

# Využití metody přeskokování písmen pro hledání šifer v textu Bible a její analýza

Using skip code method to search sipher text  
in the Bible and its analysis

Karel Koplík



# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Karel KOPLÍK**  
Osobní číslo: **A08597**  
Studijní program: **B 3902 Inženýrská informatika**  
Studijní obor: **Informační a řídicí technologie**

Téma práce: **Využití metody přeskokování písmen při hledání šifer v textu Bible a její analýza**

## Zásady pro vypracování:

1. Zpracujte literární rešerši na dané téma.
2. Seznamte se s metodou přeskokování písmen.
3. Naprogramujte vzorový software (v libovolném jazyce), na kterém budete demonstrovat využití přeskokovací metody při hledání šifer v textu.
4. Pro text Bible a další vybraný text proveďte analýzu této metody a podrobně ji objektivně kritice s využitím teorie pravděpodobnosti.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **PETZOLD, Charles. Programování Microsoft Windows Forms v jazyce C : vytváříme uživatelské rozhraní aplikací. Vyd. 1. Brno : Computer Press, 2006. 356 s. ISBN 80-251-1058-3**
2. **DROSNIN, Michael. The Bible Code. London : Orion Publishing Croup, 1997. 240 s. ISBN 07-528-0932-6.**
3. **Torah Codes [online]. 2009, 2009-01-18 [cit. poslední změna 18.1.2009]. Torahcode.net. Dostupné z WWW: .**
4. **ANDĚL, Jiří. Matematická statistika. Vyd. 2. Praha : Nakladatelství technické literatury, 1985. 346 s.**
5. **CYHELSKÝ, Lubomír; KAHOUNOVÁ, Jana; HINDLS, Richard. Elementární statistická analýza . Vyd. 1. Praha : Management Press, 1996. 302 s. ISBN 80-85943-18-2.**

Vedoucí bakalářské práce:

**Ing. Bronislav Chramcov, Ph.D.**

Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce:

**25. února 2011**

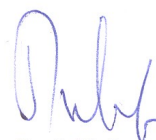
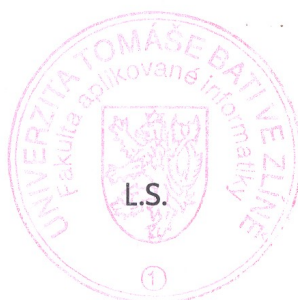
Termín odevzdání bakalářské práce:

**7. června 2011**

Ve Zlíně dne 25. února 2011



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



prof. Ing. Vladimír Vašek, CSc.  
*ředitel ústavu*

## **ABSTRAKT**

Ve své bakalářské práci jsem si vzal za cíl studovat metodu přeskakování písmen v souvislosti s jejím použitím ke hledání šifer v textu Bible. Šlo mi o objektivní reakci na fenomén The Bible Code, který je šířen do světa newyorským novinářem Michaelem Drosninem, jenž zpopularizoval také výzkum prof. Eliyaha Ripse z Hebrejské univerzity v Jeruzalémě. Částečně se opírám o kritiku prof. Brandona McKaye z Australské univerzity v Canbeře, a částečně se snažím o vlastní reakci, při které jsem provedl statistické výpočty a naprogramoval software použitelný ke hledání zmíněných šifer a automatickému spočítání souvisejících statistických výpočtů. V poslední kapitole demonstruji na ukázkách, že takto nalezené šifry nemají žádný směřodatný význam, jelikož se vyskytují přirozeně v každém dostatečně dlouhém textu.

Klíčová slova: Metoda přeskakování písmen, Kód Bible, pravděpodobnost, statistika, kritika

## **SUMMARY**

In my bachelor thesis, my goal was to study the skip code method according to its use to search a cipher text in the Bible. I was trying for objective reaction at The Bible Code phenomenon which is spread to the world by New York journalist Michael Drosnin who also popularized research of prof. Eliyahu Rips (Hebrew University in Jerusalem). I partly rely on criticism of prof. Brandon McKay (Australian University in Canberra) and partly try for my own reaction which includes statistical calculations and developing reference software usable to search mentioned cipher text and automatically count related calculations. In the last chapter I demonstrate on samples that cipher text which was found by this way, has no relevant meaning, because it can be found in any text which is long enough.

Keywords: Skip code method, The Bible Code, probability, statistics, criticism

## **MOTTO**

*„Vědec musí být ve všech ohledech jako dítě. Když něco vidí, musí říct, že vidí právě toto, nehledě na to, jestli to bylo to, co si myslel že uvidí, nebo ne. Nejdřív se dívejte, potom myslíte, a pak to ověřte. Ale vždy se nejprve dívejte. Jinak uvidíte jenom to, co jste čekali, že uvidíte. Většina vědců na to zapomíná.“*

*Douglas Adams*

## **PODĚKOVÁNÍ**

Na tomto místě bych rád poděkoval Ing. Bc. Bronislavu Chramcovovi, Ph.D. za věnovaný čas a odborné vedení mé 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 užit 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>11</b>
<b>1 LITERÁRNÍ REŠERŠE</b>	<b>12</b>
1.1 ÚVOD DO BIBLICKÝCH ŠIFER.....	12
1.1.1 Okrajové metody výkladu Tóry.....	14
1.2 MODERNÍ HISTORIE METODY PŘESKAKOVÁNÍ PÍSMEN.....	16
1.2.1 Eliyahu Rips.....	16
1.2.2 Michael Drosnin.....	17
1.2.3 Brendon McKay.....	19
1.2.4 Řešení záhady jménem Kód Bible.....	19
1.2.5 Shrnutí.....	21
<b>2 METODA PŘESKAKOVÁNÍ PÍSMEN</b>	<b>22</b>
2.1 ŠIFROVÁNÍ.....	22
2.2 DEŠIFROVÁNÍ.....	22
2.3 POUŽITÍ K VÝKLADU BIBLE.....	23
2.4 PROBLÉMY SOUVISEJÍCÍ S TAKOVÝMTO VÝKLADEM BIBLE.....	23
2.4.1 Použití výpočetní techniky.....	23
2.4.2 Důvěryhodnost původu šifer.....	23
2.4.3 Podoba prohledávaného textu.....	24
<b>II. PRAKTICKÁ ČÁST</b>	<b>26</b>
<b>3 VZOROVÝ SOFTWARE</b>	<b>27</b>
3.1 POUŽITÉ PROSTŘEDKY.....	27
3.2 VNITŘNÍ POPIS.....	27
3.3 VNĚJŠÍ POPIS.....	30
3.3.1 Hlavní a kontextová menu.....	30
3.3.2 Klávesové zkratky.....	35
3.3.3 Systém souborů.....	35
<b>4 VÝPOČTY</b>	<b>36</b>
4.1 PRAVDĚPODOBNOST NÁLEZU VÝRAZU NÁHODNÝM VÝBĚREM PÍSMEN Z TEXTU.....	37
4.2 ODHAD ABSOLUTNÍHO POČTU NÁLEZŮ VÝRAZU VE ZVOLENÉM TEXTU.....	39
4.3 ODHAD ABSOLUTNÍ ČETNOSTI NÁLEZŮ VÝRAZU V TABULCE.....	40
4.4 ODHAD ABSOLUTNÍ ČETNOSTI MATIC S OBĚMA VÝRAZY.....	41
4.5 DŮLEŽITÉ POZNÁMKY.....	42
4.5.1 Co se nedá z výpočtů vyčíst .....	42

4.5.2	Co se naopak z výpočtů vyčíst dá.....	42
<b>5</b>	<b>NĚKTERÉ ŠIFROVÉ TABULKY A JEJICH ROZBOR</b>	<b>44</b>
5.1	SVĚTOVÁ VÁLKA.....	44
5.2	WILLIAM SHAKESPEARE.....	46
5.3	JICCHAK RABIN.....	48
5.4	RENÉ MOAWAD.....	50
	<b>ZÁVĚR</b>	<b>53</b>
	<b>CONCLUSION</b>	<b>55</b>
	<b>SEZNAM POUŽITÉ LITERATURY</b>	<b>57</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK</b>	<b>58</b>
	<b>SEZNAM ILUSTRACÍ</b>	<b>59</b>
	<b>SEZNAM TABULEK</b>	<b>60</b>

## ÚVOD

Práce je určena všem, kteří mají zájem o objektivní pohled na fenomén jménem *The Bible Code*, který byl vytvořen newyorským novinářem *Michaelem Drosninem* v roce 1997. Řečený je autorem série knih, ve kterých tvrdí, že pomocí moderní výpočetní techniky je možné v hebrejském originále Bible nalézt skrytá proroctví o osudech lidstva. Prohlašuje, že některá proroctví se již naplnila, čímž byla dokázána jejich pravost, a je tedy důležité věnovat pozornost proroctvím ještě nenaplněným.

Skrytá sdělení Drosnin hledá tzv. metodou přeskokování písmen (angl. *skip code*) pomocí softwaru, který získal od *profesora Eliyahu Ripse*, jenž je lektorem na *Hebrejské univerzitě v Jeruzalémě*. Profesor Rips je uznávaný matematik a zbožný žid a s tímto softwarem provedl za spolupráce několika kolegů v roce 1994 slavný experiment, při kterém se mu podařilo najít v textu knihy *Genesis* (první kniha Tóry) jména 30 významných rabínů, kteří žili několik tisíc let po sepsání této knihy. Blízko jejich jmen byla také nalezena zašifrovaná data jejich narození a úmrtí. O tomto experimentu pak vyšel téhož roku článek v časopise *Statistical Science*, který vydává mezinárodní *Institut matematické statistiky* se sídlem v U. S. A.

Přestože byl zmíněný článek dokazující údajnou pravost těchto šifer vydán pouze jako hádanka k rozřešení, Michael Drosnin jej v úplném znění uvádí v první knize ze své série s názvem *The Bible Code I* jako podporu pro své názory. Díky tomu, že jsou jeho knihy velmi populární a jsou překládány do mnoha jazyků, a vycházejí stále v nových výtiscích, dá se říct, že se jedná o nejvíce publikovaný odborný článek vůbec.

Michael Drosnin svým knihám přidává na přesvědčivosti také tím, že čtenářům vypráví, jak se jemu samotnému povedlo předpovědět smrt izraelského předsedy vlády *Jicchaka Rabina*<sup>1</sup>, na nějž byl v roce 1995 spáchán atentát mladým aktivistou, který nesouhlasil s jeho politickými názory. Drosnin údajně v roce 1994 napsal Rabinovi dopis, ve kterém ho varoval na základě proroctví, které o něm metodou přeskokování písmen v Tóře našel.

Popularita knih Michaela Drosnina dokonce neklesá navzdory tomu, že jsou ostře kritizovány a napadány z řad odborníků na *statistickou a pravděpodobnostní teorii*. Nejznámější z nich je *Brendan McKay* učící na *Australian National University* v Canbeře. Ten v kolektivu svých kolegů vydal v časopise *Statistical Science* další článek<sup>2</sup>, ve kterém ukazuje, že zmíněnou metodou je možné najít šifry i v jiných rozsáhlejších textech,

---

1 [2], str. 3 a dále

2 [4]

konkrétně v románu *Hermana Melvilla Bílá velryba* (angl. názvem *Moby Dick*). McKey také znovu provedl s různými obměnami Ripsův známý experiment s 30 významnými rabíny, aby demonstroval, že nešlo o nic tak snadno nenapodobitelného, přičemž také důkladně rozebral, v čem se Rips a jeho kolegové v původním článku mýlili.

V této práci bych chtěl českému čtenáři přiblížit další zajímavé okolnosti týkající se jak Ripse, Drosnina a McKeye, tak přeskokovací metody samotné. Chci ji vlastním způsobem podrobně analyzovat a rovněž kriticky zhodnotit její použití na text Bible. K tomu budu využívat pravděpodobnostní a statistickou teorii a provedu několik příkladných výpočtů.

Dále bude součástí této práce ukázkový software, který bude fungovat podobně jako ten Eliyaha Ripse a jeho různé komerční napodobeniny, jimž vytváří Drosnin svými knihami značnou poptávku. V tomto softwaru bude také možné každé vyhledávání doplnit patřičnými výpočty.

V závěru se pokusím shrnout klíčové informace, který by měl znát každý, kdo se chce s výše popsanou problematikou blíže potýkat.

## **I. TEORETICKÁ ČÁST**

# 1 LITERÁRNÍ REŠERŠE

## 1.1 Úvod do biblických šifer

Nejprve je třeba připomenout, že *Bible* je sbírka náboženských textů, psaná jak židy, tak později prvními křesťany. První část, nazývaná *Starý zákon* (nebo též *Stará smlouva*), se týká převážně židů a je psána hebrejsky a místy aramejsky. Druhá část, jež začíná životem *Ježíše Krista*, a popisuje podrobně, jak jeho činy a slova navazují na dodnes zachovanou židovskou víru, se nazývá *Nový zákon* (*Nová smlouva*), a je psána řecky.

Nejmladší texty jsou dva tisíce let staré, ty nejstarší přes tři tisíce let. Je proto jasné, že *Bibli* nemůže dnešní člověk jen tak číst, přestože ji má k dispozici ve svém rodném jazyce. Bible si vyžaduje odborný výklad, který bere ohled na autora daného textu, jeho posluchače, jeho dobu, jeho záměr atd. Kromě výkladových metod obecně uznávaných v teologických kruzích však existují i metody alternativní, okrajové. Většina z nich je praktikována židy a spadá do různých jejich tradic, např. kabaly.

Je dobré také zmínit, že zatímco křesťanství hlavního proudu se shodne na tom, že pisatelé posvátných textů byli Bohem inspirováni pouze myšlenkově, u židů se objevuje názor, že hebrejský text, který tvoří celou jejich Bibli, je písmeno od písmene nadiktován samotným Nejvyšším.

Co je pro nás na tom všem ale důležité, je, že jsou známy alternativní metody výkladu hebrejské Bible, které si kladou za cíl dešifrovat některá její slova nebo celé úseky textu.

Abychom jim lépe porozuměli, je potřeba se nejprve trochu seznámit s hebrejskou abecedou. Hebrejská abeceda má 22 písmen. Před tím, než byla přijata arabská čísla, používala se hebrejská písmena také jako číslice. Kromě toho lze názvy písmen chápat i jako slova mající ještě jiný význam, podobně jako hieroglyfy. Přehled uvádí Tabulka 1:

Tabulka 1: Přehled hebrejské abecedy

hebrejské písmeno	český název	význam názvu	výslovnost	hodnota číslice
א	álef	býk, vůl	-	1
ב	bét/vét	stan, dům	b/v	2
ג	gimel	velbloud	g	3
ד	dálet	dveře	d	4

hebrejské písmeno	český název	význam názvu	výslovnost	hodnota číslice
ה	héj	okno, plot	h	5
ו	váv	hřeb	v	6
ז	zajin	zbraň	z	7
ח	chét	(živý) plot, komora	ch	8
ט	tét	kroutit, had	t	9
י	jód	zavřená dlaň	j	10
כ	káf/cháf	ruka, křídlo, otevřená dlaň	k/ch	20
ל	lámed	pohánědlo dobytka, služebnictvo	l	30
מ	mém	voda	m	40
נ	nún	ryba	n	50
ס	sámech	podpěra	s	60
ע	ajin	oko	-	70
פ	pé/fé	ústa	p/f	80
צ	cádé	háček na ryby	c	90
ק	kóf	zátylek	k	100
ר	rěš	hlava	r	200
ש	sín/šín	zuby	s/š	300
ת	táv	znak, kříž	t	400

Hebrejšťina je navíc zvláštní tím, že nepoužívá žádná písmena pro samohlásky. Slova jsou napsána jednoduše bez nich a mají tedy v mnoha případech více variant čtení, s čímž se pojí i více významů. Není potom těžké si domyslet, jak obtížně se někdy dopátrává správného výkladu seriózním vykladačům, a jak snadno se objevují často úplné nesmysly, pokud jde o jejich spíše senzacechtivé kolegy.

Tím ale nechci naznačit ani to, že židovská a křesťanská víra je založená čistě na spekulacích jejich duchovních vůdců, ba ani to, že všechny alternativní metody výkladu Bible jsou hodné zavržení. Pokud jde o to druhé zmíněné, uvedeme si nyní různé příklady, na kterých lze poměrně přesvědčivě ukázat, že šifry v Bibli opravdu jsou.

Aby jsme si ale dobře rozuměli, není šifra jako šifra. Zatímco dnes slouží šifrování k chráněné komunikaci, biblické šifry jsou spíše charakteru křížovky. Kdo šifru našel a roz-

luštil, mohl mít radost jak ze svého úspěchu, tak ze skrytého sdělení samotného.

### 1.1.1 Okrajové metody výkladu Tóry

#### *Metoda přeskakování písmen*

První případ, který si uvedeme, se váže přímo k našemu hlavnímu tématu. Jedná se o dešifrování textu metodou přeskakování písmen. Jde vlastně o to, že se vezme každé, dejme tomu třeba páté písmeno nějakého textu, a pokud nám alespoň část dává po přečtení smysl, tajné sdělení je na světě. Tato metoda je velmi stará a používala se dlouhou dobu před objevením moderního šifrování i jinde, než v Bibli.

První zmínky o ní pocházejí ze 14. století od španělského rabína *Bahyy ben Ashera*, který jako první použil židovský mysticismus zvaný kabala k výkladu Tóry. Sem tam se dá doložit, že tuto metodu někdo používal i nadále. Jeden z neznámějších případů úspěšné aplikace však pochází od maďarského rabína *Chaima Michaela Dova Weissmandela*, který svůj objev učinil někdy v průběhu 40. a 50. let 20. století během svého působení v Praze.

Rabín Weissmandel vzal každé padesáté písmeno z knihy *Genesis*, což je první z pěti knih Mojžíšových, známých jako Tóra nebo také *Pentateuch*. Sdělení, které našel, byla pouhá čtyři hebrejská písmena, která tvoří slovo tóra (*táv, váv, réš a héj*), což by mohlo samo o sobě být považováno za náhodu, kdyby se mu totéž nepodařilo i u Exodu (2. Mojžíšova). Následně objevil i to, že rovněž *Numeri* (4. Mojžíšova) a *Deuteronomium* (5. Mojžíšova) obsahují písmena slova Tóra, jenom v opačném pořadí. A konečně kniha *Levitikus* (3. Mojžíšova) obsahovala čtyři písmena božího jména, Jahve, rozmístěná se stejným odstupem. Konkrétně to byla písmena *jód, héj, váv* a opět *héj*, nazývána rovněž *tetragram*.<sup>3</sup> Výklad je potom takový: kdo čte Tóru, dojde vždy do stejného cíle - k Bohu.

#### *Gematrie*

Nyní se podívejme na velmi kontroverzní způsob zacházení s textem, jenž se nazývá *gematrie*. Její název je odvozen od řeckého slova *geometrie*, jež znamená doslova *zeměměření*. Má to vyjadřovat, že gematrie si klade za cíl vysvětlit svět kolem nás podle jakýchsi zvláštních čísel a ještě podivnější matematiky, jež mezi sebou sčítá hodnoty písmen i celých slov podle tabulky, kterou jsme si uvedli výše.

<sup>3</sup> Mezi židy není tetragram nikdy čten nahlas vzhledem k posvátné účtě k božímu jménu. Místo toho se nahrazuje slovy zástupnými, jako například Adónaj (Pán) neb Ha-šem (to Jméno).

Tato metoda spadá do kabalismu a židovské mystiky, ostatně jako většina jí podobných. Sčítání slov má samozřejmě hlubší význam. Nejde jenom o to, získat číselné výsledky (které mohou například být součinem čísel, jimž je přikládán v Bibli symbolický význam), ale také vysvětlit, co mají ta slova společného: jak po stránce číselné, tak významové.

Přestože většina z toho, co gematrie učí, zní uším nezajímavého člověka jako naprostý nesmysl, musíme přiznat, že místy to opravdu vypadá, jako by si biblický text se svými pokročilými čtenáři v tomto duchu pohrával.

Nejnámější je případ, kdy dal podle Bible Bůh *Abrahamovi* a jeho ženě *Sáře* nová jména. Abraham se totiž původně jmenoval *Abram*, což se v hebrejštině projevilo tak, že mu chybělo jedno písmeno, jímž bylo *héj*, které má hodnotu 5. Toto písmeno se i v božím jménu vyskytuje dvakrát, a je mu tedy v mnoha výkladech přikládán božský význam. Pro Abrahama získání písmene *héj* tedy mělo znamenat, že se ho v určité fázi jeho života Bůh dotknul, proměnil ho. Rovněž *Sára* dostala své *héj*. Stala se z ní *Sarah* místo původní *Sáraj*. Zajímavostí je, že *jód* z původního *Sárina* jména má hodnotu 10, takže ve výsledku měla obě jejich jména opět stejný součet.

Také zmíněné boží jméno má v gematrii svůj výklad. *Jód*, dvakrát *héj* a *váv* dává dohromady 26, což je dvojnásobek symbolického čísla 13. Třináctka je symbol božího lidu a je chápána jako 12 plus 1, přičemž 12 znázorňuje lid (12 kmenů, 12 světových stran, atd) a 1 znázorňuje Boha, jelikož židovský Bůh se vyznačoval tím, že byl jeden, na rozdíl od božstev jiných náboženství, která byla tehdy praktikována. Další zástupné názvy Boha opět obsahují třináctku, například *Echad*, což znamená Jeden, dává přesně 13, dále *Adónaj*, Pán, je dvakrát 13, *Haelohím*, Bůh, sedmkrát 13.

### *Atbaš*

Jinou zajímavostí, kterou bychom neměli v kategorii biblických šifer přehlédnout, je substituční šifra *atbaš*. Název je odvozen od pomůcky, kterou *atbaš* používá (viz *Tabulka 2*).

*Tabulka 2: Pomůcka pro atbaš*

כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת

Jak je vidět, jedná se o překlopenou abecedu, ve které se první písmeno nahrazuje posledním a poslední prvním, stejně tak druhé se nahrazuje předposledním a předposlední

druhým atd. V pravé části (hebrejšтина se čte zprava doleva) se pod sebou nacházejí písmena *álef, táv, bét, šín* - odtud tedy atbaš.

Tato šifra je rovněž velice stará a její existenci dokládá jak kabalistická literatura, tak například i četnost jejího výskytu v biblické knize *Jeremiáš*, jež je označována za knihu prorockou. Jako příklad<sup>4</sup> si uveďme text, který se nachází v 51. kapitole této knihy ve 41. verši: „*Jak je lapen Šěšak, zajata chloubá celé země! Jak je zpusťošén Babylon mezi pronárody.*”<sup>5</sup>

Jméno Šěšak, v hebrejštině psáno jako ששכ (*šín, šín, káf*), odpovídá podle tabulky slovu *Babylón*, hebrejsky *Bábel*, בבל. (*bét, bét, lámed*). Pozoruhodné na tom je, že jinde než u Jeremiáše jméno Šěšak nenajdeme, a to jak v Bibli, tak v jiných záznamech té doby.

Jiný příklad<sup>6</sup> najdeme v téže kapitole, jen v prvním verši. Text říká: „*Hle, vzbudím proti Babylónu zkázonosný vítr, proti obyvatelům onoho 'srdce mých protivníků'.*”<sup>7</sup> Jak je patrné, výraz „srdce mých protivníků” si vyžaduje speciální výklad. Nejvhodnější se opět ukázal atbaš. „Srdce mých protivníků” má v hebrejštině podobu לב קמי (*lámed, bét, kóf, mém, jód*), což se dá pomocí atbaše přepsat na כשדים (*káf, šín, dálet, jód, mém*), což znamená *Kaldejci* (obyvatelé *Kaldeje*). Tento výklad podporuje i *Septuaginta*, latinský překlad Bible 1. stol. př. n. l., který uvádí rovnou slovo *Kaldejci* místo výrazu „srdce mých protivníků”. Navíc o pár veršů dále se se slovem *Kaldejci* setkáme i v samotném hebrejském textu.

Důvod, proč se v knize *Jeremiáš* používá atbaš, nejspíš souvisí s tím, že proroctví se obecně často uvádějí v symbolech a v hádankách.

## 1.2 Moderní historie metody přeskokování písmen

Když je nám nyní zřejmé, že netradiční metody výkladu Bible mají i v seriózní teologii své místo, vraťme se zpět k metodě přeskokování písmen samotné, abychom si ukázali, jak vypadá její aplikace v moderní době.

### 1.2.1 Eliyahu Rips

Moderní použití se váže k již zmíněnému *prof. Eliyahu Ripsovi*. Prof. Eliyahu Rips, se narodil v roce 1948 v Lotyšsku. Jeho rodné jméno je *Ilya Rips*, ale dnes žije v Izraeli, kde jej všichni znají pod jeho hebrejským jménem *Eliyahu Rips*.

4 [7], str. 173

5 Jer 51, 41 (ČEP)

6 [7], str. 174

7 Jer 51, 1 (ČEP)

Pro některé je znám v souvislosti s výzkumem v oblasti *geometrické teorie grup*, pro jiné právě pro jeho podíl na fenoménu známém jako *The Bible Code* (Kód Bible) nebo též *The Torah Code* (Kód tóry). Nám z bývalého Československa jistě nebude lhostejná také skutečnost, že se v roce 1968 neúspěšně pokusil veřejně upálit na protest proti Sovětské invazi do našich zemí. Za tento čin byl zatčen a uvězněn. Díky tomu, že už v té době bylo známo, že je nebývale zdatným matematikem, byl po nátlaku ze západu propuštěn a bylo mu dovoleno emigrovat do Izraele. V roce 1975 zde dosáhl titulu *PhD* v matematice na *Hebrejské Univerzitě v Jeruzalémě*. Jeho tématem byl *problém vícerozměrných podgrup*. Od té doby zde působí jako profesor v *Ústavu matematiky* a za svůj výzkum dostal i několik cen.

A byl to právě prof. Rips, kdo jako první použil počítač ke hledání biblických šifer metodou přeskakování písmen. Společně s kolegy *Doronem Witztumem* a *Yoavem Rosenbergem* pak učinil jeden zajímavý objev, který publikovali v roce 1994 v časopise *Statistical Science*.<sup>8</sup>

Jejich experiment se týkal toho, že se pokusili najít jména třiceti významných rabinů v textu knihy *Genesis*, každého jednotlivě na jednom místě společně s daty jejich narození a úmrtí. Následně se pokusili spočítat, jaká je šance, že by se něco takového mohlo podařit náhodou - ve smyslu náhodou ospravedlnitelnou statistickými výpočty. Tehdy odhadli, že skutečná šance je kolem 1 : 62 500.

Díky tomuto tvrzení byl jejich článek odmítnut časopisem *Proceedings of the National Academy of Sciences of the USA*, kterému ho původně odeslali. Také časopis *Statistical Science* tento článek publikoval pouze s komentářem *profesora Roberta E. Kasse (Carnegie Mellon University)*, že jde spíše o hádanku k rozluštění.<sup>9</sup>

Rips ale nikdy kritiku nepřijal. Své objevy považuje za natolik přesvědčivé, že se existence biblického kódu nechce vzdát. Mimo jiné se mu údajně podařilo předpovědět válku v Peruském zálivu. A na tuto předpověď pak reagoval newyorský novinář *Michael Drosnin*, který Ripsově práci dodal značné popularity. Dlužno poznamenat, že jeho přístup se od Ripsova poněkud liší.

### 1.2.2 Michael Drosnin

Michael Drosnin se narodil v roce 1946 v New Yorku. Zde pracoval pro deníky *Washington Post* (1966–1968) a *Wall Street Journal* (1969–1970). Později se rozhodl, že bude psát

<sup>8</sup> Dostupné také v [2], str. 195 a dále

<sup>9</sup> [4], str. 7

knihy. V roce 1985 byla vydána jeho první kniha *Citizen Hughes (Občan Hughes)*, která je životopisem amerického miliardáře *Howarda Hughese*, a která je založena na ukradených dokumentech. V červnu roku 1992 mu pak během jeho pobytu v Izraeli někdo doporučil, aby se setkal s profesorem Ripse, kvůli již zmíněné předpovědi války v Perském zálivu. Drosnin vzpomíná<sup>10</sup>, že mu dal Rips tehdy přečíst citát rabína Ga'ona z Vilna, který zněl:

*„Pravidlo říká, že vše, co bylo, je a bude do konce času samotného, je obsaženo v Tóře, od prvního slova až do toho posledního. A ne pouze v obecném smyslu, ale že každý detail o všech a o každém zvlášť, a detaily všech detailů všeho, co se každému stalo od prvního dne, kdy se narodil, až do jeho posledního.“<sup>11</sup>*

Na tomto místě je vhodné poznamenat, že mnoho židů tomuto tvrzení skutečně věří, Ripse nevyjímaje. Když Rips pak překvapenému Drosninovi ukázal, že šifry v Tóře nehledá ručně, ale pomocí počítače, vedlo to k tomu, že Drosnin místo plánovaného odpoledne s Ripse zůstal celý týden.

Drosninovi se pak po dvou letech hledání povedlo pomocí Ripsova softwaru učinit jeho vlastní objev, který pak údajně změnil jeho život. V textu Tóry našel v roce 1994 jméno tehdejšího izraelského předsedy vlády, *Jicchaka Rabina*, které se křížilo se slovy „*zabiják, který zabije*“. Drosnin z toho usoudil, že se Rabin nachází v nebezpečí, a napsal mu varovný dopis. K překvapení všech, kdo o tom věděli, včetně Drosnina samotného, byl necelý rok po obdržení dopisu dne 4. listopadu 1995 *Jicchak Rabin* zavražděn mladým pravicovým radikálem *Jigalem Amirem*, který s ním tvrdě nesouhlasil, protože podepsal oselskou Mírovou dohodu.

Drosnin tehdy prohlásil, že přes svůj typicky novinářský skepticismus došel k závěru, že Bible obsahuje zašifrovaná proroctví, která popisují světové události jak minulé tak budoucí, a dal se do psaní série knih nazvané *The Bible Code*.

Přestože to Drosnin nikde neuvádí, sám Rips se od jeho knih distancuje. V roce 1997 vydal Rips prohlášení<sup>12</sup>, ve kterém říká, že se s Drosniem sice setkal, ale nikdy mu v jeho vlastní práci nepomáhal, a ani nesouhlasí se všemi závěry, které Drosnin učinil. Podle Ripse jsou sice v Tóře šifry popisující světové události, ale kategoricky odmítá, aby se s nimi zacházelo jako se zprávami, které mají předpovídat, co se stane.

<sup>10</sup> [2], str 7

<sup>11</sup> Můj překlad textu, který uvádí Drosnin - viz výše. Uvedený text: „*The rule is that all that was, is, and will be unto the end of time is included in the Torah, from the first word to the last word. And not merely in a general sense, but as to the details of every species and each one individually, and details of details of everything that happened to him from the day of his birth until his end.*”

<sup>12</sup> [6]

### 1.2.3 Brendon McKay

9. června v roce 1997 vyšel v americkém mezinárodním zpravodajském časopise *Newsweek* článek, ve kterém Michael Drosnin vyslovil následující výzvu: „Až moji kritici najdou zprávu o zavraždění předsedy vlády zakódovanou v *Bílé velrybě*, začnu jim věřit.”<sup>13</sup>

Řeč byla samozřejmě o Drosninově předpovědi atentátu na Jicchaka Rabina. A byla to právě tato věta<sup>14</sup>, která vyprovokovala *Brendona McKaye*, profesora *Australské univerzity v Canbeře*, aby se začal zajímat o práci Michaela Drosnina a nakonec také Eliyaha Ripse.

Brendon McKay se narodil 26. října 1951 v *Melbourne*, kde vystudoval *Melbournskou univerzitu*, a kde v roce 1980 získal titul Ph.D. v matematice. Předmětem jeho doktorské práce byla *výpočetní teorie grafů*. Zajímavostí také je, že jeho Erdősovo číslo je 1.

McKay zasvětil velkou část života tomu, aby dokázal, že žádný patřičně vzdělaný člověk nemůže věřit zprávám, které v Bibli našel Rips či Drosnin či kdokoli jiný používající jejich metodu. V románu *Bílá Velryba* od spisovatele *Hermana Melvilla* z roku 1851 nejen našel proroctví o smrti Jicchaka Rabina, ale také například *Johna Fitzgeralda Kennedyho* nebo *Abrahama Lincolna*, či celou sbírku proroctví o *britské princezně Dianě*.

Další jeho snahy spočívaly v tom, že se spojil s izraelskými odborníky, kteří s Ripsem nesohlasili, aby společně napsali článek do časopisu *Statistical Science*, ve kterém poukáží na slabá místa původního článku, který napsal Rips se svými kolegy. Jejich článek nakonec vyšel v květnu 1999. McKayův tým v něm přesvědčivým způsobem vysvětlil, že výpočty Ripsova týmu nemají žádnou váhu, jelikož obsahují kritické chyby. Dále zpochybnil samotné metody, které byly použity k vyhledávání rabínů.

### 1.2.4 Řešení záhady jménem Kód Bible

Brendon McKay a jeho tým svůj článek nazval *Solving the Bible Code puzzle*<sup>15</sup>. Uvádím zde ve stručnosti to hlavní, co se snažil říct. Na adresu výpočtů Ripse a jeho kolegů (dále WRR<sup>16</sup>) se v článku píše toto:

- WRR svou práci založili na složité funkci  $c(w, w')$ , kterou si sami definovali, a která má vyjadřovat blízkost (angl. *closeness*) mezi jednotlivými slovy tak, jak byly nalezeny v Tóře. Její rozsah je ostrý interval od 0 do 1.

<sup>13</sup> Originál: When my critics find a message about the assassination of a prime minister encrypted in Moby Dick, I'll believe them.

<sup>14</sup> [3]

<sup>15</sup> volně přeloženo: Řešení záhady jménem Kód Bible

<sup>16</sup> Witztum, Rips, Rosenberg

- Dále používají dvě funkce,  $P_1$  a  $P_2$ , jejichž účelem je spočítat, jaká je pravděpodobnost, že se slova podobného významu budou nacházet v blízkosti  $c$ , jež byla stanovena jako 0,2 a menší. Pomocí praktických výpočtů za pomoci těchto dvou funkcí mělo vyjít najevo, že blízkost zvolených slov je větší, než by být měla.
- Ve skutečnosti  $P_1$  a  $P_2$  nepočítají úplně přesně to, co by se dalo nazvat pravděpodobnost, a navíc jsou jejich výsledky silně ovlivněny výběrem slov. Pokud například odeberete 4 rabíny, kteří nejvíce ovlivnili původní výsledek celkové šance na 1 : 62 500, získáte nezajímavý poměr 1 : 30.

K problému s teorií pravděpodobnosti, který WRR špatně pojali, byla uvedena následující analogie:<sup>17</sup>

*Představte si, že pořádáte atletické závody ve skoku do dálky v obzvlášť větrný den, přičemž je možné, že síla větru může klidně ovlivnit délku skoku některých atletů. Když to pojmete tak, že všichni atleti mají stejnou šanci být ovlivněni větrem, takže mají také stejnou šanci vyhrát, zní to fér, ale když vezmete v úvahu, že vítěz může vyhrát taky třeba jen díky větru namísto svým schopnostem, už to tak uspokojivě nevypadá. Soutěž by jistě měla být založena na tom, že šance vyhrát je pouze věcí schopností každého atleta, jenomže to díky nepředvídatelnosti větru nemůžete slíbit.*

Touto analogií je myšleno, že výpočty, které provedli WRR, hovoří spíše o nezajímavých vlastnostech konkrétního seznamu slov, než o výjimečnosti knihy Genesis.

Dále McKayův tým napadl způsoby, jakými bylo provedeno samotné vyhledávání údajů o rabínech, tedy jejich jmen vedle dat narození a úmrtí:

- Výběr samotných rabínů měl být údajně pořízen podle jejich významnosti. Ve skutečnosti byli vybíráni z encyklopedie podle délky záznamu o nich, a podle toho, zda se dalo zjistit obě jejich významná data.
- Ne u všech rabínů byla data jednoznačná, pokud vůbec byla v encyklopedii obsažena. Některá data byla do listu dokonce zařazena přesto, že byla historicky méně věrohodná.
- Formát dat nezahrnoval roky, ale pouze dny a měsíce, přičemž byly upřednostněny některé formy, které nejsou běžně používány, jako například zápis pomocí konkrétních židovských svátků apod.

---

17 [4]. str. 8. Volný překlad.

- Také označení rabínů bylo vybíráno účelně, z mnoha možných variant. A nešlo jenom o různé způsoby zápisu jmen, ale té o akronymy. Například „*Rambam*” je akronym pro rabína nazývaného *Rabbenu Moše ben Maimon*, také známého jako *Maimonides*.
- Kromě toho, v hebrejštině je možné ta samá slova zapsat různými způsoby, což také otevírá další možnosti, které je potřeba připočítat k těm již zmíněným.

Dále McKayův tým provedl úspěšně provedl ten samý experiment v hebrejském překladu románu *Vojna a mír* od *Lva Nikolajeviče Tolstého*, čímž dokázal, že na knize Genesis není v tomto smyslu nic výjimečného.

Kromě toho také poukázal na několik dalších obtíží, jako například drobné vady Ripsova softwaru nebo více verzí prohledávaného textu.

### 1.2.5 Shrnutí

Jak jde z mnohého vidět, Ripsův pohled je především zakotvený v jeho židovské zbožnosti a je také výborným matematikem, jenže se nedá říct, že by byl zrovna expert na statistickou a pravděpodobnostní teorii. Nicméně se mu musí přiznat, že je jako žid úctyhodně skromný a čestný a na rozdíl od Drosnina mu vůbec nejde o popularitu.

Naproti tomu Michael Drosnin se na sebe neustále snaží upoutat pozornost. Na podporu jeho knih bylo v U. S. A. natočeno i několik podstatně neobjektivních dokumentů v nichž se například také propaguje komerční verze napodobeniny Ripsova softwaru. Ke všemu se Drosnin v jedné ze svých knih nepřímo přiznává, že ani pořádně neví, jak se používá teorie pravděpodobnosti.<sup>18</sup>

Zato Brendon McKay má všechny potřebné předpoklady k tomu, aby mohl vznést objektivní kritiku, a to také udělal. Je škoda, že je mu dopřáváno tak málo sluchu: ve výše zmíněných dokumentech je uváděn pouze jako bezdůvodně zákeřný odpůrce divákovi podsouvaného názoru, a je zpravidla přehlušen nepoměrným množstvím příspěvků z řad zaujatých židovských odborníků, kteří byli předem pečlivě vybráni, aby obhajovali názory jedné jediné strany.

---

18 [2], str. 29

## 2 METODA PŘESKAKOVÁNÍ PÍSMEN

Metoda přeskakování písmen by se z pohledu *kryptologie* dala zařadit mezi *klasické transpoziční šifry*.

Slovo *klasická* přitom znamená, že k šifrování či dešifrování není potřeba žádné mechanické či moderní výpočetní pomůcky.<sup>19</sup>

Slovem *transpoziční* se zase poukazuje na postup založený na změnu pozice. Přitom můžeme měnit pozici jak písmen, tak čtenářovy pozornosti. V praxi se používá obojí.

Metoda by se dala také zařadit do kategorie *steganografie*, jež obsahuje případy, kdy sdělení není nijak samo o sobě pozměněno (ve smyslu zašifrování), ale je pouze potřeba vědět, kde nebo jak ho hledat. Za skryš by pak mohl být považován okolní text.

### 2.1 Šifrování

Chceme-li tuto metodu použít ke skrytí sdělení, je potřeba si nejprve zvolit vzdálenost klíčových písmen v šifrovaném textu. Zvolíme-li si, že se písmena budou nacházet na každé  $x$ -té pozici, můžeme si například sestavit tabulku, jež bude mít  $x$  sloupců. Sdělení potom napíšeme do libovolného sloupce a zbytek tabulky vyplníme smysluplným textem libovolného druhu. Text tabulky se dále sepíše do běžné podoby, tzn. opatří se mezerami, interpunkčními znaménky a podobně, případně se spojí ještě s dalším textem.

### 2.2 Dešifrování

Dešifrování lze provádět několika způsoby. Pokud například známe rozestup klíčových písmen, stačí je pouze najít a přečíst je jedno po druhém. V opačném případě je potřeba zkoušet různé varianty. Ku pomoci přitom může být například i to, když jsme si jisti, že se v šifrovaném sdělení nachází nějaké slovo. Potom sledujeme všechny výskyty prvního písmene onoho slova a hledáme, v jaké vzdálenosti od něj se nachází další písmeno, a zda-li se ve stejné vzdálenosti nachází i písmeno třetí, čtvrté atd. V případě úspěchu se s odpovídajícím přeskokem písmen prozkoumá i okolí nalezeného slova.

Mezi některými luštiteli se pro separovaná písmena vžil pojem ELS čili *equidistant letter sequency*, což volně přeloženo znamená posloupnost písmen, mezi nimiž je stejná vzdálenost.

---

<sup>19</sup> To ovšem nemusí znamenat, že pomůcku použít nelze nebo dokonce není povoleno.

## 2.3 Použití k výkladu Bible

Vykladači Bible používající metodu přeskokování písmen vlastně provádějí pouze dešifrování. Vycházejí přitom z předpokladu, že Bible již obsahuje takto zašifrovaná místa. Slova, která hledají, jsou libovolně zvolena, a často souvisejí s vybranou pasáží, jež je použita k hledání. Zároveň také nejde o to, najít v textu skryté celé věty, ale spíše najít na jednom místě víc frází zašifrovaných s různým skokem.

Tabulka, kterou si k tomuto účelu luštitel sestavuje, bývá popisována jako šifrový válec<sup>20</sup> sestavený ze spirály po sobě jdoucích písmen, který je na jedné straně příčně rozříznut, a rozprostřen do plochy.

## 2.4 Problémy související s takovýmto výkladem Bible

### 2.4.1 Použití výpočetní techniky

První problém bychom mohli vidět už v samotném *nasazení výpočetní techniky*. Zatímco starověký vykladač byl odkázán pouze na psací pomůcky a svou hlavu, a bylo pro něj tedy obzvlášť obtížné nějakou šifru vůbec objevit, pomocí počítače se dá velmi snadno a rychle prohledat i hodně dlouhý text. Můžeme tak najít výrazy, jejichž jednotlivá písmena jsou od sebe vzdálena i o několik tisíc až desítek nebo i stovek tisíc písmen. Při sestavování tabulky potom v takovémto případě narazíme na problém, jak ji vůbec celou zobrazit - a přitom v grafickém znázornění spočívá celá krása a důvtip metody.

A dále pokud se pustíme do hledání dalších výrazů v okolí toho původního, tak zjistíme, že jestli nechceme výsledku ubrat na efektu, nesmíme překročit hranici zorného pole našich posluchačů. Tím pádem nám nezbývá než zobrazit pouze část tabulky a další výrazy hledat pouze v této části, čímž se problém vyřeší jenom částečně, jelikož tabulka sice bude vypadat působivě, ale nebude možné použít nálezy, které se do výběru nevešly.

Dá se říct, že se tím metoda stává z části klasickou a z části moderní šifrovací metodou, přičemž jí ona hybridita rozhodně moc nepřidává na *důvěryhodnosti*, jež je jejím dalším problémem, dokonce problémem zásadním, jenž se k této metodě váže.

### 2.4.2 Důvěryhodnost původu šifer

Kritici říkají, že skrytá sdělení je možné najít v každém dostatečně dlouhém textu. Na tento jejich argument pak mají zastánci metody přeskokování písmen dvě možnosti, jak reagovat.

---

<sup>20</sup> Z přísně geometrického hlediska je to spíše plášť válce bez podstav.

Ta první je dokázat opodstatnění použití metody z nějakého spolehlivého pramene, který výslovně na existenci zašifrovaných sdělení upozorňuje. To samozřejmě předpokládá existenci takového důkazu a nutno přiznat, že v drtivé většině jej nemáme. Druhá možnost je použít teorii pravděpodobnosti k odhalení náhodnosti výskytu onoho jevu. Teorie pravděpodobnosti však nikdy nenabízí jednoznačné tvrzení, ale může pouze vyčíslit pravděpodobnosti jednotlivých jevů.

### 2.4.3 Podoba prohledávaného textu

Aby toho nebylo málo, je tu ještě jeden zásadní problém - problém, na který upozornil i *Brandon McKay*, a který *Michael Drosnin* více či méně vědomě ignoruje. Jde o to, že ve skutečnosti *neexistuje* taková verze původního hebrejského textu, která by byla jednoznačně shodná s tou, v jaké byla hebrejská Bible původně napsána.

Tím, že se jednotlivé texty opisovaly, vzniklo mnoho verzí, které se od sebe navzájem liší. Příčinami mohlo být například to, že při opisování zpravidla jeden člověk četl a druhý psal, takže mohlo dojít k přeslechům. Dále se prováděly různé úpravy i z věroučných důvodů.

Teprve v 5. století se poprvé objevili tzv. *Masoretští učenci*, kteří vyvinuli snahu změnám v textu zabránit. Jednak se pokusili dát ze všech dostupných verzí dohromady jednu jedinou, která by se co nejvíce blížila původnímu textu, a jednak spočítali všechna písmena jednotlivých knih, aby pak bylo možné ověřit věrohodnost dalších opisů. Jejich činnost pak pokračovala po několik dalších staletí.

Existence *masoretářů* bývá dnes proto mylně uváděna jako argument, že původní hebrejský text k dispozici máme. Ve skutečnosti ani jejich veškerá snaha úplně nesjednotila všechny jim dostupné verze. Z jejich významných prací si uveďme alespoň dva nejdůležitější:

- *Aleppský kodex*. Byl sepsán někdy kolem roku 930. Od roku 1956 podle něj Hebrejská univerzita v Jeruzalémě sestavuje kritické vydání hebrejské Bible. Některé jeho části chybí, takže přestože je nejstarší textem, co dnes máme, nemůžeme o něm říct, že je nejstarším a zároveň kompletním dochovaným textem.
- *Leningradský kodex*. Vznikl přibližně v letech 1008 až 1009 a dodnes se dochoval celý. Jeho text sloužil jako podklad pro dílo s názvem *Biblia hebraica*, jenž bylo později upraveno a vznikla tak *Biblia Hebraica Stuttgartensia*, která je dnes většinou považována za text nejbližší těm původním.

Není těžké si domyslet, že pokud by existovaly třeba jen dvě verze textu, které by se lišily zrovna jen v jednom chybějícím/přebývajícím písmeni, a nebyl jednotný názor na to, která z nich je správná, museli by být všechny šifry přesahující text před oním sporným písmenem považovány za potenciálně nedůvěryhodné. A jestliže skutečných verzí máme dnes několik, není možné, abychom jim přisuzovali nějakou váhu, pokud zrovna nejsme pevně přesvědčeni o pravosti jedné z nich.

Například profesor *Eliyahu Rips* pro svůj pokus s třiceti rabíny použil *Korenskou Jeruzalémskou Bibli*, kdežto židovští odborníci z týmu Brendona McKaye upřednostňují *Jemenské vydání*, případně *Leningradský kodex*.<sup>21</sup>

---

21 [4], str. 27

## **II.PRAKTICKÁ ČÁST**

## 3 VZOROVÝ SOFTWARE

### 3.1 Použité prostředky

Vzorový software pro demonstraci použití metody přeskokování písmen byl vytvořen v Microsoft Visual Studiu 2010 Ultimate v programovacím jazyce C# za pomoci .NET frameworku 4.0<sup>22</sup>. K realizaci aplikace bylo potřeba připojit se k Jet databázi pomocí OLEDB Providera.

Jako jazyk programu byla zvolena angličtina, jelikož je přístupnější větší škále uživatelů, než čeština, jež je jazykem této práce. Anglicky je jak uživatelské rozhraní, tak také zdrojový kód programu.

### 3.2 Vnitřní popis

Dříve, než si popíšeme, jak software používat, podíváme se na to, na jakých principech funguje.

#### *Spuštění programu*

Během spouštění se načte do paměti soubor, jenž obsahuje celý text hebrejské Tóry. Text je prostý všech znaků, které nejsou písmena (včetně mezer). Rovněž neobsahuje nic jako názvy knih nebo čísla kapitol.

Dále dojde k připojení k Jet databázi, jež obsahuje text Tóry ve třech jazycích. Tabulka s hebrejskou verzí navíc ještě obsahuje sloupce pro index prvního a posledního písmene pro každý jednotlivý verš. Díky tomu je možné zobrazit nález hledaného sdělení také v kontextu Bible v přehledné formě a ve více jazycích.

#### *Vyhledávací algoritmus prvního výrazu (vyhledávání v textu)*

Při hledání prvního výrazu je použit následující postup:

1. Pokud nejsi na konci textu, přečti jedno písmeno.
2. Porovnej ho s prvním písmenem hledaného výrazu
  - a) Pokud se písmena neshodují, přejdi ke kroku 1.
  - b) Pokud se písmena shodují, přejdi ke kroku 3.

---

<sup>22</sup> Použitá literatura: [5]

3. Vypočítej maximální možný skok (tak, aby ještě bylo možné najít všechna písmena v prohledávaném textu).
4. Proved' zadaný skok a zkontroluj, jestli se písmeno na této pozici shoduje s dalším písmenem výrazu.
  - a) Pokud se písmena neshodují, Zmenši hodnotu skoku o 1 a opakuj krok 4, pokud není hodnota skoku rovna 0 - v tom případě přejdi ke kroku 1.
  - b) Pokud se písmena shodují, opakuj krok 4 se stejnou hodnotou skoku, dokud nedojdeš k poslednímu písmenu hledaného výrazu - v tom případě si poznamenej nález a přejdi ke kroku 1.

Poznámka: Ve skutečnosti je algoritmus o něco složitější, jelikož je použit pro vyhledávání oběma směry.

### ***Sečtení všech možných skoků a offsetů u vyhledávání v textu***

Jelikož výše popsany algoritmus automaticky přeskakuje nevyhovující možnosti, které při statistických výpočtech také musíme vzít v úvahu, je potřeba provést sečtení všech možných skoků a offsetů zvláštním algoritmem:

1. Celkový součet je nastaven na 0.
2. Pokud jsi na pozici menší rozdílu délky textu a délky hledaného výrazu, spočítej maximální skok z této pozice (viz rovnice 4 v kapitole 4.2).
3. Porovnej maximální skok a uživatelem definovaný maximální skok.
  - a) Pokud je maximální skok menší nebo roven uživatelem definovanému maximálnímu skoku, přičti jeho hodnotu k celkovému součtu.
  - b) V opačném případě přičti k celkovému součtu uživatelem definovaný maximální skok.
4. Přejdi ke kroku 2.

### ***Vyplnění tabulky***

Získáme-li při hledání alespoň jeden pozitivní výsledek, můžeme si vytvořit i tabulku okolního textu. Její rozměry jsou předem zadávány uživatelem, takže vše, co je potřeba, je umístit nalezený text doprostřed. To se udělá tak, že první písmeno výrazu se bude nacházet v polovině rozdílu výšky tabulky a délky výrazu. Následně se dopočítá index prvního písmene v prvním řádku tabulky a tabulka se začne vyplňovat buď zprava nebo zleva, podle toho, jestli pracujeme z hebrejským nebo latinským textem. Výpočty se řídí pravidlem, že mezi písmeny, jež se nacházejí přesně nad sebou, je rozdíl roven délce skoku, jenž byl použit k nalezení hledaného výrazu.

Vyplnění tabulky se provádí ve dvou případech: buď při vyhledávání více výrazů najednou (na tabulku je pak použit vyhledávací algoritmus pro druhý výraz) nebo při zobrazení výsledku v uživatelském rozhraní.

### ***Vyhledávací algoritmus druhého výrazu (vyhledávání v tabulce)***

Druhý výraz se vyhledává z tabulky, takže se nemůžeme řídit stejným postupem, jako při vyhledávání prvního výrazu, jelikož bychom se mohli dostat mimo tabulku. Je proto použit následující postup:

1. Přečti jedno písmeno z tabulky. (Písmena se berou postupně po jednom z každého řádku.)
2. Porovnej ho s prvním písmenem hledaného výrazu.
  - a) Pokud se písmena neshodují, přejdi ke kroku 1.
  - b) Pokud se písmena shodují a hledaný výraz je dlouhý jedno písmeno, poznamenej si nález a přejdi ke kroku 1.
  - c) Pokud se písmena shodují a hledaný výraz je delší než jedno písmeno, přejdi ke kroku 3.
3. Porovnej druhé písmeno hledaného výrazu s každým písmem v tabulce.
  - a) Pokud se písmena neshodují, přejdi ke kroku 1.
  - b) Pokud se písmena shodují a hledaný výraz je dlouhý dvě písmena, poznamenej si nález a přejdi ke kroku 1.

- c) Pokud se písmena shodují a hledaný výraz je delší než dvě písmena, přejdi ke kroku 4.
4. Odečti mezi sebou indexy nalezených písmen. (Indexem se rozumí jeho index v poli písmen textu Tóry.)
5. Použij rozdíl indexů jako hodnotu skoku k nalezení dalšího písmene.
  - a) Pokud ses dostal mimo hranice tabulky, přejdi ke kroku 1.
  - b) Pokud se písmena neshodují, přejdi ke kroku 1.
  - c) Pokud se písmena shodují, opakuj krok 5, dokud nedojdeš na konec výrazu - v tom případě si poznamenej nález a přejdi ke kroku 1.

### ***Sečtení všech možných skoků a offsetů u vyhledávání v tabulce***

Při prohledávání tabulky opět platí, že nevyhovující možnosti nejsou projity všechny po jedné, takže musíme i v tomto případě mít vlastní algoritmus:

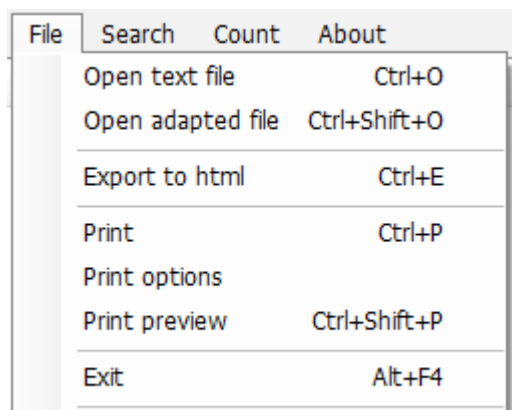
1. Nastav celkový součet na 0.
2. Pokud nejsi u poslední buňky, posuň se o buňku dál. (Buňky se berou postupně po jedné z každého řádku.)
3. Procházej znovu všechny buňky (kromě té primárně vybrané) a pro každou z nich proved'  $n$ -krát stejný posun, jako je mezi primárně a sekundárně vybranou buňkou (o  $x$  řádků a  $y$  sloupců), přičemž  $n$  je rovno délce hledaného výrazu zmenšené o jedničku. Pokud ses při tomto postupu nedostal mimo meze tabulky, přičti k celkovému součtu 1.
4. Přejdi ke kroku 2.

## **3.3 Vnější popis**

### **3.3.1 Hlavní a kontextová menu**

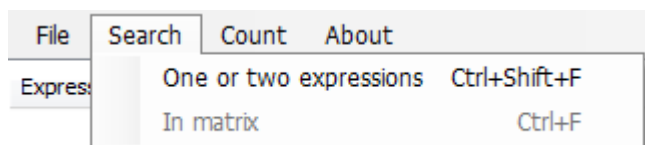
Menu obsahuje převážnou většinu funkcí, kterými program disponuje, a jeho rozložení napodobuje rozložení u většiny programů. V nabídce **File** (viz *Ilustrace 1*), je obsažena veškerá práce se soubory. Je možné načíst neupravený textový soubor v libovolném

běžném kódování (***File->Open text file***), což může trvat delší dobu, jelikož je potřeba text nejprve zbavit mezer a všech dalších znaků, které nejsou písmena. Upravený soubor se automaticky uloží do složky *adapted*, která je podložkou programu. Odtud je pak možné tento soubor opětovně načíst v podstatně kratším čase pomocí příkazu ***File->Open adapted file***.



*Ilustrace 1: Vzorový software - nabídka File*

Nyní nabídku *File* na chvíli opustíme a podíváme se na možnosti vyhledávání. Pod položkou menu ***Search*** (viz *Ilustrace 2*) se skrývají dvě varianty vyhledávání, ***Search->Search one or two expressions***, pomocí kterého můžeme hledat jeden či dva výrazy. Tímto bychom každopádně měli začít, protože teprve potom, co se výsledky zobrazí v ovládacích prvcích *ListView* v levé části hlavního okna programu, můžeme kliknutím na první výraz vykreslit matici textu, od čehož se odvíjí další funkce programu.



*Ilustrace 2: Vzorový software - nabídka Search*

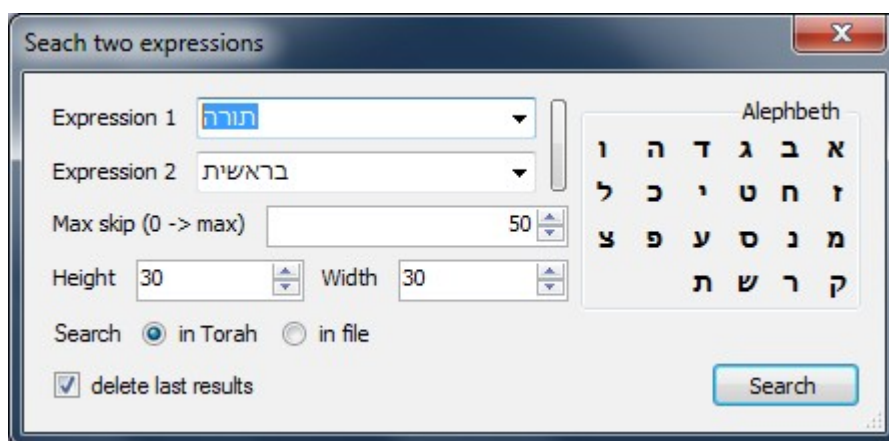
Při vyhledávání můžeme měnit různé parametry (viz *Ilustrace 3*). Můžeme prohodit výrazy tlačítkem po pravé straně polí, pro zadávání výrazů.

Můžeme změnit délku maximálního skoku (***Max skip***; jestliže zadáme hodnotu 0, bude maximální délka odvozena od délky prohledávaného textu).

Dále je možné měnit rozměry matice (*Width* - šířka, *Height* - výška). Standardně jsou přednastaveny na 30 písmen. Tato velikost je optimální vzhledem k tomu, že větší matice mají sice více možností nálezů druhého výrazu, ale projeví se to na rychlosti vyhledávání.

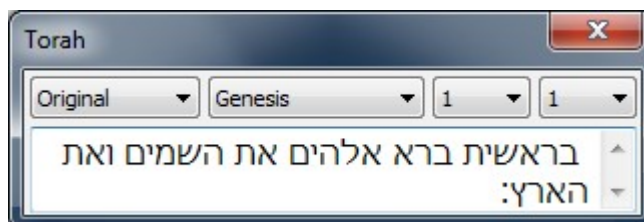
Pomocí ovládacího prvku *RadioButton* je možné určit, zda bude prohledávání probíhat v načteném souboru (*in file*) nebo v do programu zabudované Tóře (*in Torah*), která je ve variantě *Leningradského kodexu*.

Níže je ještě ovládací prvek *CheckBox*, který určuje, za si přejete smazat předchozí výsledky vyhledávání z příslušných *ListView*.



Ilustrace 3: Vzorový software - Vyhledávání dvou výrazů

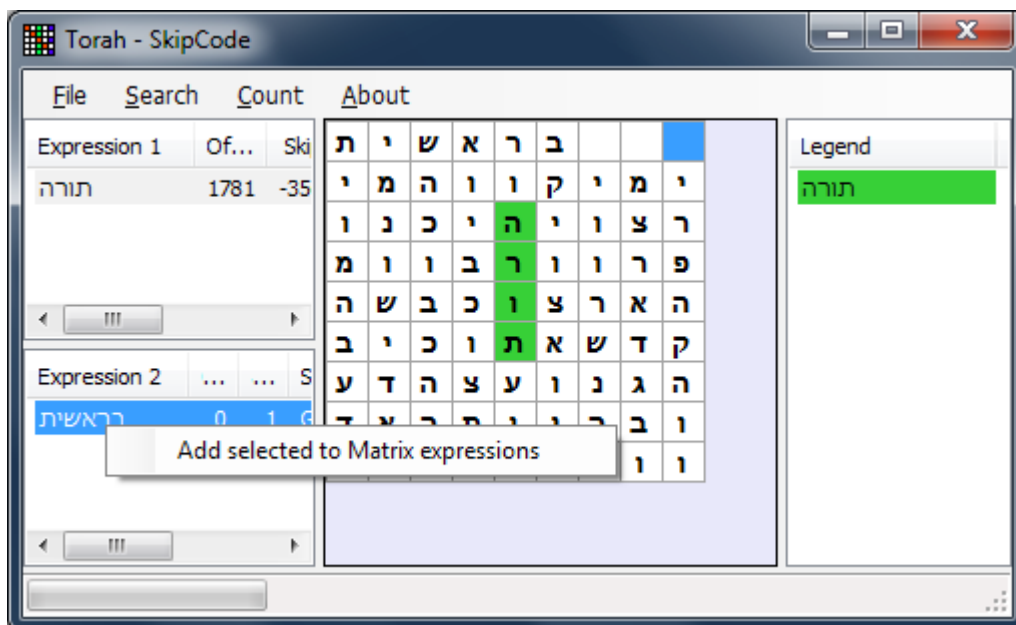
Po vykreslení matice můžeme dvojklikem otevřít Tóru (viz *Ilustrace 4*).



Ilustrace 4: Vzorový software - Tóra

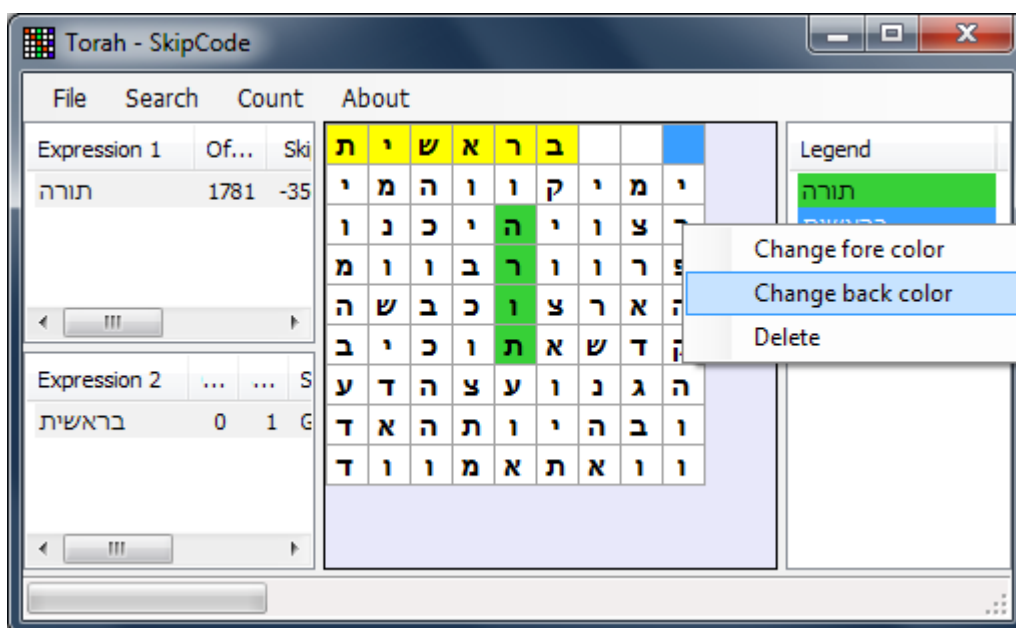
Také lze použít příkaz *Search->In matrix* k vyhledávání dalších výrazů ve zobrazené matici. Druhotně nalezené výrazy pak můžeme kliknutím na položku ve sloupci *Expression 2* dočasně zobrazit v matici. Pokud ji chceme do matice přiřadit, tak kliknutím pravým tlačítkem vyvoláme kontextové menu, v němž zvolíme položku *Add selected to matrix expressions* (viz *Ilustrace 5*), čímž se nám vybrané slovo ocitne v ovládacím prvku *List-*

View na pravé straně hlavního okna programu ve sloupci *Legend*, který slouží k vypisání legendy zobrazené matice.



Ilustrace 5: Vzorový software - Okno programu

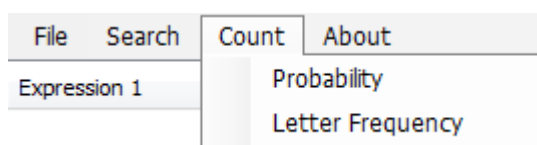
Legendu můžeme dále upravovat opět pomocí kontextového menu (viz *Ilustrace 6*). Můžeme změnit barvu písma (*Change fore color*), nebo barvu pozadí (*Change back color*), nebo položku ze seznamu odstranit (*Delete*).



Ilustrace 6: Vzorový software - Práce s legendou

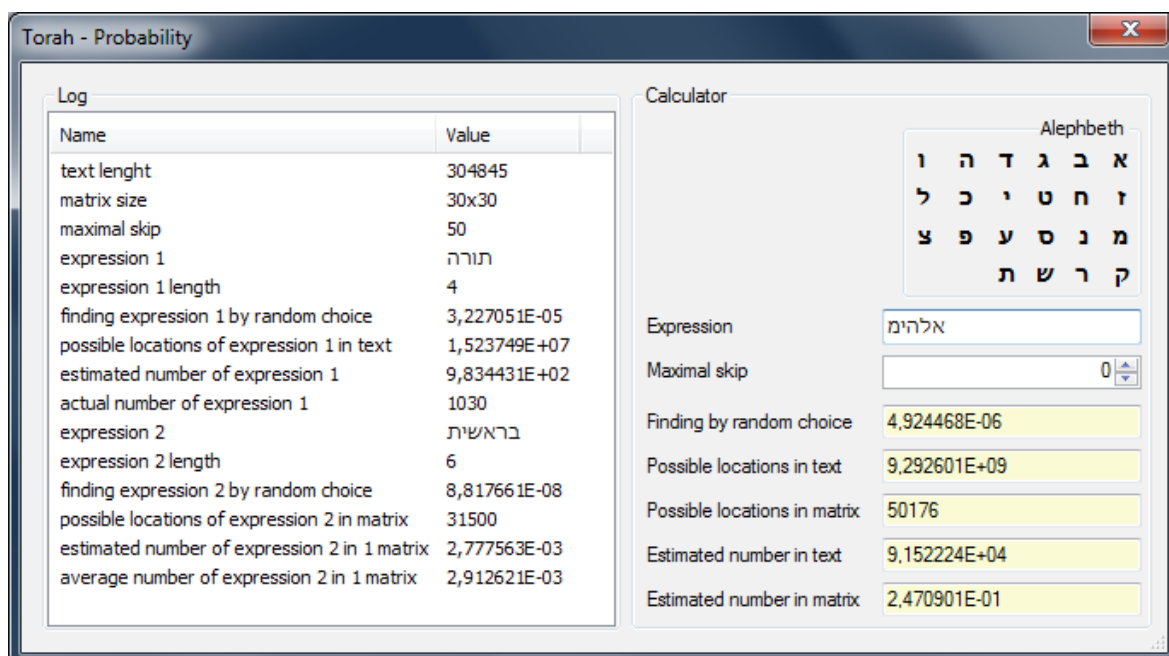
Jakmile je matice opatřena vyhovující legendou, můžeme provést export do formátu webových stránek příkazem **File->Export to html**. Při exportu se vypíší všechny údaje, které souvisí s daným vyhledáváním, včetně výpočtů. Html soubor je možné vytisknout z prohlížeče, nebo přímo z rozhraní programu pomocí příkazu **File->Print**. K dispozici jsou také další tiskové dialogy.

Výpočty je možné zobrazit i pomocí příkazu **Count->Probability** (viz *Ilustrace 7*).



*Ilustrace 7: Vzorový software - Nabídka Count*

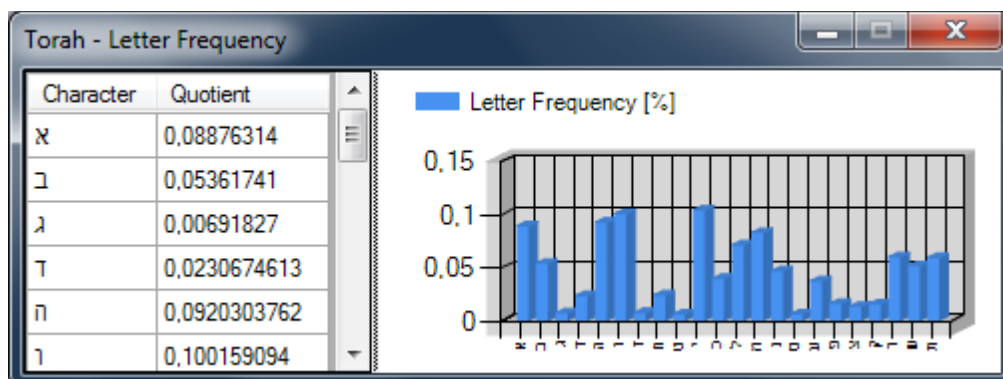
Po kliknutí se zobrazí okno (viz *Ilustrace 8*), ve kterém budou vypsány výsledky všech dostupných výpočtů. V témže okně je také možné nechat si dopředu spočítat, jaký může být očekávaný výsledek vyhledávání libovolného výrazu v naposledy prohledávaném textu či matici.



*Ilustrace 8: Vzorový software - Zobrazení výpočtů*

Pro načtený text se dá vykreslit frekvenční charakteristika příkazem **Count->Letter frequency**. V příslušném okně (viz *Ilustrace 9*) bude zobrazena i tabulka, ze které je možné

kopírovat relativní četnosti písmen.



Ilustrace 9: Vzorový software - Frekvenční charakteristika textu

Logo a informace o programu se zobrazí příkazem *About*.

### 3.3.2 Klávesové zkratky

<i>Alt+F</i>	Otevřít nabídku <i>File</i>
<i>Alt+S</i>	Otevřít nabídku <i>Search</i>
<i>Alt+C</i>	Otevřít nabídku <i>Soubor</i>
<i>Alt+A</i>	Otevřít dialogové okno <i>About</i>
<i>Ctrl+O</i>	Otevřít dialogové okno pro načtení neupraveného textového souboru
<i>Ctrl+Shift+O</i>	Otevřít dialogové okno pro načtení upraveného textového souboru
<i>Ctrl+E</i>	Exportovat dostupné údaje do html
<i>Ctrl+P</i>	Tisknout export
<i>Ctrl+Shift+P</i>	Zobrazit náhled pro tisk
<i>Ctrl+Shift+F</i>	Otevřít dialogové okno pro vyhledávání jednoho či dvou výrazů
<i>Ctrl+F</i>	Otevřít dialogové okno pro vyhledávání ve zobrazené matici
<i>Alt+F4</i>	Konec programu

### 3.3.3 Systém souborů

V adresáři programu je několik složek. S výjimkou složek *adapted* a *data* je možné se všemi volně manipulovat (přejmenovávat, mazat). Zde uvádím jejich seznam a popis:

<i>adapted</i>	- soubory upravené pro účely vyhledávání; mají příponu <i>.dat</i>
<i>data</i>	- soubory vestavěné Tóry (Leningradský kodex)
<i>export</i>	- soubory <i>.htm</i> , jež byly vytvořeny exportem
<i>txt</i>	- neupravené textové soubory ( <i>.txt</i> ), které je možné použít k vyhledávání

## 4 VÝPOČTY

Než si vůbec uvedeme první vzoreček, je potřeba definovat si, jak budu označovat jednotlivé proměnné a funkce. Toto označování vychází částečně z označování v odborné literatuře<sup>23</sup> a částečně se jedná o můj vlastní systém, který slouží pouze k označování konkrétních věcí v této práci. Viz *Tabulka 3*.

*Tabulka 3: Seznam symbolů použitých pro výpočty*

Výraz	Význam	Odvození
$p()$	relativní počet (pravděpodobnost)	<i>probability</i>
$N()$	absolutní počet	<i>number of</i>
$L()$	délka, počet prvků množiny	<i>length</i>
$E$	hledaný výraz (množina jeho písmen)	<i>expression</i>
$E_{\square}$	vektor variant $E$ (množina unikátních písmen $E$ )	
$e_i$	$i$ -té písmeno hledaného výrazu	
$e_{[i]}$	$i$ -té unikátní písmeno hledaného výrazu	
$E1$	první hledaný výraz	
$E2$	druhý hledaný výraz	
$S$	množina skoků (jejich velikostí)	<i>skip</i>
$s_i$	konkrétní skok (jeho velikost)	
$S_{\max}$	maximální skok	
$S_{\min}$	minimální skok	
$L(S)$	absolutní počet skoků pro daný ofset	
$T$	prohledávaný text (množina jeho písmen)	<i>text</i>
$t_i$	$i$ -té písmeno textu	
$t_{[i]}$	$i$ -té unikátní písmeno textu	
$L(T)$	počet písmen textu	
$N(t_{[i]})$	absolutní počet $i$ -tého unikátního písmene textu	
$p(t_{[i]})$	relativní počet $i$ -tého unikátního písmene textu	
$O$	množina ofsetů pro určení aktuální pozice v textu	<i>offset</i>
$o_i$	hodnota $i$ -tého ofsetu	
$L(O)$	počet možných ofsetů	
$M$	matice (tabulka) ELS (množina jejích písmen)	<i>matrix</i>
$m_{rc}$	prvek matice (písmeno)	<i>row, column</i>
$W(M)$	šířka $M$	<i>width</i>

23 Např. [1]

Výraz	Význam	Odvození
H(M)	výška M	<i>height</i>
D	množina směrů pro pohyb v tabulce M z jednoho prvku na druhý	<i>direction</i>
$d_i$	i-tý směr pro pohyb v tabulce M z jednoho prvku na druhý	
L(D)	počet možných směrů	

#### 4.1 Pravděpodobnost nálezu výrazu náhodným výběrem písmen z textu

Pro začátek zkusme předpokládat, že chceme pouze určit pravděpodobnost, že libovolné písmeno textu  $t_i$  bude odpovídat hledanému písmenu výrazu  $e_i$ . Tady nám nejlépe pomůže, když si spočítáme relativní četnost výskytů daného písmene  $t_{ij}$  v textu  $T$ . To se udělá tak, že nejprve spočítáme tzv. absolutní četnost, neboli konečný počet všech  $t_{ij}$  a to pak vydělíme celkovým počtem neboli absolutní četností všech písmen v prohledávaném textu. Když ten postup aplikujeme na všechna jednotlivá písmena a zapíšeme to do tabulky, získáme tím vlastně frekvenční charakteristiku (viz *Tabulka 4*).

Tabulka 4: Frekvenční charakteristika textu Tóry

$t_{ij}$	$N(t_{ij})$	$p(t_{ij})$
א	25 896	0,088 115 200
ב	15 663	0,053 295 813
ג	1 959	0,006 665 805
ד	6 794	0,023 117 650
ה	26 927	0,091 623 340
ו	29 446	0,100 194 632
ז	2 070	0,007 043 500
ח	6 943	0,023 624 646
ט	1 598	0,005 437 446
י	30 788	0,104 760 997
כ	11 541	0,039 270 062
ל	20 790	0,070 741 235
מ	24 408	0,083 052 047
נ	13 716	0,046 670 841

$t_{[i]}$	$N(t_{[i]})$	$p(t_{[i]})$
ס	1 806	0,006 145 198
ע	10 881	0,037 024 309
פ	4 607	0,015 676 040
צ	3 869	0,013 164 879
ק	4 459	0,015 172 447
ר	17 585	0,059 835 720
ש	15 041	0,051 179 361
ת	17 101	0,058 188 834
<b>celkem</b>	<b>293 888</b>	<b>1,000 000 000</b>

Když tedy známe relativní počet jednotlivých písmen, můžeme říci i to, že víme, jaká je pravděpodobnost, že při náhodném výběru z textu vytáhneme právě některé z písmen, které jsme si předem určili. Nám jde ale o to, abychom získali několik konkrétních písmen, což znamená, že budeme muset jejich relativní počty mezi sebou vynásobit. Jednotlivé výběry písmen jsou totiž na sobě nezávislé a teorie pravděpodobnosti říká, že chceme-li určit pravděpodobnost, že nezávislé jevy nastanou současně, musíme udělat součin jejich jednotlivých pravděpodobností, což se dá také zapsat jako produkt:

$$p(E) = \left( \prod_{i=1}^{L(E)} P(e_i) \right) \quad (1)$$

Ještě pro úplnost se ale zkusme zamyslet, jestli bychom neměli nějak zahrnout vliv pořadí písmen. Uvažujme takto: když chceme současně vytáhnout písmena "a" a "b", pravděpodobnost bude součinem pravděpodobností, že vytáhneme "a", a že vytáhneme "b". Co když ale vytáhneme písmena "b" a "a", tedy ta samá, ale v opačném pořadí? Nám přece o pořadí jde, jelikož my chceme poskládat konkrétní výraz!

Odpověď je kupodivu taková, že bychom si vůbec neměli lámat hlavu nad tím, kolik máme možností, že bude pořadí správné, a kolik je celkově všech pořadí, která mohou náhodně vybraná písmena mít. Vysvětlení je takovéto: Předně by nás mělo zarazit už to, že určujeme pravděpodobnost současného nastání několika jevů, a jestliže něco nastává současně, nemá to žádné pořadí. Ale ani pokud bychom se tímto nenechali přesvědčit, je tu další způsob, jak se na to podívat: Řekněme, že hledáme na konkrétním místě první písmeno. Pravděpodobnost, že ho najdeme, známe. Ve stejnou chvíli hledáme na jiném místě druhé písmeno a i u něj pravděpodobnost nálezu známe. Že uspějeme v obou případech, je vyjád-

řeno součinem. Tím, že nález těchto písmen v jiném pořadí je dán stejným součinem, se nesmíme vůbec nechat zmást.

## 4.2 Odhad absolutního počtu nálezů výrazu ve zvoleném textu

Když tedy známe pravděpodobnost nálezu náhodným výběrem písmen z textu, můžeme se pokusit o odhad celkové četnosti nálezů. Půjde vlastně o obrácený postup, než když jsme počítali relativní četnost jednotlivých písmen: Nyní víme, jak spočítat pravděpodobnost, že při jednom skoku z jedné pozice něco najdeme, takže musíme spočítat, kolik těch skoků z kolika pozic vlastně bude a tato čísla mezi sebou vynásobit.

Předně je třeba si uvědomit, že vybírání písmen z textu  $T$  probíhá podle určitých pravidel, která jsou odvozena od vyhledávacího algoritmu. V mém programu, který je součástí této práce, dochází v použitém algoritmu k několika posunům po textu, které musíme zahrnout do našich výpočtů. První posun spočívá v tom, že se prochází celý text, písmeno po písmenu, a každé písmeno  $t_i$  se porovnává s  $e_l$ . Zkusme si proto na chvíli představit, že jsme ve fázi, kdy ofset  $o_i = 0$ , tzn. jsme na začátku textu a další  $o_i$  nás ještě nezajímají.

Další posun po textu probíhá formou skoků. Skoků je vždy konečný počet  $L(S)$  a v mém algoritmu se postupuje od  $s_{max}$  do  $s_{min}$ . Je samozřejmě možné postupovat i opačně - to je úplně jedno a na výpočty to nemá vliv. Pokud jde o minimální skok  $s_{min}$ , tak ten je vždy roven 1. Maximální skok  $s_{max}$  je potřeba pro každý ofset  $o_i$  znovu spočítat. My ale máme  $o_i = 0$ , takže  $s_{max}$  se spočítá takto:

$$o_i=0: \quad L(S)=s_{max}=floor\left(\frac{L(T)-1}{L(E)-1}\right) \quad (2)$$

kde *floor* znamená, že podíl se zaokrouhluje dolů.

Nyní se vraťme k posunu v textu formou skoku. Pro všechny skoky bude tedy absolutní četnost nálezů výrazu vyjádřena sumou:

$$N(E \in S) = \sum_{i=1}^{L(S)} p(E) \quad (3)$$

Z rovnice vidíme, že v každém skoku provádíme vyhledávání se stejnou pravděpodobností, a že čím víc skoků provádíme, tím větší bude absolutní četnost nálezů.

Nakonec už nám zbývá použít tyto výpočty také pro ostatní ofsety  $O$ . Prakticky se nám změní jenom výpočet maximálního skoku:

$$L(S) = s_{max} = \text{floor} \left( \frac{L(T) - o_i - 1}{L(E) - 1} \right) \quad (4)$$

A teď už jenom vypočítáme odhad absolutní četnosti nálezů výrazu  $E$  v textu  $T$ :

$$N(E \in T) = 2 \cdot \sum_{j=1}^{L(O)} \left( \sum_{i=1}^{L(S)_j} p(E) \right) \quad (5)$$

kde 2 na začátku levé strany značí, že vyhledávání probíhá oběma směry. Dále je také potřeba říct, že počet ofsetů se spočítá jako:

$$L(T) \geq L(E): \quad L(O) = L(T) - L(E) + 1 \quad (6)$$

a to kvůli tomu, že nemá smysl výraz hledat v úseku textu, jenž je kratší než výraz sám, jinými slovy vyhledávání skončí v momentě, kdy přestane platit, že:

$$s_{max} \leq s_{min} = 1 \quad (7)$$

### 4.3 Odhad absolutní četnosti nálezů výrazu v tabulce

Vyhledávání druhého výrazu probíhá odlišně, proto musíme také vycházet z odlišného algoritmu. Místo textu  $T$  zde máme tabulku okolního textu (jež si budeme pro výpočet označovat matice  $M$ ), která má dva rozměry, šířku  $W(M)$  a výšku  $H(M)$ . Algoritmus přitom nepostupuje pouze jedním směrem, ale z každého jednoho prvku matice  $m_{rc}$  postupujeme všemi možnými směry, které vedou na všechna ostatní písmena.

Jeden jediný směr  $d_i$  nám tedy slouží k tomu, abychom zjistili, jestli když po něm půjdeme  $(L(E) - 1)$ -krát, tak dostaneme hledaný výraz  $E$ . Z toho logicky vyplývá, že některých  $d_i$  se budeme muset zbavit, protože jsme omezeni hranicemi matice  $M$ . Ale jak se jich zbavit a spočítat správně  $L(D)$ , které budeme dále potřebovat? Nejintuitivnější řešení nejspíš bude projít všechny směry pro každou buňku matice  $M$  a vybrat ty, které vyhovují. To samozřej-

mě nemá smysl provádět jinak, než za pomoci výpočetní techniky. Při tomto procházení taky nezapomeňme vypočítat počet možných skoků a vynásobit toto číslo pravděpodobností nálezů výrazu  $E$  v textu.

Po odstranění neplatných směrů z množiny  $D$  se odhad absolutního počtu nálezů pro všechny platné směry spočítá:

$$N(E \in M) = \sum_{j=1}^{L(D)} \left( \sum_{i=1}^{L(S)_j} p(E) \right) \quad (8)$$

Všimněme si, že v rovnici 8 je velmi podobná rovnici 5, ale není v ní násobení dvěma. To proto, že tentokrát je vyhledávání pozpátku zahrnuto v tom, že v algoritmu vyhledáváme všemi směry.

Poznámka: Se výše zmíněným postupem však vzniká jeden problém, který spočívá v tom, že ne všechny matice jsou vyplněny do všech okrajů, jelikož některé hodnoty skoků jsou tak velké, že není možné doplnit všechny řádky pod a nad nalezeným výrazem okolním textem, který by odpovídal danému skoku. Řešením by bylo počítat odhad pro každou matici zvlášť, ale to by v některých souvisejících výpočtech znamenalo znát dopředu každou matici, což není možné.

#### 4.4 Odhad absolutní četnosti matic s oběma výrazy

Původně jsem ve vzorovém softwaru zavedl také výpočet, který měl vyjádřit celkový počet matic, ve kterých se budou nalézat oba hledané výrazy, ale pak jsem zjistil, že je tento výpočet natolik nepřesný a zavádějící, že jsem se rozhodl jej nepoužít. Přesto si myslím, že nebude na škodu, když zmíním důvody, proč jsem jej nepoužil.

Nejprve však vysvětlím, jak měl výpočet vypadat. Uvažoval jsem tak, že když bude v jedné matici odhadovaný počet nálezů druhého výrazu například 0,5, bude to znamenat, že celkový počet matic s oběma výrazy bude roven polovině matic pouze s prvním výrazem (jednalo by se tedy o součin těchto dvou čísel). Dále, že jestliže bude odhadovaný počet druhých výrazů větší než jedna, bude to znamenat, že matic s oběma výrazy bude tolik, kolik je matic s prvním výrazem, jelikož nález druhého výrazu je odvislý od vzhledu matice vygenerované na základě prvního výrazu, tudíž v žádném případě nemůže být víc matic s oběma výrazy, jako matic s prvním výrazem, takže součin by nepřipadal v úvahu.

Dále tu byla otázka, jestli bych měl použít odhadovaný nebo skutečný počet matic pouze s prvním výrazem. Kdybych použil odhadovaný, činil bych odhad na základě odhadu, čímž bych získal značnou nepřesnost. Kdybych naopak použil skutečný počet, nezískal bych odhad, kolik najdu matic s oběma výrazy, ale odhad, v kolika maticích s prvním výrazem bude i druhý výraz - a v tom je sice malý, ale podstatný rozdíl.

Navíc je tu také již zmíněná skutečnost, že ne všechny matice jsou vyplněny po všechny okraje, což také přispívá k nepřesnosti.

## 4.5 Důležité poznámky

### 4.5.1 Co se nedá z výpočtů vyčíst

Je třeba zdůraznit, že výpočty nám mohou říct pouze jediné - jaká je pravděpodobnost, resp. odhadnutý absolutní počet nálezu konkrétního předem vybraného výrazu v tabulce resp. v textu. Ve výpočtech není zahrnuto to, že když například hledáme „prorocství“ o druhé světové válce, že jsme vyzkoušeli nejprve najít slovo „Hitler“ a pak na stejném místě ještě „Adolf“ a „válka“ a taky „oběti“, holokaust,“ a „židé“, přičemž ne vždy jsme uspěli. Tím, že nejprve najdeme dvě slova, která spolu souvisejí a pak se ještě snažíme najít ve všech tabulkách, ve kterých se tato slova nalézají, ještě něco, co by se k tomu hodilo, vlastně pravděpodobnost ještě zvyšujeme, ale to ve výpočtech zahrnuto není, jelikož výpočty se týkají pouze zpětného vyhodnocení, nikoli všech cest, které před námi ležely (a mezi nimiž byla spousta slepých ramen), když jsme s vyhledáváním začínali.

Tato skutečnost je ostatně známa i z běžného života a projevuje se tak, že když se ohlédneme zpět, zdají se nám věci jasnější (protože známe důsledky), než když jsme stáli na začátku a dívali se nervózně do nenapsané budoucnosti. Stejně je tomu při hledání šifer - když začínáme hledat, nevíme, co nakonec najdeme, ale když po mnoha hodinách hledání získáme tabulku, ve které je třeba 6 výrazů, které předpovídají, že se Adolf Hitler bude snažit vyhladit půlky Evropy, vypadá to na první pohled jako něco neskutečného a zázračného.

### 4.5.2 Co se naopak z výpočtů vyčíst dá

Výpočty byly navrženy tak, abychom podle nich mohli učinit určitý odhad, který pak porovnáme se skutečností, takže pak bude viditelné, zda se skutečný počet nálezů dal předpovídat, a nebo máme před sebou upravený text, do kterého někdo úmyslně ukryl víc slov, než je statisticky obhajitelné jako náhoda.

V malém měřítku bude naše pozorování samozřejmě zkreslené, jelikož jedno skryté slovo se mezi - dejme tomu - pěti náhodně se vyskytujícími snadno ztratí. Ale i tak nám výpočty řeknou aspoň to, že ten, kdo se se snažil vytvořit skrytou zprávu, nebyl moc chytrý, protože si neuvědomil, že jeho poselství nebude rozlišitelné od těch, která se v textu vyskytují přirozeně.

Tato skutečnost má podstatné důsledky, protože je tím vyvráceno tvrzení některých nadšenců do metody přeskokování písmen, že existence tolika šifer, které byly v Tóře nalezeny pomocí výpočetní techniky, je podmíněna existencí bytosti, která byla nadměrně inteligentní, nebo měla přinejmenším před 3000 lety k dispozici výkonný počítač. Boží či mimozemský zásah tedy můžeme s klidem přestat považovat za nezbytný.

Abychom mohli s jistotou tvrdit, že námi nalezené šifry nemají svůj původ ve statisticky obhajitelné náhodě, museli by například být mnohem delší, než je délka bezvýznamných nálezů, a měly by v lepším případě obsahovat méně častá písmena, nebo být nalezena v kratším textu (ale ne zkráceném až po nález v delším textu).

## 5 NĚKTERÉ ŠIFROVÉ TABULKY A JEJICH ROZBOR

Takto kapitola by měla nejen demonstrovat, jak použití metody přeskokování písmen vypadá v praxi, ale také provést ukázkový rozbor některých šifrovaných tabulek (matic), aby bylo více zřejmé, jak lze s výpočty ve vzorovém softwaru zacházet.

### 5.1 Světová válka

Jako první ukázkou jsem vybral matici textu, kterou Michael Drosnin uvádí ve své knize *The Bible Code 1* v páté kapitole, kde uvádí různá „proroctví“, týkající se nedávné doby.<sup>24</sup> Výřez z nalezené tabulky je znázorněn v *Ilustraci 10*.

ו	י	כ	ת	ו	א	ת	כ	מ	ב	ש	ע	י	ר	ע	ד	ח	ר	מ	ה	ו	ת
ל	ח	צ	י	ש	ב	ט	ה	מ	נ	ש	ה	כ	ל	ח	ב	ל	ה	א	ר	ג	ב
ש	מ	א	ל	ה	י	מ	מ	ע	ש	ה	י	ד	א	ד	מ	ע	צ	ו	א	ב	ב
ה	ל	ב	ב	ז	ה	ל	ה	מ	ל	י	ל	ר	א	ה	א	ת	י	ו	ל	ש	מ
צ	ר	ע	ה	י	ש	ל	ח	י	ה	ו	ה	א	ל	ה	י	כ	ב	מ	ע	ד	א
ה	ו	ה	ע	ל	י	כ	מ	ל	ה	ש	מ	י	ד	א	ת	כ	מ	ו	י	ש	מ
ל	כ	מ	פ	נ	י	פ	ת	ה	ל	ב	ב	כ	מ	ו	ס	ר	ת	מ	ו	ע	ב
א	ח	ר	י	כ	ע	ד	ע	ו	ל	מ	כ	י	ת	ע	ש	ה	ה	ט	ו	ב	ו
ע	ר	י	כ	ו	א	כ	ל	ו	ו	ש	ב	ע	ו	ל	מ	ע	נ	י	ב	ר	כ
ה	ג	ד	ל	כ	ו	ש	מ	ע	ת	ו	ד	ר	ש	ת	ה	י	ט	ב	ו	ה	נ
ו	ה	א	ל	ה	י	כ	ו	ל	ל	כ	ת	ב	ד	ר	י	כ	ו	כ	ל	ה	י
ו	א	ת	ו	ל	א	י	ש	מ	ע	א	ל	י	ה	מ	ו	ת	פ	ש	ו	ב	ב

*Ilustrace 10: Šifrová tabulka - světová válka, udeří na ně*

#### Legenda:

světová válka (ofset: 8198, skok: 2839)

udeří na ně (ofset: 16713, skok 1)

**Podrobnosti (Deuteronomium, Korenské vydání):** viz Tabulka 5.

*Tabulka 5: Šifrová tabulka - světová válka, udeří na ně (podrobnosti)*

délka textu	54892
rozměry matice	30x30

maximální skok	0
první výraz	מלהמתעלמ
délka prvního výrazu	8
náhodný nálezn prvního výrazu	1,06E-10
možná rozložení prvního výrazu v textu	1,88E+8
odhadnutý počet nálezů prvního výrazu	3,98E-2
skutečný počet nálezů prvního výrazu	1
druhý výraz	יכמלהשמיד
náhodný nálezn druhého výrazu	2,83E-11
možná rozložení druhého výrazu v matici	12096
odhadnutý počet nálezů druhého výrazu v jedné matici	3,42E-7
průměrný počet nálezů druhého výrazu v jedné matici	1,00

Nyní se podívejme blíže na získaná čísla. Čísla se týkají pouze knihy Deuteronomium, a to z toho důvodu, že verze Tóry, kterou používám ve vzorovém softwaru, je jiná než ta, kterou použil Michael Drosnin<sup>25</sup>, a já jsem si načel z externího souboru pouze jednu knihu v jeho verzi.

Odhadnutý počet nálezů prvního výrazu vychází  $3,98 \cdot 10^{-2}$ . V celé Tóře pak odhad vyšel 1,66, což přibližně odpovídá skutečnému počtu nálezů.

Dále je tu odhadnutý počet nálezů druhého výrazu v matici, který vyšel dokonce  $3,42 \cdot 10^{-7}$ , což je hodně málo, takže správně bychom neměli najít nic. Jak je ale možné, že jsme něco přece jenom našli? Je to vlastně prosté, stačí si všimnout, že výraz byl nalezen při čtení se skokem o velikosti 1, což znamená, že se normálně vyskytuje v prohledávaném textu. Michael Drosnin tedy určitě druhý výraz hledal až potom, co si nechal vykreslit tabulku s prvním výrazem, a pak se díval, jestli v rádcích, kde je vždy srozumitelný text, nenajde něco, co by s prvním výrazem souviselo.

A takovýchto jednoduchých matic, ve kterých je jeden výraz svisle a všechny, nebo přinejmenším většina ostatních byly nalezeny ve vodorovném směru, je v Drosninových knihách opravdu hodně.

<sup>25</sup> Ve vzorovém softwaru je použit Leningradský kodex, kdežto Drosnin použil Korenské vydání

### 5.2 William Shakespeare

Následující šifra je Drosninem uvedena v úvodní kapitole, kde Drosnin demonstruje, co všechno se dá metodou přeskokování písmen v Tóře najít.<sup>26</sup> Výřez z nalezené tabulky je znázorněn v *Ilustraci 11*.

א	ו	נ	ה	כ	ה	נ	ר	ה	א	ל	ש	ד	ק	ה	י	ד	ג	ב	ת	א	ש	
כ	ה	נ	ר	ה	א	י	נ	ב	ו	כ	ו	ע	ר	ש	ו	א	ה	ל	ע	מ	י	צ
א	י	נ	פ	ל	ו	ת	א	ט	ח	ש	ו	ו	ש	א	ר	ל	ע	ו	ד	י	ת	
נ	ו	ו	ע	ו	ו	ב	א	ב	ת	א	ט	ח	ה	מ	ד	מ	נ	ה	כ	ה	ק	
ה	ת	ל	ס	מ	ו	צ	מ	ק	ב	מ	מ	נ	ו	מ	מ	י	ר	ה	ו	ח	ז	
ת	א	ב	י	ק	ר	י	מ	ה	ר	מ	א	ל	ל	א	ר	ש	י	י	נ	ב	ל	
ה	ל	ע	ה	ל	ע	ה	ל	ב	ז	מ	ה	ר	ט	ק	י	מ	ו	ה	י	פ	כ	
א	ל	ו	נ	ר	ה	א	ל	א	ה	ש	מ	ר	מ	א	י	א	מ	ע	ב	ר	א	
ע	ג	נ	ה	ל	כ	מ	ל	כ	מ	ה	מ	י	א	מ	ע	ט	מ	א	ר	א	ל	
י	א	ל	נ	ה	כ	ה	ו	א	מ	ט	ו	ו	ר	ש	ב	ר	ו	ע	ב	א	ו	
ג	נ	ה	ת	ר	א	מ	מ	ע	ת	צ	ר	ע	ה	כ	א	ל	מ	ל	ר	ו	ה	
י	ל	א	מ	ש	ה	פ	ו	כ	ל	ע	ר	ש	ר	א	נ	ש	ה	נ	מ	ת	י	
ו	ר	ו	ט	ה	ר	ו	מ	י	י	ח	י	מ	י	מ	ב	ו	ר	ש	ב	צ	ח	
ק	ל	כ	ד	ע	ב	ו	ו	ת	י	ב	ד	ע	ב	ו	ו	ד	ע	ב	ר	פ	כ	
ב	מ	ת	מ	ב	ש	ר	י	ש	ר	י	מ	צ	ר	צ	מ	צ	ר	א	ה	א	כ	
י	ל	מ	ו	ש	א	ת	א	א	י	ב	ה	ו	ה	ש	פ	ה	א	ל	י	כ	ו	
א	ש	ב	ד	ו	ב	ל	ח	ב	ז	צ	ר	א	ה	ת	א	ת	א	ל	ש	ר	ל	
ו	ה	ו	ה	י	ל	ו	מ	י	ר	י	ר	ש	ר	א	ת	א	ל	א	ר	י	י	
י	נ	ב	ל	א	ר	ב	ד	ר	מ	א	ל	ה	ש	מ	ל	א	ה	ו	ה	י	ר	
ל	א	ה	ו	ה	י	י	נ	א	י	כ	ה	י	ה	י	ה	ז	ר	א	כ	א	ג	
א	ו	ו	ת	ו	ו	פ	ש	ל	א	ב	א	ו	ו	ע	מ	ו	י	נ	ב	ו	א	
ת	א	י	ת	ר	ס	י	ו	י	ר	ק	ת	מ	ח	ב	מ	כ	מ	ע	י	ת	כ	
ה	י	ל	ש	ד	ק	ל	ב	י	ב	ו	ת	א	צ	ב	ה	ד	ש	ה	ה	ה	י	
ע	מ	ו	ה	ו	ש	מ	י	ר	ש	ר	נ	ב	מ	ת	ו	מ	ש	ר	פ	ס	מ	
י	ע	ג	פ	ר	ש	א	י	נ	ב	ל	א	י	ש	ו	ר	א	ה	א	ט	ה	י	
ק	ה	ר	ז	ה	ו	ל	א	ר	א	י	י	נ	ב	ת	ר	מ	ש	ל	מ	ש	ד	

Ilustrace 11: Šifrová tabulka - Shakespeare, Macbeth, Hamlet

**Legenda:**

Shakespeare	(ofset: 187821, skok: -2085)
Macbeth	(ofset: 150287, skok: -2084)
Hamlet	(ofset: 162789, skok: -6252)

<sup>26</sup> [2], str. 31

pódium (ofset: 166971, skok: -2085)

**Podrobnosti (Tóra, dvě různé verze):** viz Tabulka 6.

Tabulka 6: Šifrová tabulka - Shakespeare, Macbeth, Hamlet (podrobnosti)

	Koren	WLC
délka textu	304805	304845
rozměry matice	50x50	50x50
maximální skok	0	0
první výraz	שקספיר	שקספיר
délka prvního výrazu	6	6
náhodný nálezn prvního výrazu	4,60E-10	4,61E-10
možná rozložení prvního výrazu v textu	7,74E+9	7,74E+9
odhadnutý počet nálezů prvního výrazu	7,12	7,14
skutečný počet nálezů prvního výrazu	19	4
druhý výraz	מקבת	מקבת
náhodný nálezn druhého výrazu	4,00E-6	4,00E-6
možná rozložení druhého výrazu v matici	693056	693056
odhadnutý počet nálezů druhého výrazu v jedné matici	2,78	2,77
průměrný počet nálezů druhého výrazu v jedné matici	0,47	0

Tentokrát uvádím pro srovnání podrobnosti pro dvě různé verze Tóry. Jak se můžete přesvědčit, odhady vychází velmi podobně, ale skutečné výsledky už si tak podobné nejsou. První výraz byl v Korenském vydání nalezen 19-krát a v Leningradském kodexu jen 4-krát, přičemž odhad byl okolo 7. Na první pohled by se mohlo zdát, že Korenské vydání je nějak zvláštní, jestliže v něm nálezů bylo skoro třikrát více, než předpověděl odhad. Ve skutečnosti je ale takováto odchylka úplně běžná a dochází k ní často u výrazů, které se vyskytují v malém počtu.

Také si povšimněme, jakou formou se Drosnin rozhodl zapsat anglická slova. Slova *Macbeth* a *Hamlet* má zapsány běžnou formou, ale slovo *Shakespeare* zapsal שקספיר místo běžnějšího שייקספיר, které by totiž vůbec nenašel, jelikož jeho odhadnutá četnost je například v Korenském vydání  $5,71 \cdot 10^{-2}$ . V hebrejštině je skutečně možné některá písmena vynechat, říká se jim podklady a slouží ke zvýraznění samohlásek ve slovech, jejichž

čtení je sporné. Například písmeno *jód*, které Drosnin na začátku slova dvakrát vynechal, slouží jako podklad pro samohlásky *i* či *e*. To ale znamená, že druhé *jód* Drosnin vynechat neměl, protože sloužilo jako souhláska - nikoli jako podklad.

Avšak i kdyby místo druhého *jód* vynechal třetí, které jako podklad slouží, stejně by „Hamleta” i „Macbetha” vedle „Shakespeara” našel, jelikož takto krátká slova se dají najít v matici hebrejského textu úplně snadno. A pokud jde o výraz „pódium”, tak takové tří-písmenné slovo se může v matici 30x30 vyskytovat klidně i stokrát.

### 5.3 Jicchak Rabin

Za pozornost jistě stojí i šifra, která Michaela Drosnina ovlivnila ze všech nejvíc, šifra, díky které se mu podařilo předpovědět atentát na izraelského premiéra Jicchaka Rabina.<sup>27</sup> Výřez z nalezené tabulky je znázorněn v *Ilustraci 12*.

א	ל	ו	ש	ו	י	ח	נ	ו	ב	ר	פ	י												
צ	ו	ה	י	ה	ו	ה	ל	ב	נ	ו	ת	צ	ל	פ	ח	ד	ל	א	מ	ר	ל	ט		
ו	ל	מ	ל	ח	מ	ה	י	ה	צ	ה	ו	י	ת	נ	ה	ו	ה	ו	ה	א	ל	ל		
ש	מ	ה	ר	ו	צ	ח	א	ש	ר	י	ר	צ	ח	ח	א	ת	ר	ע	ה	ו	ב	ב	ל	
ג	מ	א	ת	ה	צ	ר	ע	ה	י	ש	ל	ח	י	ה	ו	ה	א	ל	ה	י	ה	י	כ	ב
ש	מ	ר	ת	מ	ש	מ	ר	ת	ו	ו	ח	ק	ת	י	ו	ו	מ	ש	פ	ט	י	ו	ו	
מ	ו	צ	י	א	כ	מ	א	ר	צ	מ	צ	ר	י	מ	מ	ב	י	ת	ע	ב	ד	י	י	
א	ת	ה	א	ש	ה	ו	ס	ק	ל	ת	מ	ב	א	ב	נ	י	מ	ו	מ	ת	ו	ע	ע	
ו	ה	כ	ה	נ	י	מ	ב	נ	י	ל	ו	י	כ	י	כ	י	ב	מ	ב	ח	ר	י	ה	ו
י	ו	מ	ת	ו	א	ב	ו	ת	ע	ל	ב	נ	י	מ	ו	ב	נ	י	מ	ל	א	י	י	י
ת	כ	ש	ג	ר	א	ל	פ	י	כ	ו	ע	ש	ת	ת	ר	צ	א	נ	כ	א	ר	ו	ו	ו
ש	ר	א	נ	כ	י	מ	צ	ו	כ	ה	י	ו	מ	א	ת	ה	ו	ב	נ	י	כ	ב	ב	ב

Ilustrace 12: Šifrová tabulka - Jicchak Rabin

#### Legenda:

Jicchak Rabin (ofset: 254245, skok: 4772)  
 zabiják, který zabije (ofset: 259008, skok: 1)

Podrobnosti (Tóra, Korenské vydání): viz Tabulka 7.

Tabulka 7: Šifrová tabulka - Jicchak Rabin (podrobnosti)

délka textu	304805
rozměry matice	30x30
maximální skok	0
první výraz	יצחקרבינ
délka prvního výrazu	8
náhodný nálezn prvního výrazu	7,46E-12
možná rozložení prvního výrazu v textu	5,81E+09
odhadnutý počet nálezů prvního výrazu	8,67E-02
skutečný počet nálezů prvního výrazu	1
druhý výraz	רוצחאשרירצ ה
délka druhého výrazu	11
náhodný nálezn druhého výrazu	9,30E-16
možná rozložení druhého výrazu v matici	7200
odhadnutý počet nálezů druhého výrazu v jedné matici	6,70E-12
průměrný počet nálezů druhého výrazu v jedné matici	1

Jak je vidět, v tomto případě jsou rozdíly mezi odhadnutými a skutečnými nálezy opravdu velké. Na druhou stranu vše, co nějak souvisí s druhým výrazem, nesmíme brát za směrodatné už jen kvůli tomu, že výraz je v textu nalezen se skokem o velikosti 1 písmeno, takže i tady vidíme, že Drosnin pravděpodobně druhý výraz nehledal, ale jednoduše si jej přečetl až po vyobrazení matice textu obsahující jméno *Jicchak Rabin*. Jak je ale možné, že našel jméno izraelského premiéra, přestože pravděpodobnost takového nálezu byla odhadnuta na  $8,67 \cdot 10^{-2}$ ? Přiznám se, že pro to nemám žádné jiné vysvětlení, než že je to sice málo pravděpodobné, ale není to úplně nemožné.

Michael Drosnin ale tuto matici použil k tomu, že předpověděl událost, která se skutečně stala. Znamená to, že bychom měli onu malou pravděpodobnost přece jen považovat za důkaz? Osobně si myslím, že ne, a to hned z několika důvodů.

Předně se mi zdá, že stejně jako v mnoha jiných maticích, tak i v této, hrála velkou roli Drosninova fantazie. Ve mně například, by spojení frází „Jicchak Rabin“ a „zabiják, který zabije“, evokovalo spíše to, že tím zabijákem by měl být sám *Jicchak Rabin*, nikoli, že to on bude oním zabijákem zabit. Možná to Drosnin chápal tak, že když se tyto výrazy kříží, tak snad také zabiják zkříží cestu Jicchaku Rabinovi, což zase na druhou stranu neaplikuje

v žádných jiných maticích.

Je tedy vidět, že ani samotná skutečnost, že jsme našli související výrazy, nemusí ještě znamenat jednoznačně interpretovatelné sdělení. Kdybychom našli celé věty, jistě by to mělo jinou váhu, než když najdeme pouze úločky myšlenek, které si může každý individuálně poskládat do jednoho srozumitelného celku svým vlastním způsobem.

Dále byl chtěl poukázat na to, že samotná fráze „zabiják, který zabije“ může být v hebrejštině interpretována více způsoby. Původní antická hebrejšтина, na rozdíl od té moderní, vůbec nerozlišuje slovesné časy a způsoby. Onu frázi tedy můžeme také přeložit jako „zabiják, který by zabil“ nebo třeba „zabiják, který by byl zabil“. Sám Drosnin si do fráze přidal budoucí čas, a ve své knize uvádí překlad „zabiják, který bude zabíjet“. Pro úplný obrázek ještě dodejme, že z hebrejského originálu Tóry je tato fráze vzhledem ke kontextu celého oddílu překládána do moderních jazyků v podmiňovacím způsobu.

#### 5.4 René Moawad

*René Moawad* byl libanonský prezident, který vládl pouze 17 dní. Bylo to v roce 1989, od 5. do 22. listopadu, kdy na něj byl spáchán atentát - zabila jej exploze bomby, která vybuchla, když projížděl se svou kolonou aut západním Bejrútem. Společně s ním zemřelo také 23 dalších lidí.

„Proroctví“ o jeho zavraždění bylo nalezeno kritikem *Brendonem McKayem* v knize *Bílá velryba*, aby dokázal, že nálezy v Tóře nejsou nijak výjimečné.<sup>28</sup> Výřez z nalezené tabulky je znázorněn v *Ilustraci 13*.

```

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

```

*Ilustrace 13: Šifrová tabulka - René Moawad v Bílé velrybě*

#### Legenda:

Moawad (ofset: 812367, skok: -116726)

<sup>28</sup> Všechny nálezy: [3]

explodující bomba	(ofset: 812354, skok: 1)
René	(ofset: 228727, skok: -1)
auto	(ofset: 462192, skok: 116723)

**Podrobnosti (srovnání románu Bílá Velryba a Tóry):** viz Tabulka 8.

Tabulka 8: Šifrová tabulka - René Moawad v Bílé velrybě (podrobnosti)

	Moby Dick	WLC
délka textu	924956	304845
rozměry matice	30x30	30x30
maximální skok	0	0
první výraz	moawad	מואוואד
délka prvního výrazu	6	6
náhodný nález prvního výrazu	1,12E-8	1,50E-7
možná rozložení prvního výrazu v textu	7,13E+10	7,74E+9
odhadnutý počet nálezů prvního výrazu	1596	2,32E+3
skutečný počet nálezů prvního výrazu	1899	2611
druhý výraz	bomb	בומב
délka druhého výrazu	4	4
náhodný nález druhého výrazu	5,64E-7	2,37E-5
možná rozložení druhého výrazu v matici	89100	89100
odhadnutý počet nálezů druhého výrazu v jedné matici	5,02E-2	2,11
průměrný počet nálezů druhého výrazu v jedné matici	2,42E-2	8,92E-1

Tentokrát jsem provedl experiment, který má ukázat, jaké odlišnosti vzniknou, používali-li texty v různých jazycích. Při prvním hledání jsem použil originální anglickou verzi *Bílé velryby* (původním názvem *Moby Dick*), kterou jsem stáhl ze stránek *Brandona McKaye*<sup>29</sup>. Pro porovnání jsem stejný pokus provedl také na Tóře (*Leningradský kodex*), přičemž jsem použil všechny samohláskové podklady, abych získal slova stejných délek jako v angličtině.

Na vyhledávání s takto velkou četností je krásně vidět, jak přesně odhady vyšly. V *Bílé velrybě* měl být první výraz nalezen zhruba 1596 krát a nalezen byl 1899 krát. V Tóře byl odhad spočítán na 2324 nálezů a bylo jich učiněno 2611.

<sup>29</sup> Soubor je přiložen také u vzorového softwaru.

Někteří zastánci metody přeskakování písmen prohlašují, že Brendon McKay je podvodník, který velkou náhodou objevil něco málo v Bílé Velrybě, a myslí si, že může klamat veřejnost, když to používá jako důkaz, že objevy lze učinit všude. To je pravda jenom z poloviny. Ze srovnání hebrejského a anglického textu skutečně plyne, že hebrejský text Tóry je výrazně bohatší na domnělá „proroctví“, než text anglického románu, jenomže to není dáno zázračnými vlastnostmi Tóry, nýbrž menším počtem písmen v hebrejské abecedě. Přestože je Tóra zhruba třikrát kratší, než román Bílá velryba, odhady byly téměř dvakrát vyšší. Nemluvě také o možnosti manipulace s podklady samohlásek za účelem vytvoření více verzí téhož slova.

## ZÁVĚR

Během sbírání materiálů pro Teoretickou část a během vlastní práce v Praktické části jsem zjistil několik důležitých poznatků, které bych se nyní rád pokusil shrnout.

Ke běžně uznávanému tvrzení, že v Bibli šifry opravdu jsou, musím dodat také to, že tyto šifry jsou převážně hledány lidmi, kteří se nezajímají ani tak o jejich původ, jako spíše výklad, který by k nim připojili, což vede k tomu, že mnoho jejich objevů je vlastně učiněno navzdory tomu, že jim nepředcházelo samotné vytvoření šifer v minulosti.

Je velký rozdíl mezi myšlením člověka, který je zvyklý pracovat s exaktními vědami, a člověkem, který je při své práci zaměřen na hledání souvislostí mezi abstraktními pojmy. Právě proto dochází k tomu, že jsou jedni lidé schopni přijímat objevy učiněné metodou přeskakování písmen jako pravé, zatímco jiní se proti nim ohrazují, a prohlašují, že tomu přece nemůže nikdo rozumný věřit.

Během svých studií jsem si vyzkoušel uvažovat jako obě strany, a přiznám se, že nemůžu jinak, než přidat se k těm, kteří jsou ochotni se svých názorů pod tíhou argumentů vzdát, spíše než se jich držet za každou cenu, zatímco si vždy najdou způsob, jak se vyrovnat s názory těch, kdo s nimi nesouhlasí.

Proto také zavrhuji přístup Eliyaha Ripse, přestože si jej velmi vážím, a také přístup Michaela Drosnina, kterého bych se nebál označit za vědomého lháře, vzhledem k tomu, jaká tvrzení je ochoten předkládat veřejnosti, jen aby si udržel přízeň. Prohlašuje o sobě, že je skeptik, a že každou matici textu, kterou uvádí ve svých knihách má matematicky ověřenou, což jistě nemůže být pravda, když tomu ani sám nerozumí.

Naopak velmi oceňuji měsíce práce, které fenoménu *The Bible Code* věnoval Brandon McKay, aby dokázal, že nikdo, kdo má zájem udělat si objektivní pohled na celou věc, nemůže doopravdy věřit v její pravost. To se mi ostatně také potvrdilo při mém vlastním zkoumání.

V následujících odstavcích už tedy uvedu přehled toho, co považuji za klíčové informace ze všech bodů obou částí mé práce:

První námitkou proti samotné metodě přeskakování písmen by mělo být jistě to, že i kdyby byla univerzálně použitelná na biblický text, a bylo by díky ní skutečně možné odhalit osudy lidstva minulé i budoucí, stejně dnes nemáme k dispozici text, na který bychom ji mohli aplikovat, ale můžeme použít jen různé jeho varianty, které se liší na tolika místech, že

snad můžeme uznat pravost pouze šifer objevených H. M. D. Weissmandelem, jelikož se nacházejí vždy v malé vzdálenosti od začátku knih.<sup>30</sup>

Takzvané „objevy“ se dají vždy vysvětlit pomocí pravděpodobnostních a statistických výpočtů a dají se najít v jakémkoli dostatečně dlouhém textu. Pokud by měla v Bibli nalezená „proroctví“ opravdu pocházet od Boha nebo třeba od mimozemšťanů, určitě by nám je neukryli tak, abychom je nemohli odlišit od náhodně se vyskytujících výrazů - ledaže by to byli opravdu hloupí mimozemšťané.

S tím souvisí také to, že všechny nalezené výrazy jsou vždy krátké, tedy vyjadřují vždy samostatné pojmy, nikdy ne souvislá tvrzení, což znamená, že neexistuje objektivní cesta, jak údajná „skrytá poselství“ dát dohromady, ale velmi často to záleží na fantazii toho, kdo se pokouší o výklad, což vede ke značné subjektivitě.

A v neposlední řadě: napadnutelný je také postup, který je použit ke hledání souvisejících výrazů. Jestliže hledáme rovnou pojmy, které spolu souvisejí, nedá se říct, že bychom postupovali objektivní cestou. Správné by bylo najít nejprve všechno, co v dané matici dává smysl, a pak to kriticky zhodnotit. Když tedy například Drosnin našel v jedné matici slova „Shakespeare“ a „Hamlet“, svědčilo to pouze o tom, že našel jen to, co chtěl najít, místo toho, co tam opravdu bylo:

Nic, co by opravdu stálo za řeč.

---

<sup>30</sup> I když je rovněž pravda, že se nedají najít ve všech verzích Tóry.

## CONCLUSION

During gathering materials for Theoretical Part and during my own work in the Practical Part I have found out several important facts which I'd like to resume now.

Though theologians confirm there are cipher texts in the Bible, it is to say that these are mostly searched by people who are not really interested in their origin, but how to interpret them, which leads to that lots of those discoveries were done although there was no efforts to create that particular cipher text in the past anyway.

There is a big difference between the way of thinking of a man who works in some exact science and a man who is mainly focused on explaining relationships between abstract terms. That's why there are people able to accept discoveries made by skip code method as real, whilst others disagree claiming that there cannot possibly be any reasonable person who would believe them.

As I studied, I used to think as both those kinds of scientists and I must admit that after all I can only accept the way of thinking of who is willing to change his opinion, when he knows that his arguments cannot stand against his opponent's ones, instead of always looking for some great explanation that would prove his rightness.

That's why I reject Eliyahu Rips' approach (though I very respect him) and also Michael Drosnin's approach who I'm not afraid to call a calculating liar, because of his false claims he's not ashamed to public just to keep being famous. He says he is a sceptic and every matrix in his books are mathematically verified, but it certainly can't be true, because he simply doesn't understand that at all.

On the other hand, I appreciate months of work which Brandon McKay gave to the Bible Code phenomenon, so he can prove that no one who is willing to make an objective opinion about the whole thing, can't really believe it's all perfectly right. Moreover, I've confirmed this by my own study.

So in following paragraphs I'm going to summarize everything I consider as key facts from whole of my thesis:

The first objection against the skip code method itself should surely be that even if it was usable on the Bible text in general and if there was that possibility that there might be prophecies about human destiny about both past and future, we don't have any useful text in these days anyway. Today we have only few texts which are so different from each other

(and from the original one too) that only cipher texts which could be relevant, are those ones discovered by H. M. D. Weissmandel, because they can be found in short distance from where the books start.<sup>31</sup>

Every so-called "discovery" can be explained by statistical calculations and can be found in every text which is long enough. If any of those "prophecies" found in the Bible should be in any way relevant, because it was put there by God or aliens, it would not be very clever of them to hide actual cipher text in text which naturally includes lots of random expressions, being spread there just by chance - unless they were very silly aliens.

In this context, it's also to say that every found expression is always very short, so it represents single term only, but never the whole coherent sentence, which means that there is no objective way of how to put it together and it very often depends on fantasy of who is trying to interpret that so-called "prophecy", which leads to that it's all a matter of huge subjectivity.

And finally, the way of searching related expressions in letter matrix is also wrong. If your attempts are just to search related terms one by one, you can't possibly be doing it objectively because the right approach would be to search every meaningful expression in the matrix and then check critically, whether there are any connections. So when Drosnin found words "Shakespeare" and "Hamlet" in one matrix, it did only mean that had found what he was looking for - but not what there really was:

Nothing worth to mention.

---

<sup>31</sup> Although it's also true that they can't be found in every version of Torah.

**SEZNAM POUŽITÉ LITERATURY**

- [1] BUDÍLKOVÁ, Marie. KRÁLOVÁ, Maria. MAROŠ, Bohumil. *Průvodce základními statistickými metodami*. Vydání první. Praha: Grada, 2010. 272s. ISBN 978-80-247-3243-5.
- [2] DROSNIN, Michael. *The Bible Code 1*. Vydání první. London: Orion Publishing Group, 2003. 240s. ISBN 978-0-7528-0932-8.
- [3] MCKAY, Brendan. *Assassinations Foretold in Moby Dick* [online]. 1997. [cit. 2011-05-27]. Dostupné z www: <<http://cs.anu.edu.au/~bdm/dilugim/moby.html>>.
- [4] MCKAY, Brendan. BAR-NATAN, Dror. BAR-HILLEL, Maya. KALAI Gil. *Solving The Bible Code puzzle* [online]. 1999. [cit. 2011-05-24]. Dostupné z www: <<http://cs.anu.edu.au/~bdm/dilugim/statsci/StatSci.pdf>>.
- [5] PETZOLT, Charles. *Programování Microsoft Windows Forms v jazyce C#*. Vydání první. Brno: Computer Press, 2006. 356s. ISBN 80-251-1058-3.
- [6] RIPS, Eliyahu. *Public Statement By Eliyahu Rips* [online]. 1997. [cit. 2010-05-24]. Dostupné z www: <<http://www.torahsoft.com/PSEliRips.htm>>.
- [7] ŘEHÁK, Robert. *Synchronní metody výkladů hebrejských proprií ve Starém zákoně a v rabínské literatuře*. Disertační práce. Praha: Karlova univerzita v Praze, 2007.

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

ČEP	Český ekumenický překlad (jeden z českých překladů Bible)
ELS	Equidistant letter sequency (posloupnost písmen, mezi nimiž je stejná vzdálenost)
WLC	Westminsterský Leningradský kodex (jedna z verzí hebrejské Bible)
WRR	Witztum, Rips, Rosenberg

**SEZNAM ILUSTRACÍ**

Ilustrace 1: Vzorový software - nabídka File.....	31
Ilustrace 2: Vzorový software - nabídka Search.....	31
Ilustrace 3: Vzorový software - Vyhledávání dvou výrazů.....	32
Ilustrace 4: Vzorový software - Tóra.....	32
Ilustrace 5: Vzorový software - Okno programu.....	33
Ilustrace 6: Vzorový software - Práce s legendou.....	33
Ilustrace 7: Vzorový software - Nabídka Count.....	34
Ilustrace 8: Vzorový software - Zobrazení výpočtů.....	34
Ilustrace 9: Vzorový software - Frekvenční charakteristika textu.....	35
Ilustrace 10: Šifrová tabulka - světová válka, udeří na ně.....	44
Ilustrace 11: Šifrová tabulka - Shakespeare, Macbeth, Hamlet.....	46
Ilustrace 12: Šifrová tabulka - Jicchak Rabin.....	48
Ilustrace 13: Šifrová tabulka - René Moawad v Bílé velrybě.....	50

**SEZNAM TABULEK**

Tabulka 1: Přehled hebrejské abecedy.....	12
Tabulka 2: Pomůcka pro atbaš.....	15
Tabulka 3: Seznam symbolů použitých pro výpočty.....	36
Tabulka 4: Frekvenční charakteristika textu Tóry.....	37
Tabulka 5: Šifrová tabulka - světová válka, udeří na ně (podrobnosti).....	44
Tabulka 6: Šifrová tabulka - Shakespeare, Macbeth, Hamlet (podrobnosti).....	46
Tabulka 7: Šifrová tabulka - Jicchak Rabin (podrobnosti).....	48
Tabulka 8: Šifrová tabulka - René Moawad v Bílé velrybě (podrobnosti).....	50