUNTDYSTTOCXBRZLENBCEZNTZYQEMGVRPQUCPGLQBQZCEBTQIACPRUZ  
RPEQQFEEGLQTWBCQIFKXLPMIFIEKENJMBVRABTUQXGQHNPVEJQWHCZ  
QFRTVNATKSQAVVYRWXDOEMNDCCHHZJNPHGJQEXKWSMPVFDNZWAW  
GCCJPMQCASCYIYBVUFVVKAXDSYGBODYCWAOCTRCIJXDMHUMFUJFA  
EWUVRUQJRCTUSQYRVFNPZMGVDRNZKXMAQBHRNZLTLBVNXJTRNPKMW  
AHRPKCSPQHUEFORJABVRRRGKYMEXGCHIALFWPGLZREEPWPDFBVVWOQ  
FIAMFREEGDYCRUOACZQICIHWFZXUCKGRHCZQRGKEAANLSQYRVFQETKS  
YMZKKYIBWBFYAFZYEHCTMMGZLPWDOAGRKWGSBLBGMAECSSXGCHVS  
CMMGBBSGSBNZFPWZCBQGQTMKXZCAPLOPDPOWFVXRURLSMZWRHGQG  
GRDBVRFRUKMUUZSRHVPVYRAKOGITQIWXFAIEIFQDCLBTZQMSHVPLBBVZ  
CPJFGRXATRIYHICTMWSZEVNDCPMBACACUQNJTMBCEKNPUNTKPOCWGJFQ  
TPQZYQNMVGIBVHBESWKSXMRVXVQEYRDVCJPRFXKTGBGGLVUSMDDE  
CHPQPKZTIWGFMONVUXMPCHXGJVRXKMZR WFGWDDKBBJCTFEGTUARV  
FCCJPKWIAHGJVUDKTRZEXKEEVKMOGSCGEQDNZQRWBHKUPKMWQRNOV  
YUXEPHXJQLJSMFGEVPCWAXIJRXBQDYCRWIGXUCEIHYWFLSHTXPTTBGB  
JGYRPTBLZVORVFRWTVYZCOWJGCXAGCEEVECGZTSARXTRKTKNCEEFUZQ  
IBVUJMGJGPDHNWAKGJZQQHWYNWJGCJPLUWAHVPRWXJIFMAGJQLAQZ  
RMJCJZJLGHECVPRDFIYRHRCUJXGMGNRQOPLTLAIFGBODYCWKSAXRTEA  
RIZCWIPVDYIXAPEMNPTPTWMIEPBTVJAAIHUGBEBYCWUOGXFKJIUBVOYPL  
OPJDOMOAHTTRRXMCRRKBGJRDFGZBZRNPUXYMQLRGJZYPGLRNYTJKCGL  
KOEMACRLSTTOARNYYMHTKFFVJVEVBRHCBGPRUJFDNZGJMGJFSIACGOEAF  
RLSWIRQCGQDYZXBVVWOQFIWTXDRR

## **PŘÍLOHA P IV: PLAYFAIROVA ŠIFRA – ŠIFROVANÝ TEXT**

OE CB IY RP BP YL PX YR YK IG IV OY CP QZ KZ YF TY TC PN QO TS TP NO IG  
AD CP TD NY CN OV AD PI AM OI ZH BC IA ZH NA SH OV AD CP TD NY CN IV  
PX VL TD RU AM IP MZ PU RT CF OV IA HT CZ OI GA VP OI VO BY TC PN YC  
NP CN UN CX PX VL SH UN QO IX YT MH HZ IP TL HZ HN YT WF YI QV SN HZ  
OI FT FV OI GA VP AT NC QA XE RN OE GQ YO QK ZQ WE SH KH TC FV FA YF  
RI TD OG MK AD NB IQ PO RV YT KC ZA LA CK KY TL SI TM ZF FI BA IX NY  
KQ AQ PN SI TM KY NX NY MA RV CV FA YF EX YL SI CE CN ZM ZQ NY UN YQ  
SI OA NG IQ IX FA YF EX YL SI CE IG AD NP GA ZK TY HL IG SI TM TC DQ AM  
AL TR AD CP TD NY CN IP TL IG RI XE KY AD PB AT VK OY PT IY BY UC HK  
NY UN OG CN AD TC HG GO KZ YN AM AD PI VO BY TC PN YC NP AM TS AI YF  
YP BP NG EP IA RG BP YL PX YR YK IG IV OY CB GO AD PI RA WE TY AD TY  
LP BY GC RU YK IG IV OY CB PX TL PI OA ED LH VE OW MT EV ZO TL MT EV  
LA GO ZT VL ZH TL AD NP GA ZK TY HL IG YT KC KN QZ KA OG QO IS WQ NY  
MZ GA BE OV AD CP YG OY FV GO SP TL MZ YP IO TD AI BY OE GQ YO QK AD  
PI EX TD TG HA MA TD NY CN IV FA KN AT NC QA XE RN OE GQ YO QK RI UN  
CO ZK IP GP VP NU NY AH KA NR IA MI IQ BE PN YQ IG IV OY CB OG WI IQ TK  
NP RP BP YO IO RD ZA LA CK ZH TL HO KC LA IX GO BT OG RN QZ QA YQ TY  
GV HT IP HP KY LA FA KH GR PQ OE FW OY TM NH YP MK CF AD IA RG MK  
ZK NB TC RI KI VP NY KY EW CO AN TC AD YK NR XE OI CH PC VL AD NY YP  
YN OE GQ YO QK AD PI TH VG YN QZ KY UN YE TA QZ MA DK YP RD KN IG OI  
KY EW CO AN AD NY YP YN AT NC QA XE RN MF YN ZI QV MK TC ON ZK OA  
TL NP NR IO TR ZA LA CK LZ VK CN YO FP MT AN MY TY VR NY MH GO NC  
MA NI GR TQ ZH TL EW OV IO RD NB BR OE GQ YO QK GI YO YN HZ ZQ WE SH  
MZ OC NK YK ZQ RI QW KW CT YI IO TR LA BY YN OY PE KZ TS VQ CS VK IO  
TK NR GA FI YK TC YP YF YI PN QG YE IG SI PV YN LA PH KN OE GQ YO QK  
AD PI RI KI OY CB TZ GO PH SN CF AD RI QW KC YR OP KT OG BV NI MA SH  
UN ON PC LD IR GA RG KY AD PK YK IA GD YN UR FT CN IY FS PO GO OY YP  
IG TC GI CQ PI OA YL NR XE OI CA CL RA TO CT TR IG RI XE KY OT YN KY TD  
VO BY WF YT BN IP TM NB SI RV CN YQ GA CF RD RA VE AI PW LA GA VI AO  
YL IP QV ST TL EX TD BY KF VP TS QA GA VI PX KY AD CK TC RA XE NU NY  
NH HA XI EQ IA SH UN IS GO YK NR XE NC NP XI EQ ZK TC DO BY AT NC QA

XE RN QA DI ZI YN BN MY CO KP FT TD FA KH GR PQ RA WE TY KY EW YN  
RA XE NC PN EO CO KY GC IQ GP AD TC PN YC TS TY BN VO NY YT MK NR XE  
OI NA GY YP AL CF AD IS TC FW TS RI LA TY FL OZ FW WK KP CN MF ID GO  
GP AD AD NR IQ TP CE TY HN PX BP YQ TR TS VQ CA KP MT NU NR IQ FP CT  
RD AD NR TR RN TI QA MF CD GO SI IO TR KY EW CO AN CF AD AT NC QA XE  
RN QA DI ZI YN IG WG NY QA CN IG AD CK AQ IT IX NY BW VD GR TQ MH GO  
KY EW CO RD RA XE RI KI TY AZ TC GC HZ ON WE PV YN TY FD EN VO NC  
MA TR AD RU NC IO YN TC PN YC NP OI AM RI QW QI EL RT VM NB BR AD PI  
ST OQ YK YI KN WT EX MA CD NR IO TR ZH TL XI CQ ZH YN PH KN IA KA YN  
TH KP YI ZK CK TY AZ AZ PN QK OY CP KI OG BP NQ AZ NR XE NB PF NK PC  
UN AD PI HE NB WE PI TC DO BY YO EL TY FG TM YK AZ PN QW SI YT BR YQ  
TY FH TW TC DO BY LI BY IA RG MK IA BR OV AD CP PG GT CN UC YI CL PS  
NP BY TC PN YC NP QI YN KY EW YN TR NC NP XI EQ PI PI FW YP VB PC CR NP  
BY PZ FT NC RN GI NO FA KH GR PQ AM TC PN TL NB IA KP AD YP UN YO BR  
CN IV GO QP YQ AZ PN SI FL TC AM ON PI GO ZF AQ CP PG BV IO YK OY NC AI  
KA NR FM FI TS VQ AZ NR XE OI AH TL ZF AG HZ PI KN HZ AL NU NY TS EN  
OY QA BC UO NY PC CR NP FA MA LY AI VO AQ HA AD PI KY EW CO AN BX  
EX MZ TR OD NP TY NA FA RD PX IA DI FA KH GR PQ AD NY CK OF DA KP OY  
YP QA NO GR TQ LH AM EW QZ KY LD SH IP YN CN VI AR PX TY LV PM CU  
AM YK IQ RP CN PW LA BR OV IO RD TC IA OI CF QV QV KN OY RL WP PN PH  
OI HE TC LA TS VQ TC HO TL ZK TC DO BY KY IA RG MK AD NR TR RN TI LH  
AM EW QZ KY HT TL PN YF CT KX YK ZK NB HZ ZQ WK YP WF CT SI QV KN  
UN QT MI IQ BE PN YO TL CN IV GO UB OG MF IF NC RE AD NY CP ZH MK AP  
GE AP FH OG EB IG YN TH NY LA SH IO QA DI NC TX NY QT RG UP FD NA BY  
SI CE AT NC QA XE RN GP RG LK AD YK YP YN AD CU TC GT ZM ZQ AZ PN SI  
FL TC AM ON PI GO LA BY TC GI KY EW CO AN NK OI RP DI NC SH ZH RN NO  
PO TL AM HT TC GI CX TC GT ZM TR SN TH WF CT LA YO IA YQ TY LV OI VO  
KN SH KH RU NC XC OI VO NC TR KX TS OI RA BP YL PX YR YK IG IV OY CB  
GO CF TL IX ZS IX NU NY AD CB IY ON CK PO YL AD PI CF TL IX QZ KY NX NY  
KQ PS PE TI BY MT TR QZ ZS OY RP DI BY TC PN YC NP TC GC HZ ON WE PV  
YN TY FT DR GO TC DO FA MA LH AO RD TH AM ZQ NY WT RN IA AD CK TY  
LD BY KY EW CO AN RI QW KW CT AN PI ST OQ CU FA KN TX NY TS VQ AD  
PK GR PQ AM ZQ IO QV VD TM PN LD IX OY HL MT EV ZV CT UG NR PZ KY QI

LA AT NC QA XE RN OE GQ YO QK OY YK IO QV QV MT EV ZV CT RG TV CA  
SH UN ON PC LD AT VP CF TL IX KH HZ NB KY EW CO AN IA RG MK TC NU NY  
ER SH TI NY TW YP MK AO CR KV BN FB NK IB VK FA TD ZH TL BW QV KN UO  
ST YT IO TR MH GO AD AQ CU GA SH UN CN UN OR EX YT VE OW SI YF TC NR  
TR PN TD LA FA KH GR PQ RI UN YQ QI LA IG AD CK PO GO OY YP QA MF CD  
GO SI IO TR KY EW CO AN TY LD BY AT NC QA XE RN IA RG MK RA WE TY ZK  
NP AG NK AK NR XE NP BY LI BY YF PT PN YQ OY NB YK OF CN HT OG VE LD  
BY SI OA NG AM IF TK TC YK IG TC GI CQ PI OA YL NR XE OI AH TL UP ER TR  
RN TI ZH YN RI UN YN FT CN IY FY SH TI NY AD NP GR TQ MA CR KV BN GT  
TD BY GP RG LK NF OG SI QV QT CM GO TS PH MT UP UR TN OC TR KC TD VO  
SH PN UN YE TR NR TY TP NO FI OT PI CP YT QV SN PX CN UR FT ZH IE TY LD  
FA KH GR PQ MY GN IQ IA LA OY PV MA RD AD NP GR TQ LH YK RY PF NB BY  
YN TC AD AM GP RG SP MK IR TR IP TC QZ QA KC KX FI LP VP GO OP MK TR  
HP MA RC NP XI EQ PN CQ TC TQ GQ AH TL RI CR PB AL AF TZ CB PX TL AD PI  
ZF TM CK TY NA NR DY FI OP YL OY CU NK VQ MY GA RG KN FT TD BY OC TP  
NO FI VK OY TK PI GI CQ QA YO OU TK FI PI OA YL AD NE IG PN TV IY SP EV  
TL NY LA TY FT RD IG AD NC NP XI EQ OE AI IR TQ ZH TL GA VI BY CZ GO LP  
GQ NP BY NO GQ NP RA XE TC GI CQ PI OA CD OG KI AO TD PI AT AO TD KE  
TL NY LA TY FT RD AD YK NR TR RN TI ZH YN WT IP VD AQ NR XE TC HR PX  
YC NP XI EQ TY FT KI KN KC TD TC DO BY KY IA RG MK OE AT NY SN QA ZF  
TM NP FA KH GR PQ SI AZ RU CK KM TY PN LD IX OY HL AD NC NP XI EQ MA  
BN IG KY EW CO AN QI LA IG AD NP GY YP AL OY NR IQ TC HG OG LI BY YN  
AD YK NB HA QZ QA AD AM AM AD PK YK IT ST RN IA LA OY IN TX NY OH RP  
BC IY SZ NR XE OI NA GR TQ AM OE CB IY NB HE HZ WK WQ OY RA DI BY IA  
RG MN TR IP NI TC GI CQ PI OA YT TL ZT CO PX QY YK PX YR YK GI YQ EB UO  
GO IP TL QI YN TC GI CQ PI OA CV FA KN OF TW YP HI OC SN BN IP TM NB QT  
RG SP OV AD NP GR TQ MY TX NY NB ZF TQ PK GR PQ MY TY TY FB TZ PK RU  
NC XC OI VO NC TR SI CE IG AD PB OG QO IS LH AM EW QZ KY LD BY KY YN  
QA XE RN QH TW NE PX AT IO TR MH GO BW NO BY OR YN KY OY YF ZG NK  
IB VK TY HL IQ NP FW YK BZ QI OG ZK IO AK TY LD CO EM ZH TL IP RD NC AL  
OY PE KY LD AP RW RN TD GO CK AB HZ AW YP YT YN PA BI OY IO EW ST CO  
KI GO IP CR NP BY KY OY CP TD OG BV RN FD CH ST KC NA BY PN YF PX YG  
NK IB VK EN AL IQ NP FW YK IY NY FP IW HZ RI IV GA AM AD NY NP AG NK

TP TL TC GI CQ AD NC CU FP YK HZ UC QV ST KL RU PB TC DO BY QI YN PN  
YF CT YI QN YP BN YQ TC PN YN LA NB TC KY NI OA YL ZF NY CU YP NI ZP  
QV SN SI UP QA KC WF RT CQ TG FM FI PI OA YL IA AD PB OG QO IS RI BN BY  
YN KY KF KN LA BY BN CT UY YL RA WK HA NC RI VE PN CO TD BY AT NC  
QA XE RN XI NQ FT CN UO QT CO RD AD RP BP YL PX YR CU GO VL RA VX TM  
VQ KC UR IL TY NH TW NY KY GE TM VQ OP TD TY HL IQ NP FW YK FP YH OR  
YN BP YQ TR TS OI PC ZA PX SH UN IA KP TS YP LA TS OI VO KN KP TD VO AQ  
BP TL HZ KW YF VE TP TF IO KC TR AD YK PB OG QO IS ZH QZ QA KC IG ZK  
GT LE IX TC DO BY OE AT NY NP OM EP OV PN TY BT OG IA RI MV TM VQ BR  
AN PX TS AI HI NO BY YO TL CF AD BC UC CG ST KC QA YT QI YN KY CO PX  
LY AI CK TY RA DI BY IA RG MK TC AD AM GP RG ME TY KP BN LA EX NI TW  
RP CQ TS FI OA ZK FM ZK NB TC AD CU OG RD ZI AZ RA WE TY VE TC PN TD  
OA YT QV SN GE YP LP BY ST CF HC PX ZV KY AD YK NP GR TQ MA YT EV CT  
CD GO KC GT YR OY NK YK ZQ SI RV CN CG GO RU IS TK YP RW IF BN TD TS  
VQ AZ YI RV CT RD OT TH VG YN QZ KY LA SH IP YN TD RA XE MZ OI SZ IH  
CK TG RP GW GW DM IS NE CF QV ST MV HA KA OT PE TI IX OY CE PX ZF NC  
AD AM AM PT AQ ZQ PF TM OI RA BP YL PX YR YK NR XE OI NA GR TQ TC BN  
WO QW KC FT PI NK CH TQ VQ IX TC DO FA KA YN HI RN AM TS AM IO RD IG  
TS VQ AD NP GR TQ ZH TL AD PB OH YK ZF NY NP BY AH YN RI UN YN LD FA  
MZ HA ZR PX YI YL MP TP QV VD BY HP EM QO PX TL TY FH AQ ON PO HB OV  
IA TC LA TS VQ TC DO BY IA RG MK FM RA VX TY IN SH TI NY TC GI CQ PI OA  
YL NR XE OI AH TL AT NC QA XE RN QA DI ZI YN AD AM YF PT PN OG GW BC  
YQ TY TC ON TG WE IO TR IA AD CU GO VL IG TC GI CQ PI OA YL NR XE OI AH  
TL AT NC QA XE RN QA DI ZI YN AD NR XE RO NC AL IP PN IG RI KI VP NY KY  
EW CO AN AM FT MY ZK ZQ NB TS TR FX OI SH GE PC GB AM IA YE IG AD RP  
BP YL PX YR CK TX CK NC IN SH TI NY AT NY PI TC HQ AZ PN LI GR TQ LA FA  
MY SH TI NY RI UN YQ AD CP KI GO IP CR RP HM NP VO TC BX AE PX YQ NR  
XE OI NA GR TQ ZA LA CK HZ ZQ NR XE NK AH KA AQ ZQ PF KN PI GR TQ GI  
YG OY BN CT RD MT EV ZQ AZ PN QK AM FT MY ZK ZQ NB HZ UC QV ST MY  
TR MA BN YO IO TR MH GO SH NG NC TC FX TC GT ZM ZQ AZ PN QK ZQ NU  
NY TS AT NY PI TC HQ AZ PN QM NU NK IA RG MK OY NY NU PC UC LD GR AI  
BY KY HP MA NI GR TQ ZH YN MT UP HZ NR XE OI AH FL TC AM ON PI GO QZ  
MY YN VF CO UN YO TL CF QV KD PE KY HT HO TC TY HT HO TC AD OG XB

GA VP VO BY RI XE KY IG AD AM GP RG SP TL RA XE OA FE SH TI NY MF YN  
ZI QV MK AD PK HZ FI QA DI EI OT RI QW KW CT YI IO TR ZH TL GA CM OC CU  
TS VQ MZ GO SP YN RI UN YN FB NY PK CB GO CP WK TO RD TC IA TC LA TS  
VQ TC HO TL KY OV IO RD EB RA XE IX RT BP YL PX YR CB OC CU TS VQ YF  
PT PN EO GO AL YI RV CN YQ AD AM YF PT PN NG NK UN LH RU PB NY TC IA  
AD NP EI OT LA IY UP KA NR OP QV SN AD YP OU TK FI PI OA TV HA NY TY  
BT GO AL OI BN MY CO KP LA BY TC LA TS VQ PI OA YT TL ZK YK GI YO TA  
NO MY TY VR NY ZF FI BD WP VL KZ TI AI BY CN VO YF PT PN YR SH TI NY  
WV VT NY PH TM OI AZ YI RV CN YQ AD AM YF PT PN NG NP PO MK PI GR TQ  
AD PI ZK YK ZQ IQ RP DI BY UR OY MT NY PN YF RT QT HR KZ YF HZ TA NO  
MY TY VR TC HD VP VO PS YK OI HZ PN IB XE AD NY TY HT NI ZP QV SN PN  
LA LA BY KY EW CO AN IG AD RP BP ET GO AL GI VE LD FA QZ KY EW CO AN  
MZ AM ZQ OY SC LE FM CU TM VQ MY TY RA XE ZF TQ NC NP XI EQ TY FH  
TW NE PX TH NP PO KN GN PB GO IA YT CE KY EW CO AN GA KN LA SH IO ID  
TC HL YF PT PN YC NP XI EQ LY FM WG NY LA FA MY SH TI NY OE FW OY TM  
NH YP MK CF AD AD NK IX NY KN UN MK IG AD RP MA QI BN ST TL GA VI IR  
PT PV YN YO VF PI PA GW DI BY CF YN SI CE IG AD NK PI NY IA RG MK ZK NP  
FA KH HZ FI PN YF RT QT HR TY FT AL GA ZM GA ZM CT GW BC YQ YI ED PE  
KY LD TG OP DR AQ YP QV ML TC HL IG CN IV GO MP QZ KZ YK TC TH VG OI  
OA TD AI YO EM TC HF IX YL NR XE OI EA OG DK CK MY SH TI NY TC ON ZK  
OA TL NP NR IO TR ZA LA CK ZH IA RG VD SH PV KY LA BY LY FM WG NY PN  
YF RT QT HR TC ON TG WE NB TC AD PB YN WT PX MY SH TI NY AM ZK NB  
BY YN IA KE TM HT CN IV GO MP TD EX MA TR BN PN NI OA YL AZ PN WF YL  
IP QV ST IO TR SI TC PN YT CR YP TL AT IO SI KV KY OY YP MK TG AM EW QZ  
KY FN SH TI NY TY TS AZ AM TY FL TY OH CK NC OV IA RG MK AD AM YF PT  
PN YN ZO WF CN ZS IX IA UP UR TI YO EM IG KY EW CO AN HT IP ZO TL QT FO  
PN GW MF IF NC DV CH GO ST PN OR YN WT CU OI TS QA QT RG LK PI VO GR  
TQ LA SH AD NK AE PX TY TS AY NP BY KY EW CO AN HT IP ZO TL BE IO IO  
YT QI YN ZK PH KN GI CQ PI YF PT PN YN CR YE TI OA TD GR TQ QZ KY TL TC  
HQ NC MA IO UN HT IP TX NY AD CP TD NY CN IO ZH FP FR TR RN YC AD YK  
NB HA ZA NP OI AM KP RI WF RD QI YN TY FL GO RP HI YN KX OC CK NC OV  
AD YK NP GR TQ MZ TM VQ BY KT RA EP CR YE TI RA XE RI QW KW CT YI IO  
TR ZH TL MF KN MZ OI SZ ON TR BR CR YE TI OA YT MZ NK VQ HZ RY YP PN

OT KY NW TE MY SH TI NY CF YN KN QZ LA GR TQ MZ OC NK YK ZQ CN IV  
GO LK OY PK NR IQ TC QX WP PN TA BE ST YO TL AD NP GR TQ MA TD FA MY  
SH TI NY CF QV SD NK AE PX SI UP KZ YN AD PI TY CZ OC NK YK ZQ CN IV  
GO LK RA XE RI KI TY EZ KY ZH YN KY EW YN TY LD SH OV AD NY YP YN TD  
CF YN KN QZ KM TY ZA PX GT TD LE IX PH PX IN SH TI NY GI YN YL FI IA RG  
MK AD NP GR TQ LH AM EW QZ KY FT TD FA MY SH TI NY CF QV SD NK AE  
PX TC UN LA OF PI PB HZ PD YN PS TC ZH TL GA VI AT OG BP NQ ER TQ VQ  
NR DL OF OI TS NU TF NC RN YF PT PN CQ GO RP RT BP YL PX YR YK IG IV OY  
CB TC TS VQ NA FA MY SH TI NY CF QV QD TW NE PX YN QA XE RN MH GO  
MF TL TC QG VP QI YN PH PX IA BP YL PX YR YK IG IV OY NU OY OA ZK UP  
CZ PK MA PN KQ PO MT RD MT LA ZH TL AI BY CO TD NY CN PD HZ NB YN  
QA XE RN ZH YN TF NC IO MF NB TS QA OF TW YP EV KF NY IG ZI AZ IA KP RI  
KC QI YN TC XT VN NB TC AD RP BP YL PX YR CK TX CK NC IO HC PX QA BN  
MA YN PT UO NC FT ZO RI QW QI RT BP YL PX YR NK FI NC KY MY TR IP TC  
LA BY IV IQ PO RT BP YL PX YR NK FI NC KY LA BY BO ST TL HK HL IG IV OY  
NK FI NC KY ZH OU BP TL OW GU HP MA NM TC VZ VE OW RI QW SI TL MY  
TR IP TC KH HZ FI YT WT HO IO TR TY FG TM CK TY OT VK PI OA CR IQ WQ  
TY HL GI NO GA KY CN VI PX CT ZO TL MT EV ZO OU BP TL OW IC NK VQ LE  
IX TD EI OT UO GO DT WK KP YQ RI TD PO YL TS AM IO RD IG TS VQ AD PU  
RT VC TA NO EV KF NY ZH KA NY OP YT RT PN AD PI VO FA QZ KY NI OA CT  
LY AI TC PN TL NB IA KP RI KI YN BY YL TW YP TL AM ZQ EK PC NI VO IR TR  
LA TY PV TB PI PB KN HZ NR BY EM AD CP TY IZ PK MA PN GI NO BY QI LA  
EW OR YN TD TC GI CQ PI OA YT OU BP TL OW FH NC NY TS BP CQ AM ZQ OA  
YT TL ZI TW NY GI CQ RI TD PO YL PI CK TK PI CB GO BR OV IO RD BP CQ AM  
ZQ OA TD AQ YI YT AD OC BT OY AN CN IV GO QP CN AD PI AM RT AN PX OG  
VC AD AM AM TC PN TL NB IA KP ZK NB HZ TY RU IS TK RP TV AH TL AM RT  
IO TD NC BN HT ZH KN HO VL IR WK NC IP OU BP TL OW NC YK ZQ ZK TK XB  
TC MY TR IP TC ZH TP NO OP QV MT LA TC QG BI KV FO YL GI NO BY CN QZ  
KZ LZ VK CN YO FP MT AN MY TY VR NY FT MY ZK ZQ NB TC YF PT PN NO FA  
KM AM IO RD CF QV VT AI KP AD CK AQ IN XE RO NC AL TC RN AD PB KV FO  
YL OY PE TB PI NB VG PO SN AD NC YK ZQ ZK UC HK OI YK GA VK FD NR TR  
KZ VD NB GI EO KV FO YL TH VG NB IH PN CO TY ZP YE NF OG WI TR PN TD  
ZH TL GO HO CT YH IO TR AD NR GN IQ AD PI IY WR IQ TP CT YK AD AM GP

RG SB HZ QI LA IG AD RP BP YL PX YR YK NR XE OI NA GR TQ QA CT ID GO  
YP ZA IY WR YK ZQ TY FT YL IP QV ST IO TR AD NB AM MP QA OQ TY AW NB  
TC IA FT YN NI GO PC KM PH NK NB HE IA RG MT DI BY YN OY YK PB OY PI  
CB TM YK GI CX TC GT ZM TY LV TC VZ AD NE CF QV KD CP TD BY OC IX TL  
OC NR IA CO YK AD NB OC NR IA YE WF MY SH LZ OY OA ZK GN TW NY ZH  
TL AI BY NG IR WK NC IP IO TR KZ YF HZ CG YM AD PI CF QV KD RP GH NC  
NY TS ZK NP GY PX HB RA XE RO YP FT RD ZK TC DO BY IA RG MK ZF NC NU  
NY TA QZ MA DK NP BY IA RG MK TC AD AM GP RG SP YN OE TX TF NB TC  
YN FB PI TP EM OH CK TY OH NY RO IK GI CQ PI IG RI XE KY RA VB TR AD TZ  
NP PG NY VE VR TC QO NB SH DV TC VZ IA ZK NY IK AD NY NB SH ID TQ LK  
GO OF TC TS VQ NH YK OF CN FT PD VP RT CF IN IQ YK CF AD QI LA MT EV  
ZW NY MA TR LA BY YN FB PI TP EM OH CK TY OH NY PZ IA SI PN LA BY TC  
LA TS VQ PI OA ET OG RN QZ QA HI OE GQ YO SI TL SI UP QZ KZ YN RA ZB TZ  
YP QV VD BY KZ OU TA NO TC BO OG QO IS ZH TL QA GI NO FA IO QZ MA WF  
ST NO AP CF TL IX MA YL IP QV ST IO TR OE IR YK ZQ ZF NY NE PX OY RB WP  
BN LD GY PX HB AD PB OG RN QZ QH YO AB FI TS VQ AH TL OE IQ TI NB ZF  
NY NC NR YK ZQ OY EZ MA RD AD NY IK AM TS QI LA TS ZI AZ OE CB NY PH  
KN IA GT TC HO SI EV TS TC LA TS VQ PI OA CV BY CE PX CN UR LD AQ NP  
EW LA IQ TC LA TS VQ TP YO KC PN YQ GO FM OY IK MF KN AM RT IP ZT TM  
PH KN GI YE PX NG AM ON PF VP OA CT BN MY CO KP GA VI AO YL IP QV VD  
BY OE GQ YO QW SI EV TS VQ CA DI BY EO WM TM CP KA OG WT BN HL FW  
TK NH IX TV AP LD BY MF KN GO RI AE OI GC IQ AD NR GN IQ AD PI RI KC MZ  
OI DA FA KH GR PQ TY FN MT EM TR OI RA XE UN YQ OA RT GC IK CF QV VD  
PS NR OY RP DI BY YN LA FM RA VZ ZK YP CE IG AD RP AD NY ZT CO PI OA  
YL IG VE OW HK HL TQ OY AM BA VZ TY HL GR TR AD NE CF QV KT OG HP  
DK CZ GO MU OI DA BY IA RG MK TC AD AM GP RG UK VP VO BY TC LA TS  
VQ PI OA CT YL ON WE IO TR KQ HA KP FT GW BC YN TD RA WE TY EX CL AQ  
IA DI BY IA RG MK TC AD AM GP RG QP YT VD NY YT IO UN UN YQ OA YL IG  
VE OW GO MT EV ZQ IP CA RD CF AD TC AD NK TC VZ HI WF SN CF QV MN  
NY IP TC SN SI UP RI KI PI PF TM OI CS GO NK PM NK CZ OI DA BY IY PV TS IA  
RG MK TR AD NR GN IQ FM RA ZB TZ NP TG IX TV AP HT FT GW BC YN TD UN  
YQ OA RT DI BY OE GQ YO QK IQ RP DI BY BC PI XE YK FT MY ZK ZQ NB SI EC  
AI KP KZ OU TA NO NB KE IO HC PX OY YP QA ST CO ZH MF IF TR TH GR GO

KP MT NU NP SH PD LH AM AD RP TV CZ HA IA QG BC UR MD YN UR IA ZK CP  
IP ZA PX YQ NR XE OI CZ GO LK IP IO TR PW LA KP IZ OY NP SH OV AD CP YL  
ON WE IO TR MA TD FA KH GR PQ UC YN BN MA DR NB GI YO KA NR FM FI  
FW TK CK NC IP IO TR TY HN PX SI AS TZ NP TG AQ IQ YP GV FT IO TR TS GA  
KC XI EQ IA BR IO OV IA XI EQ AD PB ST ID GO QK ZQ EB UO GO PN HT YN MT  
LA NB PI VO BY KP FO RV CT RD IG YP YF IA RG VL YK RY OT IO TR YN BC  
YN CR CP YL IP QV ST IO TR QI LA IG AD NP GR TQ MA TD FA KH GR PQ UC  
YN PN LA NB TY GN NU PC UC GT TD BY GI QV QT CF RD TK PI GI CQ KQ TY  
GN PS NK TC VZ TR HS TU NR ON HZ NY PC KA YI TL IY IQ TP KO YN ZH CO  
TQ PT IA IU TC GT ZM UO UO OG TY FV TC GT ZM OE GR TR IY IQ TP KO OG  
MA DR OP KY CO YK BN KL IA TP TL RI KI OS OY SI HT ST TI AT TC BE IA NX  
OY OP DK YK TC RI BN TY FN IQ WQ TY BN ZO KI KN MA IP MT YM OY PE KY  
LD TG YK OF YT PN ZK NY TC BE OV AD CU GO HL TC OI TS FI QZ ZS PX VL  
KP YN TK IY NB CF AD AD NU OY OP DK YK GO ZT KV YK ZQ BP IF MF NI AR  
PX CO YL IP QV ST IO TR AT NY PI TC HQ AZ PN QM NU NK RI QW SI TL ZH OU  
BP OY MT UP AD AM ZQ ZQ DS VQ GQ TC GA LA YT KC BV NP AT OH YK AW  
NK FW OI MY TG NK TC YK AD PI XC PT OY CP TL NC PN FV OI SH KQ TS VQ  
TC BN TD AF AT NE PX NC OA AH TL KN OY CD OG LI FA KH GR PQ AD NY YP  
YN SI CE SI CE QI YN IA RG MK AD PI FI PX VL TD TC NM VB NB EP IA KA IY  
NK FW OI PI OA YL TY FT PT TQ GQ AW CP YT LN TY RN FM TF TF TD TC NM  
VB NE PX CG TZ GO OI NP GR TQ AF TH OG RG LI IR TX NY TR SN SC HI XT CO  
PN ZH TL ON PC LD AT FI LP BY KP LA IG GE RU NB TC YP YF YI PN QG YE FW  
KZ YN QA KC CF QV VL FM WG NY CF AD SC YF AO RN MH RU NK GC RU NP  
PR SI TM KC PI VO TR AS IX KN OV IA OQ TY BT NY SH AK AD AQ CU TM VQ  
SI UP OI TC IA IH VP XE RU NB OI OA YT EM RT VM NB FQ NC AL AD AM GP  
RG MU PX VL TD KP TA QZ MA DK CU OI GA VP VO BY IO YN KN QZ KY GW  
GI NO QA BI OG QO IS WQ NY ZH QV ST OG VE LD BY XI NQ FL PS TC QR QO  
YP IA BP YL PX YR YK IG IV OY CP LT IS YP BC UF VP XI VK FN NY IP TC SN  
KN TZ NP GR IQ TY RA VP VO SH EL MH GO RA XE QO YP AL IG IV OY CP LV  
PM NP AI SH EL SC KE MA CN QZ KA OY DT NY DQ NC VR QE IS NY GI YO QZ  
MA LA TC FX OI BA OG RG MF RD AD AM GP RG SP MZ NK VQ HZ WF TL TC  
DO BY KE MA CN QZ MZ FA KN FC HZ KE ZA ON CA RD IA SI UP BN TH MT CN  
ZH TL SC CN QZ KZ MY IQ WQ TY FN NC PN YC RW EI OG PC NI SI PN KH CO

TY RY NB PE NQ GO NK VQ SH AD RI EM TY FL PI VO MA KL MF YT QV SN SC  
QT UN TY FH YO IO PV BN QG YK IA SC QT UN SN CF BC RE TD FA OZ TY GV  
HT XB DA NY MY OY TC OZ TY HT ST RV YT ZF AQ IY CO MF RN FN PX TD KN  
QZ ZS PX YQ CF AD PX AD ZK HP TL TY GV HT GV HN IA SI UP AD AM GP RG  
SB PT UO NC