

# **Moderní kryptologie v běžném životě**

Modern Cryptology in Everyday Life

Jiří Garba

---

Bakalářská práce  
2013



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2012/2013

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: Jiří GARBA  
Osobní číslo: A09109  
Studijní program: B3902 Inženýrská informatika  
Studijní obor: Informační a řídicí technologie  
Forma studia: prezenční

Téma práce: Moderní kryptologie v běžném životě

Zásady pro vypracování:

1. Vypracujte literární rešerši na dané téma.
2. Proveďte teoretický rozbor současných technik a metod moderní kryptologie, které se v běžném životě používají v celé řadě běžných aplikací.
3. Vypracujte jednoduché demonstrativní ukázky šifrovacích metod a principů a porovnání různých metod zabezpečení.
4. Vytvořte multimediální pomůcku případně webovou prezentaci pro účely zkvalitnění výuky předmětu Kryptologie na FAI.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: tištěná/elektronická

Seznam odborné literatury:

1. ZELENKA, J., ČAPEK, J., FRANCEK, J., JANÁKOVÁ, H. Ochrana dat, Kryptologie. Gaudeamus, září 2003. 171 s. ISBN 80-7041-737-4.
2. ČANDÍK, Marek. Základy informační bezpečnosti. vyd. Zlín : Univerzita Tomáše Bati, 2004. 107 s. ISBN 8073182181.
3. VONDRUŠKA, P. Kryptologie, šifrování a tajná písma. Albatros, 2006. ISBN 80-00-01888-8.
4. KATZ, Jonathan. Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall, 1 edition. 2007. 552 s. ISBN 978-1584885511.
5. MURPHY, Sean. Kryptografie – Průvodce pro každého . Dokořán, 2006. 157 s. ISBN 80-7363-074-5.
6. BITTO, O. Šifrování a biometrika. BEN, 2005. 168 s. ISBN 80-86686-48-5.
7. KLÍMA, Vlastimil; ROSA, Tomáš. Kryptologie pro praxi ?DSA, ECDSA. Dostupné z WWW: [http://crypto-world.info/klima/2004/st\\_2004\\_04\\_21\\_21.pdf](http://crypto-world.info/klima/2004/st_2004_04_21_21.pdf).

Vedoucí bakalářské práce:

Ing. Roman Šenkeřík, Ph.D.

Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce:

24. února 2013

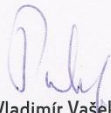
Termín odevzdání bakalářské práce:

14. června 2013

Ve Zlíně dne 24. února 2013

  
prof. Ing. Vladimír Vašek, CSc.  
děkan



  
prof. Ing. Vladimír Vašek, CSc.  
ředitel ústavu

## **ABSTRAKT**

Bakalářská práce se věnuje v teoretické části rozboru současných používaných technik kryptografie, kryptoanalýzy a steganografie. Zabývá se dále současným použitím jejich technik v moderním životě – jejich integrací a aplikací.

V praktické části se bakalářská práce zabývá vytvořením demonstrativních ukázek šifrovacích metod a porovnání jejich bezpečnosti.

Poslední část práce je zaměřena na vytvoření multimediální pomůcky – webové prezentace pro zkvalitnění výuky Kryptologie na FAI.

Klíčová slova: kryptologie, šifrování, šifry, hashe, komunikace, bezpečnost

## **ABSTRACT**

This thesis focuses on the theoretical analysis of the current used techniques of cryptography, cryptanalysis and steganography. It also deals with the concurrent use of this technique in modern life - their integration and applications.

In the practical part of the thesis deals with creating demonstrative examples of encryption methods and comparing their safety. The last part is focused on the creation of multimedia tools - website for the improvement of teaching Cryptology at FAI.

Keywords: cryptology, encryption, ciphers, hasls, comunication, security

Děkuji vedoucímu práce za umožnění vytvoření bakalářské práce pod jeho vedením. Dále bych chtěl poděkovat rodičům za trpělivost, kterou se mnou měli.

Motto:

Velký bratr tě sleduje.

*George Orwell, 1984*

**Prohlašuji, že**

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

**Prohlašuji,**

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

Ve Zlíně

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD .....</b>	<b>10</b>
<b>I TEORETICKÁ ČÁST .....</b>	<b>11</b>
<b>1 KRYPTOLOGIE - ROZDĚLENÍ .....</b>	<b>12</b>
1.1 KRYPTOGRAFIE .....	12
1.2 KRYPTOANALÝZA .....	13
1.2.1 Základní Kryptoanalitické úlohy: .....	13
1.2.2 Útoky proti šifráům (Kryptoanalitické metody): .....	13
1.2.3 Útoky proti klasickým šifráům: .....	13
1.2.4 Útoky proti současným šifráům: .....	13
1.2.4.1 Útok hrubou silou: .....	14
1.2.4.2 Slovníkový útok: .....	14
1.2.4.3 Frekvenční analýza: .....	14
1.2.4.4 Kasiskiho metoda: .....	14
1.2.4.5 Korupční/pendreková analýza: .....	14
1.2.4.6 Útok postranými kanály .....	14
1.2.4.7 Diferenciální kryptoanalýza: .....	15
1.3 STEGANOGRAFIE .....	15
1.4 ZÁKLADNÍ POJMY .....	15
1.5 ROZDĚLENÍ ŠIFER .....	17
1.5.1 Historické šifry .....	18
1.5.2 Současné šifry .....	19
1.6 KRÁTKÁ HISTORIE .....	20
<b>2 SOUČASNÁ KRYPTOLOGIE V BĚŽNÉM ŽIVOTĚ .....</b>	<b>21</b>
2.1 SOUČASNÁ KRYPTOLOGIE - ROZDĚLENÍ .....	21
2.1.1 Symetrická kryptologie .....	21
2.1.1.1 Blokované symetrické šifry .....	21
2.1.1.2 Proudové symetrické šifry .....	21
2.1.2 Asymetrická kryptologie .....	21
2.1.3 Hybridní Kryptologie .....	22
2.1.4 Experimentální Kryptologie .....	22
2.1.4.1 Kvantová Kryptologie .....	22
2.1.4.2 Fraktální kryptografie: .....	22
2.1.4.3 Kryptografie pomocí chaosu .....	22
2.1.5 Hashe .....	23
2.2 POUŽITÍ ŠIFER V MODERNÍM ŽIVOTĚ .....	23
2.2.1 Bezdrátové sítě WIFI .....	24
2.2.1.1 Technologie WEP .....	24
2.2.1.2 Technologie WPA .....	24
2.2.1.3 Technologie WPA-PSK .....	25
2.2.1.4 Technologie WPA2 .....	25
2.2.1.5 Technologie WPA2-PSK .....	25
2.2.2 Telekomunikační sítě GSM .....	25
2.2.3 Internetová bezpečnost .....	27
2.2.3.1 HTTPS .....	27
2.2.3.2 Emailové protokoly .....	28

2.2.3.3	SSH.....	29
2.2.3.4	Bittorent .....	29
2.2.4	Internetové Bankovníctví.....	30
2.2.5	Bankomaty .....	30
2.2.6	Anonymní internetové bankovníctví .....	30
2.2.6.1	BitCoin.....	30
2.2.6.2	eCache.....	31
2.2.7	Digitální podpisy .....	31
2.2.8	Ochrana autorských práv .....	32
2.2.9	Vlastní šifrování souborů.....	32
2.3	ŠIFRY .....	33
2.3.1	Šifra Lucifer .....	33
2.3.2	Šifra DES .....	33
2.3.3	ŠIFRA 3DES .....	34
2.3.4	Šifra IDEA .....	35
2.3.5	Šifra GOST.....	36
2.3.6	El Gammal .....	37
2.3.7	DSA .....	38
2.3.8	AES – Endvanced Encryption standart.....	38
2.3.9	Rinjdael.....	38
2.3.10	RC6.....	39
2.3.11	MARS .....	40
2.3.12	Blowfish.....	40
2.3.13	Serpent .....	40
2.3.14	Twofish.....	41
2.3.15	Threefish .....	42
2.3.16	RSA.....	42
2.3.17	A5/1 .....	42
2.3.18	A5/2 .....	43
2.3.19	A5/3 .....	43
2.4	HASHOVACÍ FUNKCE/ALGORITMY .....	43
2.4.1	MD2.....	44
2.4.2	MD4.....	44
2.4.3	MD5.....	44
2.4.4	MD6.....	45
2.4.5	SHA-1 .....	45
2.4.6	SHA-2 .....	46
2.4.7	SHA-3 .....	47
2.4.7.1	SKein .....	47
<b>II</b>	<b>PRAKTICKÁ ČÁST .....</b>	<b>48</b>
<b>3</b>	<b>DEMONSTRATIVNÍ UKÁZKY ŠIFROVACÍCH METOD.....</b>	<b>49</b>
3.1	POROVNÁNÍ SOUČASNÝCH METOD ZABEZPEČENÍ .....	50
<b>4</b>	<b>MULTIMEDIÁLNÍ POMŮCKA PRO VÝUKU NA FAI.....</b>	<b>51</b>
4.1	ZÁKLADNÍ POHLED NA STRÁNKY .....	51
4.2	POPIS ODKAZŮ MENU.....	52
4.2.1	Úvod .....	52
4.2.2	Základní pojmy.....	52
4.2.3	Historie – vývoj.....	52

---

4.2.4	Rozdělení .....	52
4.2.5	Principy .....	52
4.2.6	Příklady šifer .....	52
4.2.7	Programy .....	52
4.2.8	Zdroje .....	53
<b>ZÁVĚR .....</b>		<b>54</b>
<b>ZÁVĚR V ANGLIČTINĚ .....</b>		<b>55</b>
<b>SEZNAM POUŽITÉ LITERATURY .....</b>		<b>56</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK .....</b>		<b>58</b>
<b>SEZNAM OBRÁZKŮ .....</b>		<b>59</b>
<b>SEZNAM TABULEK .....</b>		<b>60</b>
<b>SEZNAM PŘÍLOH .....</b>		<b>61</b>

## ÚVOD

V teoretické části práce rešerše rozebírá oblasti kryptologie a jejich definice. Dále rozdělení šifer na různé typy a krátký náhled na historii odvětví.

Dále se v teoretické části poukazuje na to, kde v současném životě kryptografické techniky používáme. Následuje přehled zmíněných technik s krátkými informacemi o daných šifrách.

V praktické části jsou vytvořeny demonstrativní ukázky šifrovacích metod, které se v současné době používají. Část metod zabezpečení je dále porovnávána.

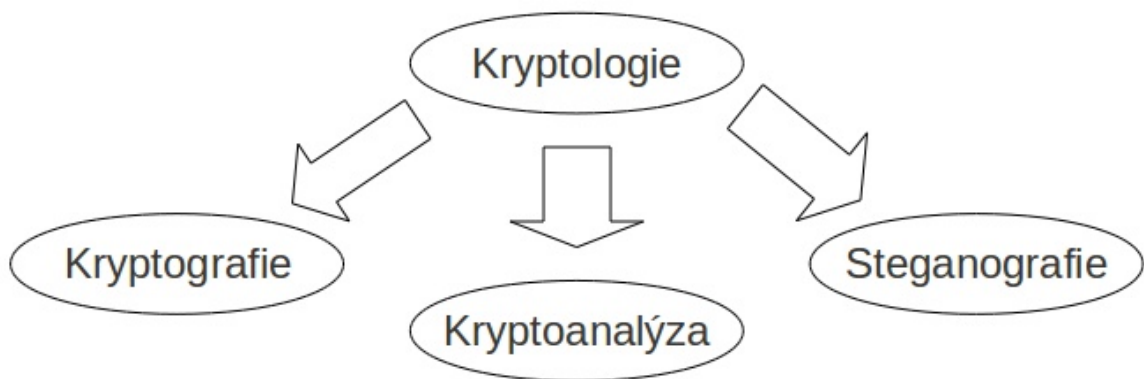
Jako poslední část je vytvořena webová stránka – prezentace pro podporu výuky kryptologie na fakultě aplikované informatiky. Na webové stránky jsou použity technologie CSS a Javascript.

## **I. TEORETICKÁ ČÁST**

# 1 KRYPTOLOGIE - ROZDĚLENÍ

## Kryptologie

Kryptologie je matematická disciplína. Zjednodušeně je to věda o utajení obsahu zpráv. Vzniká spojením kryptografie, kryptoanalýzy a steganografie. Zahrnuje tvorbu kryptografických technik a metod tvorby šifer. Testování odolností vytvořených šifer proti možným - známým typům útoků.



Obrázek 1: Rozdělení kryptologie

## 1.1 Kryptografie

Kryptografie se zabývá matematickými metodami se vztahem k prvkům informační bezpečnosti.

*z řeckého kryptós – „skrytý“ a gráphein „psát“*

Jsou jimi následující:

- důvěrnost zprávy
- integrita dat
- autentizace entit
- původ dat
- zabezpečení přenosu dat

Veškeré výše zmíněné lze dosáhnout pomocí šifrování. Ve starším chápání to byla především disciplína zabývající se převodem informací do formy, ve které je obsah skrytý před neoprávněnými osobami. Úkolem tedy bylo učinit zprávu pro nepovolanou osobu nečitelnou (nesrozumitelnou) [1] [2] [4].

## 1.2 Kryptoanalýza

Kryptoanalýza je v podstatě opakem kryptografie.

(z řeckého *kryptós* – „skrytý“ a *analýein* – „uvolnit“ či „rozvázat“)

Hlavním cílem je luštění šifrovacích algoritmů a jejich prolomení. V moderním pojetí to znamená, že testujeme sílu, robustnost daného šifrovacího algoritmu a metody vedoucí k jeho prolomení. Na druhé straně barikády vždy budou pokusy buď jednotlivců, skupin nebo dokonce celých vlád o prolomení nových šifer - zabezpečení.

Zabývá se zkoumáním slabých, silných stránek a odolností algoritmů vůči vnějším útokům [1] [2] [4].

### 1.2.1 Základní Kryptoanalitické úlohy:

- dešifrování ze znalosti otevřeného textu
- dešifrování s částečnou znalostí otevřeného textu
- dešifrování se znalostí přímého textu
- útok se znalostí otevřeného textu

### 1.2.2 Útoky proti šifráům (Kryptoanalitické metody):

- útok hrubou silou  
(vylepšená modifikace je útok pomocí "rainbow tables", v podstatě se jedná o tabulku s předhashovanými hesly)
- frekvenční analýza
- pendreková kryptoanalýza
- korupční kryptoanalýza
- diferenciální kryptoanalýza
- luštění ze znalostí šifrovaného textu  
(zmenšení prostoru klíčů)
- luštění se znalostí klíčů  
(zmenšení prostoru klíčů)

### 1.2.3 Útoky proti klasickým šifráům:

- frekvenční analýza
- Kasiskiho metoda
- metoda ad-hoc

### 1.2.4 Útoky proti současným šifráům:

- útok hrubou silou
- útok postraními kanály
- Korupční/pendreková kryptoanalýza
- diferenciální kryptoanalýza

#### 1.2.4.1 *Útok hrubou silou:*

- Nazývá se také brute force attack
- Principem útoku je zkoušení hesla dokud nám nevyjde

#### 1.2.4.2 *Slovníkový útok:*

- částečně vylepšený útok hrubou silou
- Principem útoku je zkoušení hesla dle slovníku hesel, který pro daný jazyk je vytvořen.
- Ve slovníku je většina slov dané abecedy.

#### 1.2.4.3 *Frekvenční analýza:*

- 100% účinná pouze na starší typy šifer
- V celém šifrovaném textu se vyčíslí počet a pravděpodobnost každého znaku a seřadí se do sloupcového grafu.
- Podle vzorů jazyků určíme jaké jsou které znaky

#### 1.2.4.4 *Kasiskiho metoda:*

- Je založena na jednoduché myšlence.
- Pokud máme N substitučních abeced (klíč o délce N) a v OT se objevuje k krát stejný řetězec pak bude tento řetězec přibližně  $k/N$  krát zašifrován stejným způsobem.
- Proto hledáme minimálně 3 znakové kombinace, které se v textu opakují.
- Pak zjistíme vzdálenosti jejich počátků tzv. diferencí.
- Dostaneme tak několik čísel jejichž nejmenší společný dělitel nebo jeho násobek je délka klíče.

#### 1.2.4.5 *Korupční/pendreková analýza:*

- Při správných podmínkách 100% účinná
- Pendreková - vynucování hrubou silou hesla, principů
- Korupční - úplatky získané hesla, přístupy, principy

#### 1.2.4.6 *Útok postranními kanály*

- nesnaží najít teoretické slabiny v matematické struktuře algoritmu, ale pokouší se o zneužití informací, které unikají přímo z fyzické implementace systému během běhu kryptografického algoritmu.
- Pokud je totiž uniklá informace nějakým způsobem závislá na tajném klíči algoritmu, může tato informace pomoci útočníkovi klíč odhalit.
- Cílem útoku postranními kanály nemusí být pouze kryptografický klíč, ale například jen informace o tom, jaký algoritmus se pro šifrování používá, jak dlouho trvá vykonání algoritmu nebo jeho části, či odhalení PINu

#### 1.2.4.7 Diferenciální kryptoanalýza:

- metoda používá dvojice otevřený text - šifrovaný text a rozdíly v nich
- rozdíly mohou být definovány několika způsoby, ale nejčastěji XOR
- útočník počítá rozdíly šifrovaných textů a detekuje statistické vzory

[1] [7]

### 1.3 Steganografie

Steganografie se zabývá vlastním utajením komunikace.

*(z řeckého steganós-schovaný, gráphein-psát)*

Dlouho považována za nedůležitou ve srovnání s kryptografií. Zpráva je ukryta tak, aby si náhodný pozorovatel vůbec nevšiml, že probíhá nějaká komunikace. V minulosti se pro utajení komunikace používali neviditelné inkousty. V současnosti se digitální data ukrývají buď do obrázků nebo videí. Ukrytá data nejsou v souborech pouze pro utajení komunikace. Slouží i jako digitální podpis pro určení majitele, zamezení duplikace, omezení duplikace a dalších. Pokud nikdo neví, že probíhá komunikace, tak není nutné oběť sledovat [1] [2] [4].

### 1.4 Základní pojmy

#### Otevřený text

- je to srozumitelný text, zpráva, kterou nechceme aby někdo znal.  
(pokyn k taktickému útoku, milostný dopis a podobně)

#### Šifrovaný text

- text (zpráva) převedená do nesrozumitelného tvaru pro kohokoliv jiného než příjemce a odesílatele.

#### Šifrovací systém (kryptosystém)

- jakýkoliv systém (algoritmus), který převádí otevřený text na šifrovaný text. Neboli převádí srozumitelný text na text nesrozumitelný.

#### Šifra

- systém utajení zprávy  
- ve většině případů používá klíč  
- často se plete s kódem

#### Šifrování

- proces převádění otevřeného textu na text šifrovaný za pomoci kryptosystému.

#### Dešifrování

- proces převádění šifrovaného textu na text otevřený za pomoci kryptosystému.

**Abeceda otevřeného textu**

- je to abeceda, lépe řečeno znaky textu, který chceme zašifrovat

**Abeceda šifrovaného textu**

- je to abeceda, lépe řečeno znaky šifrovaného textu

(nemusí být shodný s abecedou otevřeného textu)

**Klamač**

- znak nebo více znaků šifrované abecedy, kterým neodpovídá ekvivalent z abecedy otevřeného textu

- slouží pouze pro vyšší bezpečnost

**Bigram**

- dvojice sousedních znaků, které jsou pro daný jazyk typické

**Trigram**

- trojice sousedních znaků, které jsou pro daný jazyk typické

**Polygram**

- blíže neurčený počet sousedních znaků textu, které jsou pro daný jazyk typické

- například Bigram, Trigram

**Mezinárodní abeceda**

- nejčastěji používaná abeceda pro šifrování

- specifické abecedy (česká, německá, čínská ...) kladou vyšší nároky na algoritmus (systém)

- znaky abecedy:

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

**Útočník**

- nepovolaná osoba snažící se dozvědět obsah utajené (zašifrované) komunikace

- většinou v příkladech a principech ji označujeme jako Evu.

(Ne že by biblická Eva byla zlá, když Adamovi nabízela jablko ze zakázaného stromu, ale Eva představuje Enemy (nepřítele) z anglického pojetí, důvodem je historické označení)

**Luštění**

- takzvané prolamování šifry útočníkem

**Odesílatel**

- člověk odesílající zašifrovanou zprávu

- většinou tuhle osobu označujeme jako Adama nebo Alici

**Adresát**

- člověk schopný zašifrovanou zprávu přečíst bez větších obtíží v reálném čase

- většinou označujeme jako Boba

**Kód**

- úprava zprávy (textu nebo slov) pro zpracování technickým prostředkem

- většinou pro přenos na komunikačním kanále
- například ANSII kód či Morseova abeceda

### Klíč

- slovo nebo řetězec znaků, s jejichž pomocí se mění otevřený text na šifrovaný text

### Klíčový prostor

- počet různých klíčů, které lze u určitého systému použít
- ze všech možných klíčů jsou vyloučeny ty slabé
- u substitučních šifer je to klíč s hodnotou 0

### Inicializační vektor

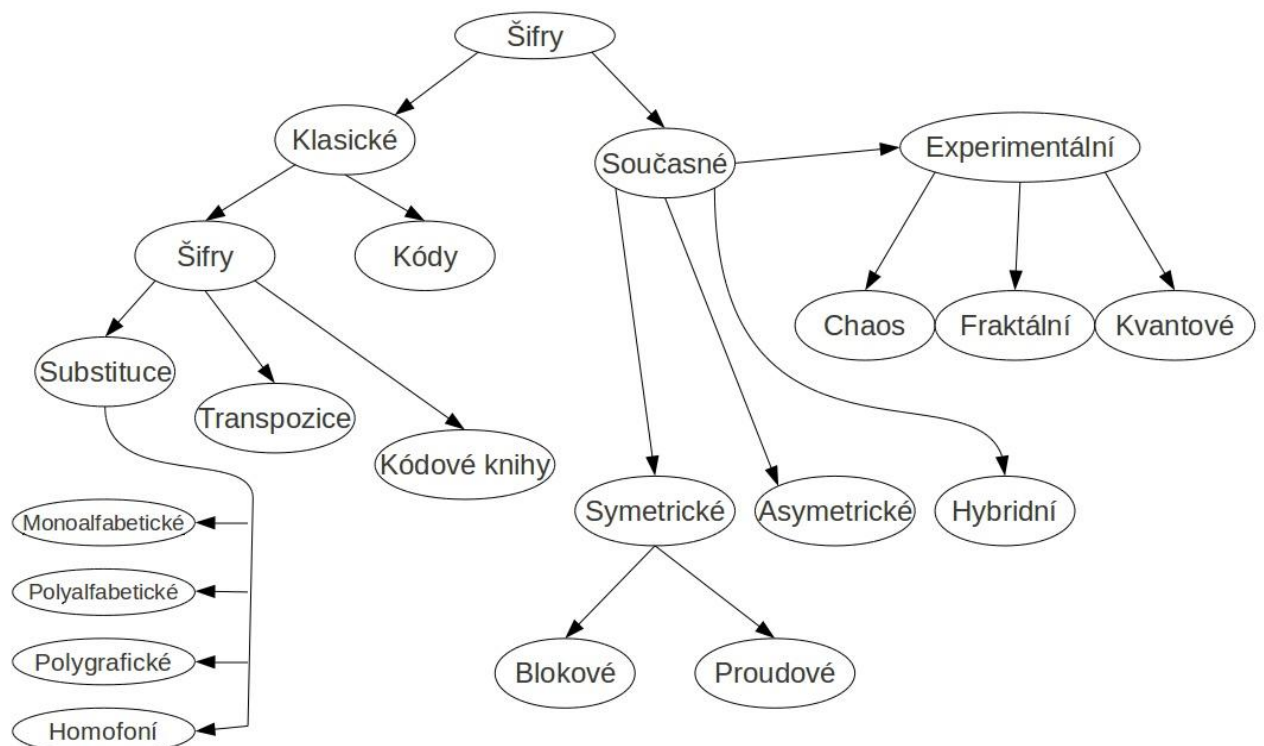
- vektor, číselná kombinace k inicializaci klíče
- využíván v digitálních šifrách

### key stream

- generovaný klíčový proud proudovými šiframi
- často pro vytvoření hesla/klíče

[1] [4]

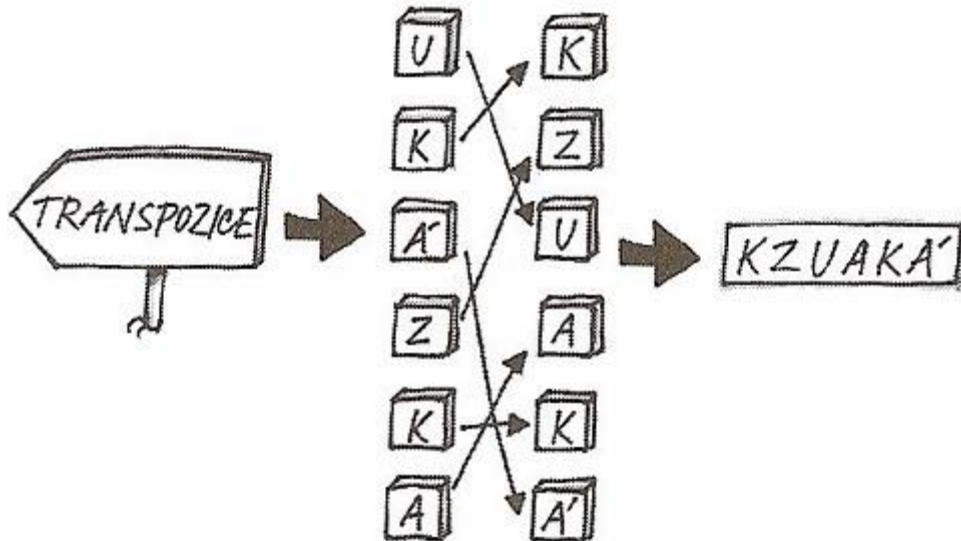
## 1.5 Rozdělení šifer



Obrázek 2: Rozdělení šifer

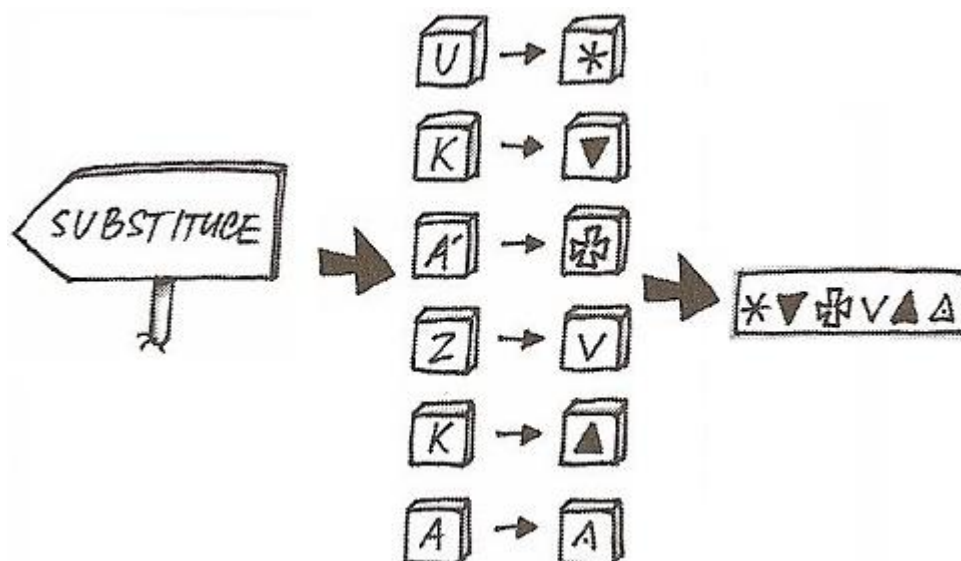
### 1.5.1 Historické šifry

- Transpoziční
  - změna pouze pořadí znaků v textu
  - rozdělení výskytu znaků zůstává zachováno



Obrázek 3: Transpoziční šifra

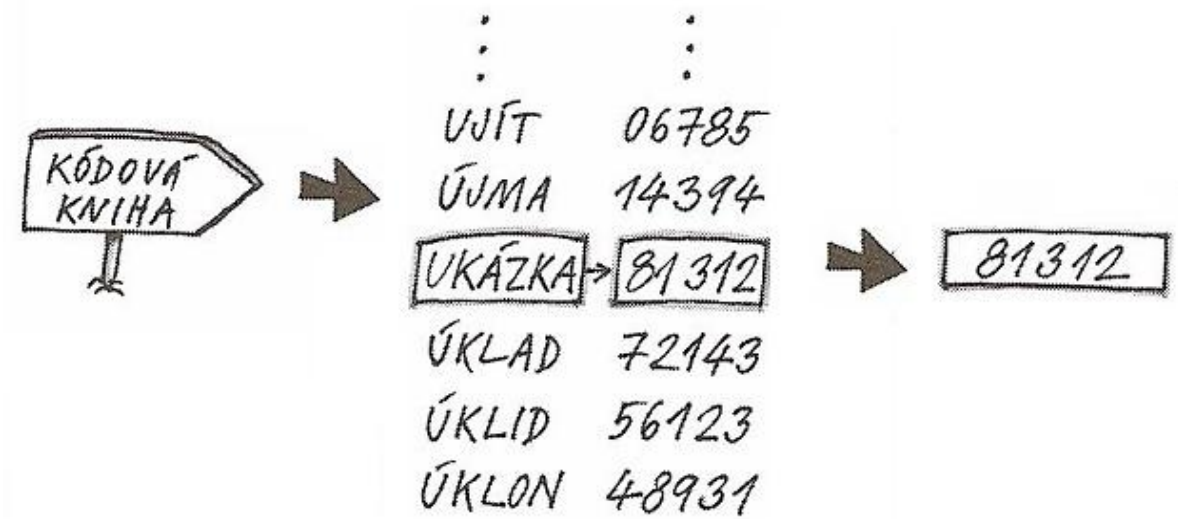
- Substituční
  - nahrazuje znak textu za jiný
  - jeden znak textu se může nahradit i více znaky
  - rozdělení výskytu znaků je pozmeněno a znemožněna frekvenční analýza



Obrázek 4: Substituční šifra

- Jednoduchá substituce
- Homofoní substituce
- Polyalfabetická substituce
- Bigramová substituce
- Trigramová substituce

- Kodové tabulk



Obrázek 5: Kódová kniha

- Kombinované  
kombinuje náhradu znaků jako substituční a změnu pořadí, tak jako transpozici

[1] [2] [4]

### 1.5.2 Současné šifry

- Symetrické
  - Blokové
  - Proudové
- Asymetriické
- Hybridní  
-kombinuje symetrickou a asymetrickou šifru
- Experimentální
  - Kvantové  
- využívají principů kvantové fyziky (nosiči dat jsou fotony)
  - Fraktální  
- využívá fraktály pro substituci
  - Chaotické

## 1.6 Krátká historie

Období	Charakteristické rysy
Počátek – 15. Století	Kódování, jednoduché šifry, skrývání zpráv
15. století – počátek 20. Století	Zdokonalené jednoduché šifry, kryptoanalýza jednoduchých šifer, základy teorie Kryptologie
20. století	Ucelenější teorie, postupný rozvoj mechanických a elektrických šifrovacích zařízení, symetrická a asymetrická kryptografie, kryptografické protokoly, masivní nasazení kryptologie jako jednoho z kamenů moderní společnosti, kryptografie se stává nepostradatelnou
21. století	Alternativní počítače, pravděpodobnostní kryptologie, kvantová kryptografie

Tabulka 1: Charakteristické rysy etap rozvoje kryptologie Zdroj: Ochrana dat. Kryptologie

## 2 SOUČASNÁ KRYPTOLOGIE V BĚŽNÉM ŽIVOTĚ

Současná kryptologie, co je používaná se dá rozdělit do několika kategorií. Jimiž jsou: symetrické šifry, asymetrické šifry, hybridní šifry a hashe.

### 2.1 Současná kryptologie - rozdělení

#### 2.1.1 Symetrická kryptologie

Používá pro šifrování jeden klíč, který je znám pouze aktérům komunikace. Klíč je nutno přenést po zabezpečeném kanále před šifrování nebo i v průběhu šifrování. (nejlepší je osobní předání na osamoceném místě, ale k tomu dochází jen zřídka) Společně klíčem se přenáší taky informace jaký algoritmus se použije a další důležité údaje. Vyniká nízkou výpočetní a časovou složitostí [1] [5].

##### 2.1.1.1 Blokové symetrické šifry

Otevřený text se při šifrování rozdělí do bloků o stejné (stanovené) délky, pokud po rozdělení do bloků je jeden blok nekompletní, tak je na zbylé místo bloku dána výplň. Každý blok se šifruje zvlášť vlastním sub-klíčem vytvořeným z klíče hlavního.

##### 2.1.1.2 Proudové symetrické šifry

Vstupní data jsou kombinována s pseudonáhodnými bity (stream) vytvořenými pomocí algoritmu a klíče (typicky XOR). Jsou rychlejší a jednodušší jako blokové šifry, ale náchylnější vůči kryptoanalýze. Inspirace u Vernamovy šifry.

##### *Synchronní*

Pseudonáhodné bity generovány nezávisle na klíči a zprávě (XOR).

##### *Samosynchronní*

Používá N čísel šifrovaného textu k vypočítání klíče.

[1] [4] [5]

#### 2.1.2 Asymetrická kryptologie

Pro šifrování používá dva klíče, soukromý (známý jen odesílateli/adresátovi) a veřejný (volně dostupný u certifikační autority nebo odesílatele/adresáta). Klíče jsou navzájem rozdílné, ale je mezi nimi matematická souvislost. Šifrování/dešifrování je časově, programově i výpočetně složitější jak u symetrických šifer. Bezpečnost klíčů a algoritmů je

založena na jednocestných funkcích (faktorizace čísel, výpočet diskretního logaritmu, kombinatorická optimalizace).

[1] [4] [5]

### 2.1.3 Hybridní Kryptologie

Kombinuje výhody symetrického a asymetrického systému. Typický zástupce je PGP

### 2.1.4 Experimentální Kryptologie

#### 2.1.4.1 Kvantová Kryptologie

Využívá kvantové počítače a kvantové fyziky. Struktura počítačů není plošná jako u současných digitálních, ale prostorová. Měření ovlivňuje stav -> zjištění/odposlech stavu komunikace (spolehlivá detekce odposlechu) Kvantová mechanika zahrnuje procesy, které jsou zcela náhodné, což se uplatní pro náhodné generátory čísel.

#### 2.1.4.2 Fraktální kryptografie:

Fraktály - objekty jejichž struktura se opakuje v nich samotných, soběpodobné (PC simulace) a soběpříbuzné (přírodní objekty). Metody fraktální kryptologie: IFS, HIFS, TEA.

##### **IFS**

Substituční šifra, znaky se nahrazují koeficienty afinních transformací. Možné ztížení použitím více iterací - textový fraktál (šifrovaný text bude mít větší velikost). Klíčem je rozměr matice a počet iterací

##### **HIFS**

Substituční šifra, jedná se o kombinace více úrovní IFS.

##### **TEA**

Substituční šifra, náhradou jsou souřadnice pixelu fraktálu, klíčem jsou souřadnice, rozsah a počet iterací.

#### 2.1.4.3 Kryptografie pomocí chaosu

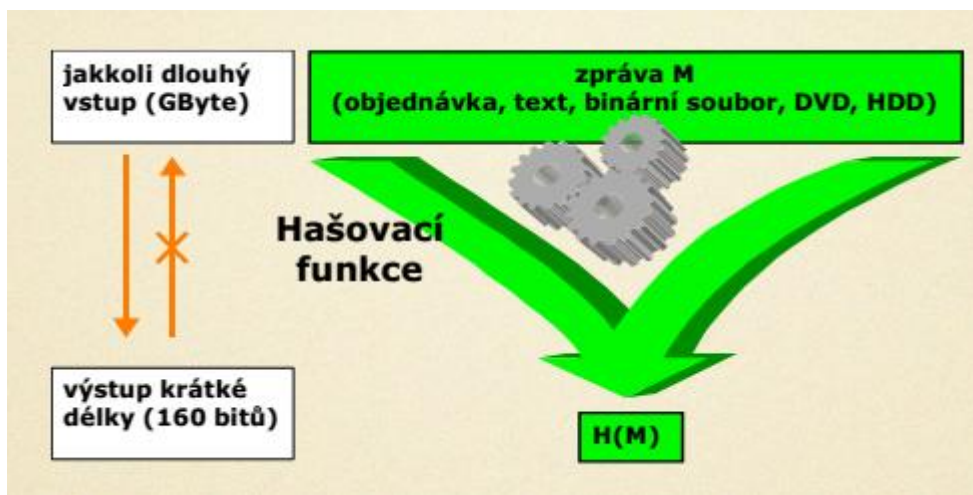
Chaos je velmi citlivý na počáteční podmínky (Butterfly efekt). Deterministický chaos se vyskytuje v systémech, kde je dán soustavou rovnic (predátor vs kořist nebo výdělek manžela vs utrácení manželky). Typ systému a jeho parametry jsou šifrovacím klíčem.

Použití: chaotická modulace, chaotické maskování, chaotické klíčování, chaotická transformace

[8] [9]

### 2.1.5 Hashe

Algoritmy vytvářející otisky z jakkoliv velikých souborů, jakýchkoliv přípon, textů.



Obrázek 6: Hashovací funkce Zdroj: Přednášky předmětu Kryptologie, FAI, UTB Zlín

## 2.2 Použití šifer v moderním životě

V současné době používáme šifry a šifrování skoro v každém aspektu našeho života. Mezi ty nejčastější oblasti používání patří bezdrátové sítě – připojení k internetu pomocí technologie WIFI, telekomunikační sítě – komunikace pomocí mobilních telefonů, brouzdání po internetu a obecný pohyb o něm, výběry z bankomatů, digitální podpisy, internetové bankovníctví, ochrana autorských práv a vlastní šifrování souborů. Mezi méně známe, ale dost využívané patří i anonymní internetové bankovníctví.

### 2.2.1 Bezdrátové sítě WIFI

Jak název napovídá technologie wifi nepoužívá žádné vodiče, které by přenášeli data. Veškerá data „letí“ vzduchem a kdokoli je může zachytit, odposlechnout, pozměnit. Z toho důvodu je potřeba zavést nějaké bezpečnostní opatření. Na výběr máme ze 6 možností. Těmi jsou: nezabezpečit, zabezpečit technologií WEP, zabezpečit technologií WPA, zabezpečit technologií WPA-PSK, zabezpečit technologií WPA2, zabezpečit technologií WPA2-PSK.

#### 2.2.1.1 Technologie WEP

*Wired Equivalent Privacy, tj. soukromí ekvivalentní drátovým sítím*

Používán od roku 1997, kdy byl poprvé nasazen a to pomocí standartu IEEE 802.11. Zabezpečení mělo poskytnout bezpečnost sítě na úrovni kroucené dvojlinky. Pracuje na linkové vrstvě, kde šifruje přenášené rámce šifrou RC4 a ověřuje integritu dat pomocí CRC-32. Základní WEP používá několik verzí. 64 bitová verze používá 40 bitový klíč a 24 bitový inicializační vektor. 128 bitový WEP používá 104 bitový klíč a 24 bitový inicializační vektor. V roce 2001 byla technologie prolomena. Jako odezva na prolomení vznikly vylepšené zabezpečení WEP+ a WEP2. Obě technologie nejsou od Klasického WEP nijak odlišné, pouze rozšiřují inicializační vektory a klíče. Čili prolomení trvá pouze delší dobu.

#### 2.2.1.2 Technologie WPA

*Wi-Fi Protected Access, tj. chráněný přístup k Wi-Fi*

Definována v roce 2002 jako část standartu IEEE 802.11i. Základní myšlenka byla aktualizace software, který se používal na starých zařízeních, čili nebyla nutná změna hardwaru. Používá stejně jako WEP proudovou šifru RC4, která je ale doplněna o TKIP (Temporal Key Integrity Protocol), který se staral o správu klíčů. Na rozdíl od WEP je pro šifrování každého rámce WPA použit jiný klíč, oč se stará TKIP. Velikost šifrovacího klíče změněna na 128 bitů a inicializační vektor na 48 bitů. Využívá autentizace pomocí serveru. WPA má možnost volit mezi zabezpečením TKIP a použitím šifry AES.

### **2.2.1.3 Technologie WPA-PSK**

Jedná se o klasické WPA, které používá jinou metodu autentizace. Je navržen pro domácí a malé sítě, které si nemohou dovolit kupovat autentizační server. Autentizační metoda je předsdílený klíč.

### **2.2.1.4 Technologie WPA2**

Schválen roku 2004. Používá blokovou šifru AES. Používá 128 bitový klíč a 128 bitovou velikost bloků. Pro autentizaci používá protokol EAP, autentizační server a metodu Four Way Handshake.

### **2.2.1.5 Technologie WPA2-PSK**

Modifikace klasické varianty WPA2. Modifikace spočívá stejně jako u WPA-PSK v jiné metodě autentizace. Jedná se o předsdílený klíč.

[10] [11] [12][13]

## **2.2.2 Telekomunikační síť GSM**

Označovány jako 2G či 3G sítě Komunikace pomocí mobilních telefonů se stala součástí naší každodenní činnosti. Stejně jako bezdrátové sítě wifi i GSM komunikace je bezdrátová čili je nutné zabezpečení. Jako zabezpečení se používá autentizace a šifrování. Autentizace se provádí pomocí SIM modulů, pro vyšší zabezpečení se používá modul USIM. SIM autorizuje uživatele do sítě. USIM autorizuje uživatele do sítě, ale i síť uživateli. Pro šifrování se používají algoritmy A5/1, A5/2 a A5/3 (známá také jako KASUMI). A5/1 se používá nyní v Evropě. A5/2 se používá v ostatních zemích. Bohužel je ale možné jej prolomit v reálném čase. A5/3 je na rozdíl od předchozích dvou bloková šifra. Je možné ji použít jako bezpečnější metodu. Záleží ale co dostupný operátor nabízí. Od roku 2010 se šifra A5/3 nedá považovat za bezpečnou pro komunikaci, díky prolomení na průměrném zařízení. Od roku 2011 je možné prolomit šifru A5/1 již v řádu sekund na nejlepších výpočetních zařízeních. Veškeré systémy 2G i 3GPP sítě jsou s dostatečně kvalitním vybavením prolomitelné v reálném čase. Z tohoto důvodu existují po celém světě firmy, které se tímto problémem zabývají a nabízejí nám produkty, které nám umožní bezpečné – neodposlouchávací hovory. Nastaví šifrování na vyšší úroveň než je standard operátorů, sítě. Základním principem programů je vytvořit virtuální mobilní

telefon uvnitř fyzického telefonu. K tomu využívají především programovací jazyk JAVA. Pro šifrování používají několik metod. Buď použijí jednotlivé šifrování pomocí šifry AES-256 nebo použijí dvojitě šifrování. Nejprve šifrují šifrou RC4 a poté ještě podruhé zašifrují šifrou AES-256.

- CryptoCult** -používá pro šifrování volání AES-256 šifru  
-pro SMS/Emaily a podobně používá standart PGP  
-systém založen na jazyce JAVA  
-vytváří v telefonu další vlastní telefon  
-původ:CZ
- SMS007** -volná aplikace pro šifrování SMS zpráv  
-používá AES šifrování  
-systém založen na jazyce JAVA  
-vytváří v telefonu další vlastní telefon  
-původ:CZ
- Silentel** -Používá AES-256  
-používá packetové IP spojení pomocí internetu  
-vlastní certifikát NATO Confidential  
(udílí se výrobkům, které splňují NATO standarty bezpečnosti)  
-původ: SK
- Cellcrypt:** -používá dvojitě šifrování  
-1. Šifruje klasicky pomocí RC4 – 256 bitové verze  
-poté šifruje přes AES-256, eliptické křivky či Diffie Hellmanů algoritmus  
-původ: USA
- Silencircle** -používá dvojitě šifrování  
-1. Šifruje klasicky pomocí RC4 – 256 bitové verze  
-poté šifruje přes AES-256, eliptické křivky či Diffie Hellmanů algoritmus  
-původ: USA

[14]

### 2.2.3 Internetová bezpečnost

V současné době se každý pohybuje na internetu a to do konce i v desítkách hodin denně. Na internetu se pohybujeme pomocí různých protokolů. Ty jsou buď nechráněné (http, ftp, POP3, ...) nebo zabezpečené (https, s-http, SSH, Bittorent).

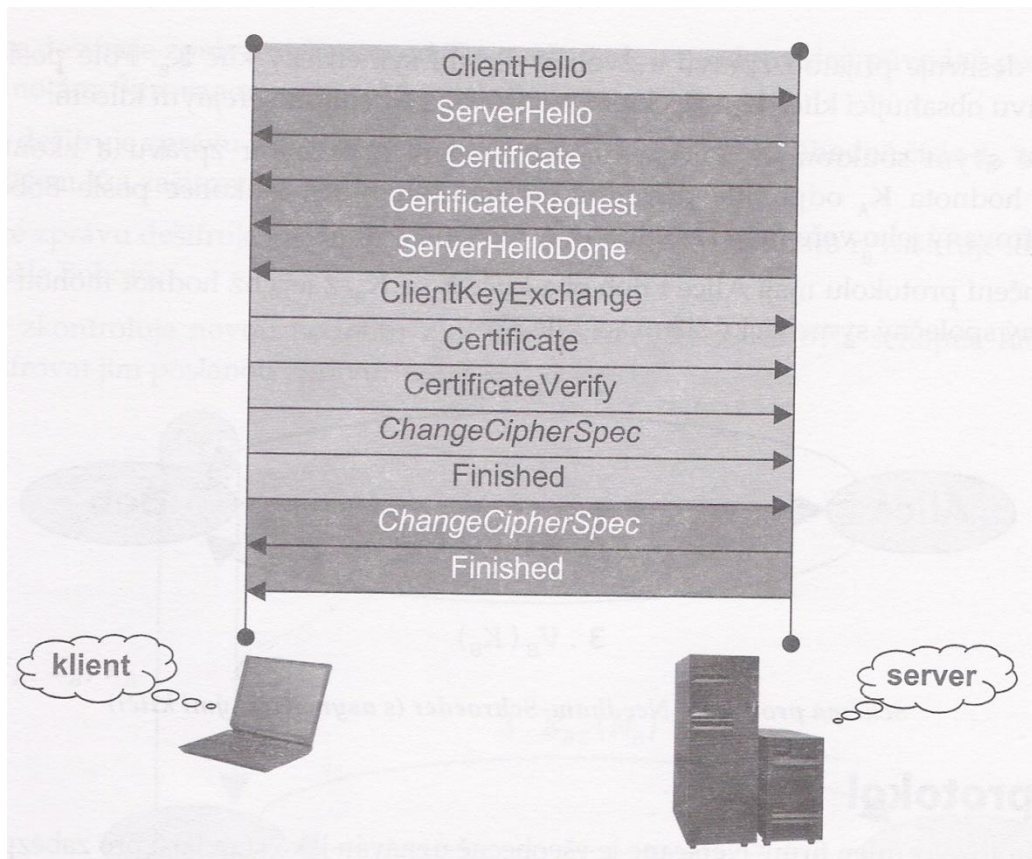
#### 2.2.3.1 HTTPS

Nadstavba protokolu http umožňující zabezpečení mezi prohlížečem a serverem. Používá se asymetrické šifrování a výměna klíčů. Důvěryhodnost se dokazuje klíčem a digitálně podepsaným certifikátem, integrita dat se kontroluje otiskem dat pomocí md5. Pro šifrování se používají protokoly SSL a TLS.

##### 2.2.3.1.1 SSL

*Secure Sockets Layer, SSL (vrstva bezpečných socketů)*

Protokol vložený mezi transportní a aplikační vrstvu. Používá nejčastěji certifikáty. Vytvoření SSL spojení funguje na principu asymetrického šifrování, ale vlastní šifrování se provádí již symetrickými šiframi. Nejprve se provede takzvaný SSL Handshake. (Prohlížeč odešle dotaz na server žádající SSL spojení doplněn o informace, jaký typ šifrování je počítač schopen použít. Server odpoví zprávou s certifikátem a informacemi o SSL a možných šifrách. Prohlížeč ověří se certifikát serveru, certifikát obsahuje veřejný klíč serveru. Prohlížeč vygeneruje základ šifrovacího klíče a zašifruje ho veřejným klíčem serveru a odešle ho. Server rozšifruje základ a vygeneruje plný šifrovací klíč pro komunikaci a odešle ho prohlížeči. Server i prohlížeč si vzájemně potvrdí klíč) Poté je již šifrované spojení vytvořeno. Pro výměnu klíčů se používají algoritmy RSA, DSA a Diffie-Hellmanova metoda. Pro šifrování se používají šifry RC2, RC4, IDEA, DES, 3DES a AES. Při výměně klíče se používají následující hashovací algoritmy: MD5 nebo SHA-1. Protokol má celkem 3 verze. Používaná je pouze verze SSL 3.0. Předchozí verze měli mnoho bezpečnostních rizik.



Obrázek 7: SSL Handshake

### 2.2.3.1.2 TLS

#### Transport Layer Security

Nástupce SSL. Principiálně je stejný jako SSL 3.0. Existuje více verzí protokolu. TLS 1.0 je základní protokol ve většině částí shodný s SSL 3.0. TLS 1.1 má na rozdíl od předchozí verze změněný inicializační vektor a způsob chování při chybách. TLS 1.2 nahrazuje hashování funkce SHA1 a md5 za hashování funkci SHA-256. Otisk stále ale má velikost 96bitů.

### 2.2.3.2 Emailové protokoly

#### POP3

Protokol používaný pro stahování emailových zpráv. Standart vydán roku 1996. V první verzi byl přenos hesla a uživatelského účtu mezi prohlížečem a serverem nešifrovaný. V současnosti se nabízí několik variant zabezpečení. První je heslo a uživatelské údaje se

hashují pomocí algoritmu md5. Jako další možnost je využití šifrování celé komunikace POP3 protokolu pomocí SSL či TLS.

### **IMAP**

Protokol používaný pro stahování emailových zpráv. Drobné rozdíly oproti POP3 vzhledem k chování sessions. Používá šifrování pomocí SSL a TLS.

#### **2.2.3.3 SSH**

Protokol umožňující bezpečnou komunikaci mezi počítači v zabezpečeném kanále. Navržen jako náhrada za protokoly Telnet (práce na vzdáleném počítači), Rlogin (přihlášení na vzdálený počítač) a RSh (spouštění příkazů na vzdáleném počítači). Používá výměnu klíčů pomocí Diffie-Hellmana. Rozdělen do 3. Vrstev. Transportní, autentizační a vrstva spojení. Transportní vrstva zajišťuje výměnu klíčů a autentizaci. Autentizační vrstva zajišťuje autentizaci klientů. Vrstva spojení definuje kanály a globální požadavky SSH.

#### **2.2.3.4 Bittorent**

Protokol p2p (*peer-to-peer*) pro distribuci dat na internetu. Používá se pro distribuci souborů o velikosti 1GB a více. Používáný při distribuci Linuxových distribucí, nejnovějších her a jejich patchů (World of Warcraft, Starcraft2, Star Wars: The Old Republic, ...) či v poslední řadě k distribuci warezu. Důvod šifrování je utajení paketů protokolu jako odezva na omezení bittorent komunikace některými ISP (Internet Service Provider – poskytovateli internetových služeb). Bittorent a obecně p2p protokoly zabírají celou šířku pásma komunikace.

Metody šifrování:

- PE (Protokol Encryption) [šifrování protokolu]
- MSE (Message stream encryption) [šifrování datového proudu]
- PHE (protokol header Encryption) [šifrování hlavičky protokolu]

### **PHE**

Prvně se oběvil v klientu BitComet v 0.60 roku 2005. Šifruje pouze část datového proudu, přesněji hlavičky paketů. Z toho důvodu je snadno detekovatelný a neúčinný.

### **PE a MSE**

Používá Diffie-Hellmanův algoritmus pro výměnu klíčů. Klíč se vytvoří pomocí hashe torrentu. Jako hashování Algoritmus se využívá SHA-1 a SHA-2. K šifrování je použita proudová šifra RC4. Síla odpovídá asi 60 – 80 bitovým symetrickým šifrám. Pro zvýšení bezpečnosti se navrhovalo použití AES algoritmu a šifrování pomocí eliptických křivek, ale to by znamenalo vyšší zatížení CPU, proto se od toho upustilo.

[15] [16]

#### **2.2.4 Internetové Bankovníctví**

V současné době většina lidí používá internetové bankovníctví. Do něj se dostaneme na nějaké adrese, většinou začínající https. Což znamená, že spojení bude šifrované buď pomocí SSL se 128 bity nebo TLS se 168 bity. K vaší identifikaci, ale bude server banky požadovat nějaké údaje. Buď je to klientské číslo a heslo nebo heslo a nějaký certifikát/soubor jehož šifrovaný otisk se poté v datech posílá. Pro výměnu klíčů se používá RSA o velikosti 1024 bitů. Pro šifrování dat se používá AES, 3DES a RC4 128 bitové.

#### **2.2.5 Bankomaty**

Stejně jako při internetovém bankovníctví se používá šifrovaného spojení, tak i při výběru z bankomatu se používá šifrování. Pro výběr z bankomatu, přesněji peněz z účtu se musí bankomat připojit do databáze dané banky. To se děje přes bankovní síť, po které se data posílají zašifrovaná pomocí DES a 3DES algoritmů z platformy založené na systému Windows XP nebo Windows NT u starších přístrojů.

#### **2.2.6 Anonymní internetové bankovníctví**

Nezávislé na současné měně. Jsou vytvořeny vlastní měny. Jsou jimi BitCoin, Open-Transaction, eCache, Pecunix, Private payment systém či PayPal.

##### **2.2.6.1 BitCoin**

Decentralizovaná open source p2p měna. Měnu nelze ovlivnit, zničit, padělat, kontrolovat její tok, způsobovat inflaci či zabavovat účty. Celkové množství peněz je konečné a to 21 000 000 BitCoin. Měna se do oběhu uvolňuje postupně. Veškeré BitCoiny budou v oběhu až v roce 2140. Hodnota měny je založena na důvěře a výpočetní síle těžícího sítě. Autor je znám pod pseudonymem Satoshi Nakamoto. Pro ověření transakce jsou použity

dva hashe SHA-256, pro digitální podpis a vytvoření adresy jsou použity SHA-256 a RIPEMD-160. Struktura je založena na principu Merkleho stromu a eliptických křivek RSA.

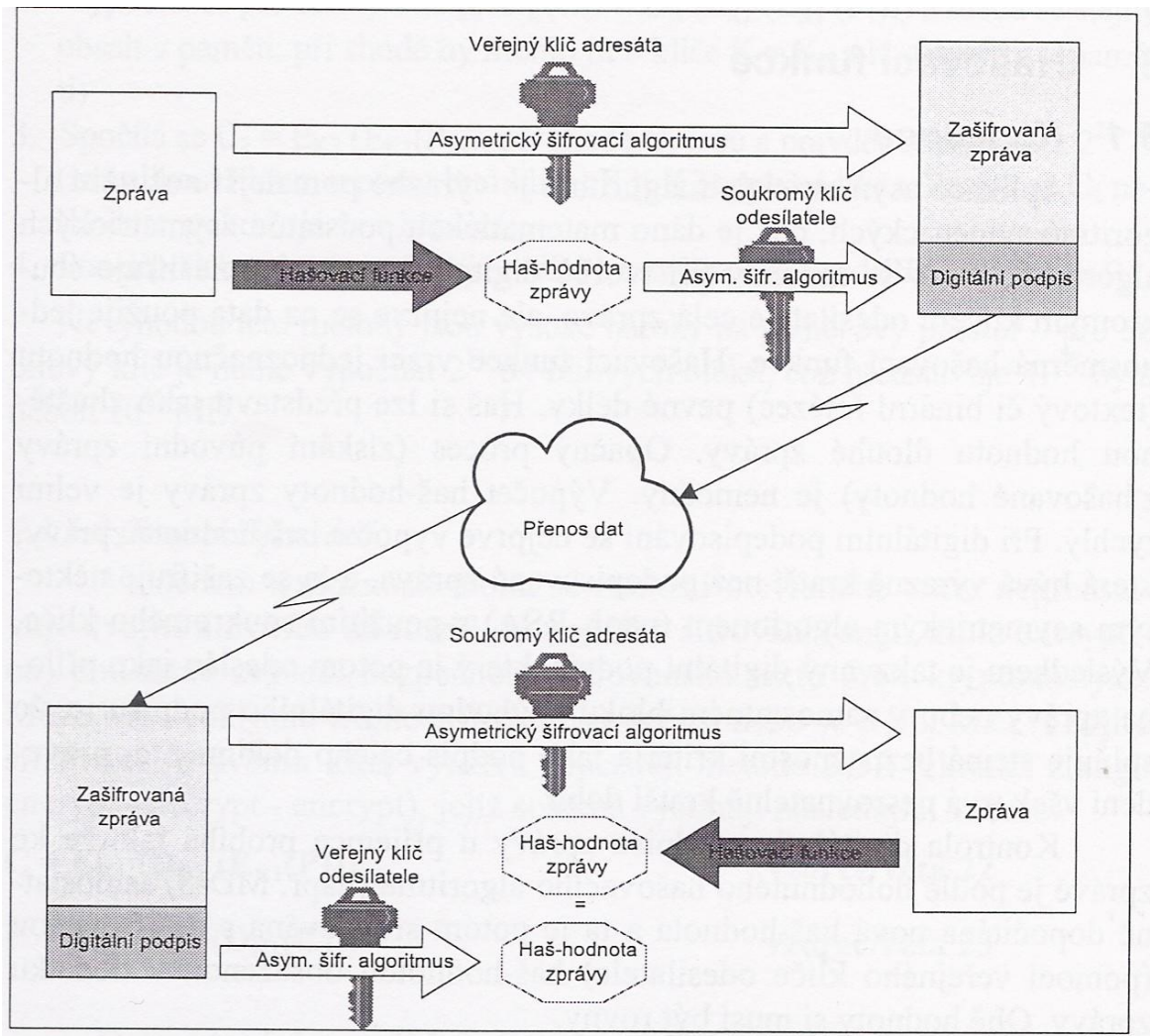
[17]

#### **2.2.6.2 eCache**

Používá virtual private network (VPN) TOR. A pro komunikaci slouží IRC. Měna založena na slepých podpisech RSA. V roce 1998 byla měna dostupná v: švýcarské bance Credit Suisse, německé Bank of Germany, finských Merita bank a Eunet, švédských Posten a v norské Bank of Norway.

#### **2.2.7 Digitální podpisy**

Elektronická/digitální podoba klasického podpisu. Zaručuje, že ten kdo podepsal soubor je opravdu ten, za koho se vydává. K použití digitálního podpisu je třeba mít certifikát vydaný certifikační autoritou. Digitální podepsání zaručuje, že dokument je původní a nikdo ho neupravoval (autenticita), nepoškozenost dokumentu (integrita), identifikace odesílatele (nepopiratelnost) a čas, kdy byl soubor odeslán (časové razítko). Postup vytváření digitálního podpisu: Z dokumentu se vypočítá hash. Hash se zašifruje autorovým soukromým klíčem a odešle. Důvěra podpisu se dokazuje platným certifikátem od Certifikační Autority ve kterém je i veřejný klíč autora. Certifikát se přikládá společně se zašifrovaným hashem k souboru. Pro digitální podpisy se používají následující algoritmy: Blokované šifry: CAST5, 3 DES, AES, Blowfish a Twofish. Asymetrické-klíčové šifry: ElGamal a RSA. Hashe: RIPEMD-160, MD5, SHA-1, SHA-2.



Obrázek 8: Schéma digitálního podpisu

[1] [2]

### 2.2.8 Ochrana autorských práv

Na digitální díla se používají jak digitální popisy, tak i vodoznaky a různé ukryté razítka, která zabraňují kopírování souboru či omezení vytváření kopií souboru. V případě vytvoření kopií je tak možné dohledat osobu, které dílo okopírovala či od které bylo dílo zkopírováno.

### 2.2.9 Vlastní šifrování souborů

Šifrování souborů se používá především pro utajení citlivých informací. Informací týkajících se speciální výroby a podobných tajných materiálů. Existují dva způsoby šifrování dat – souborů. Buď se šifruje virtuální disk, který se vytvoří na fyzickém a má

dynamickou velikost. Nebo se šifruje každý soubor zvlášť. Oba dva typy šifrování používají stejné algoritmy (DES, 3DES, AES, Blowfish, Serpent, Twofish).

## 2.3 ŠIFRY

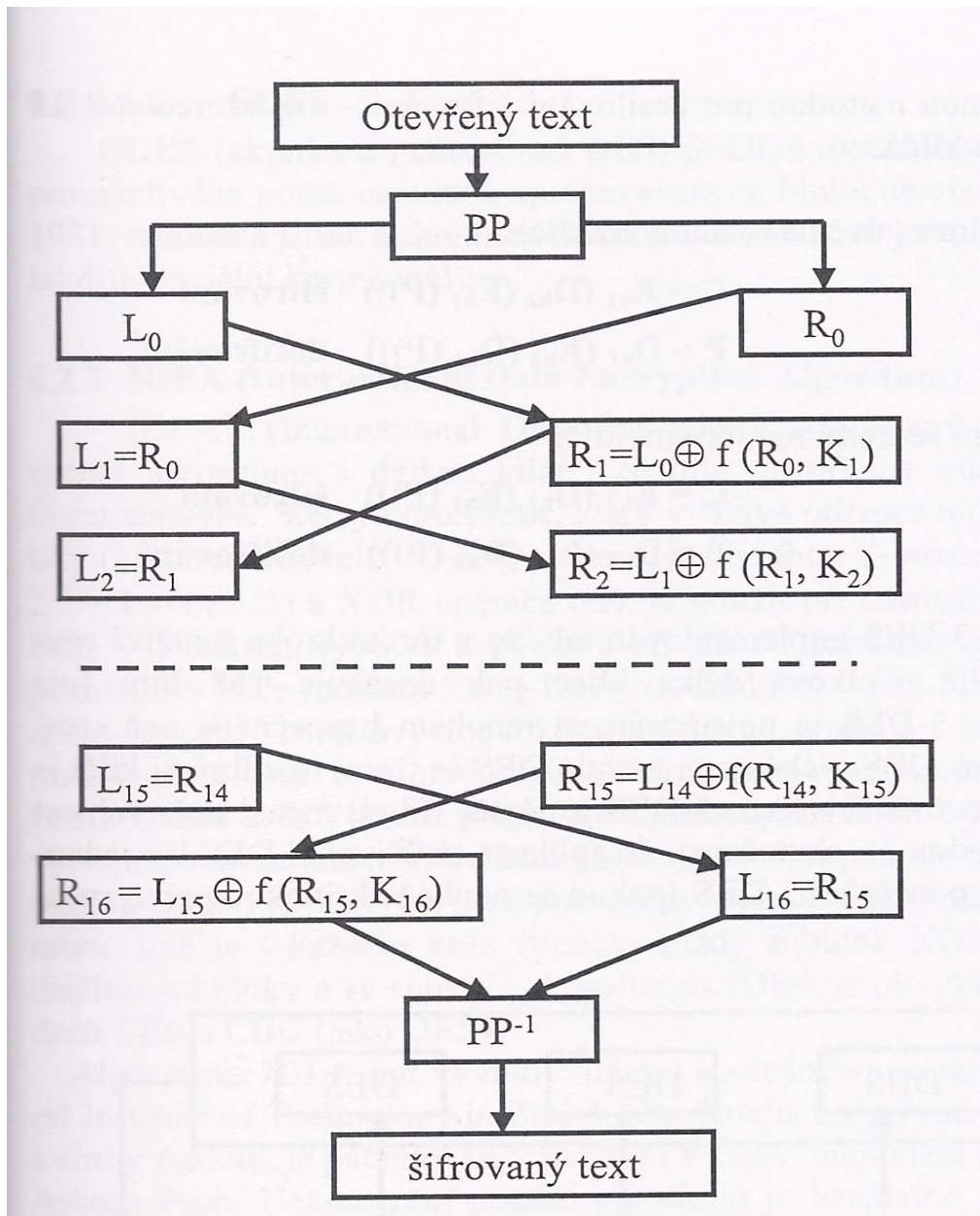
### 2.3.1 Šifra Lucifer

Prapředek současných šifer. Vymyšlena Horstem Fiestelem a jeho spolupracovníky v IBM roku 1970. Šifra je založena na feistelových sítích (substitučně-permutační síť využívající dvojice S-boxů). Měl více variant. Verze 1.0 používala 48 bitový klíč a vstupní text/data rozděleny do bloků o délce 48 bitů. Verze 2.0 používala 64 bitový klíč a vstupní text/data rozdělena do bloků o délce 32 bitů. Verze 3.0 používala klíč délky 128 bitů a vstupní data/text rozdělen na 128 bitové bloky.

[1] [2]

### 2.3.2 Šifra DES

25 let standart pro blokové šifry. Vyvinuta v roce 1975 firmou IBM. 1977 byla šifra publikována a 1979 přijmata jako standart NSA. Základem je šifra Lucifer. Vstupní text je rozdělen do bloků o 64 bitech, klíč má velikost 56 bitů z něhož je 8 bitů paritních – nevyužitelných. Používá 16 kol výpočtu (takzvaných rund). Používána do roku 2000.

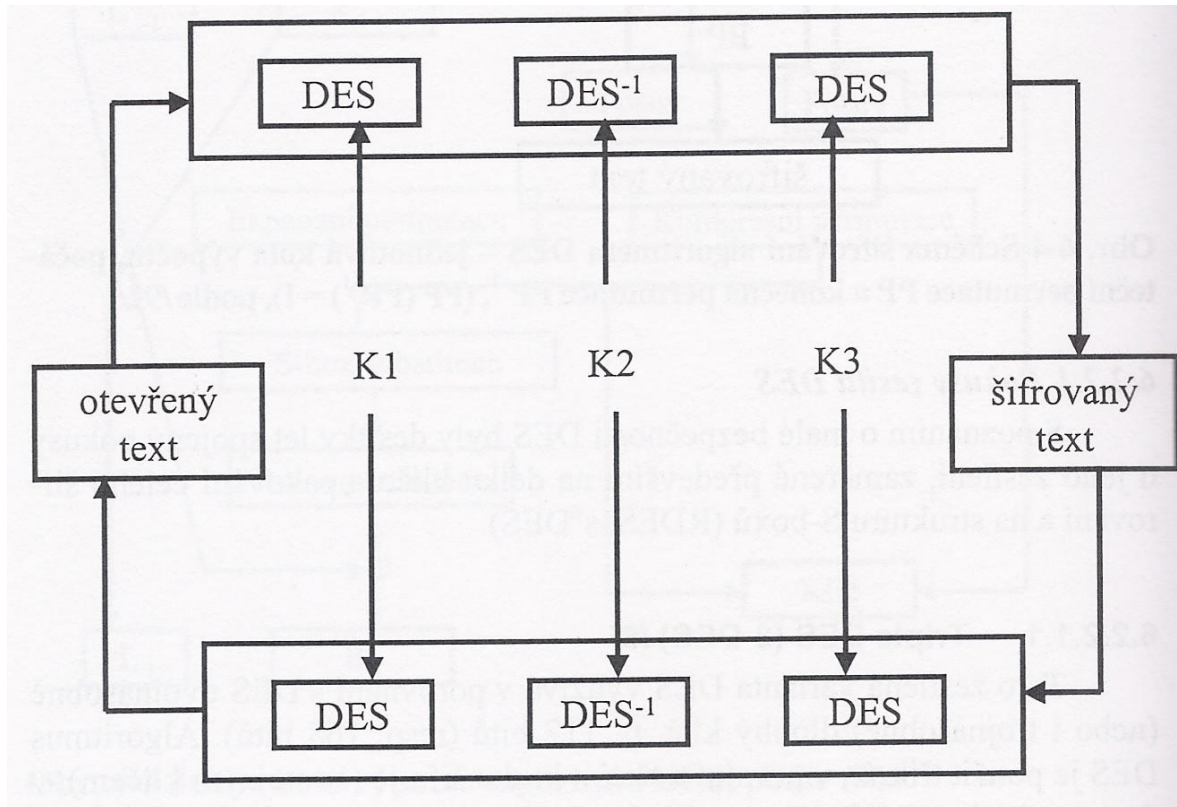


Obrázek 9: Počáteční a finální kolo výpočtu šifry DES

[1] [2]

### 2.3.3 ŠIFRA 3DES

Náhrada šifry DES. Využívána od roku 2000. Kombinace 3 DES šifer, více možností kombinací DES šifer. EDE nebo EEE, 1 klíč, 2 klíče, 3 klíče a dombinace.

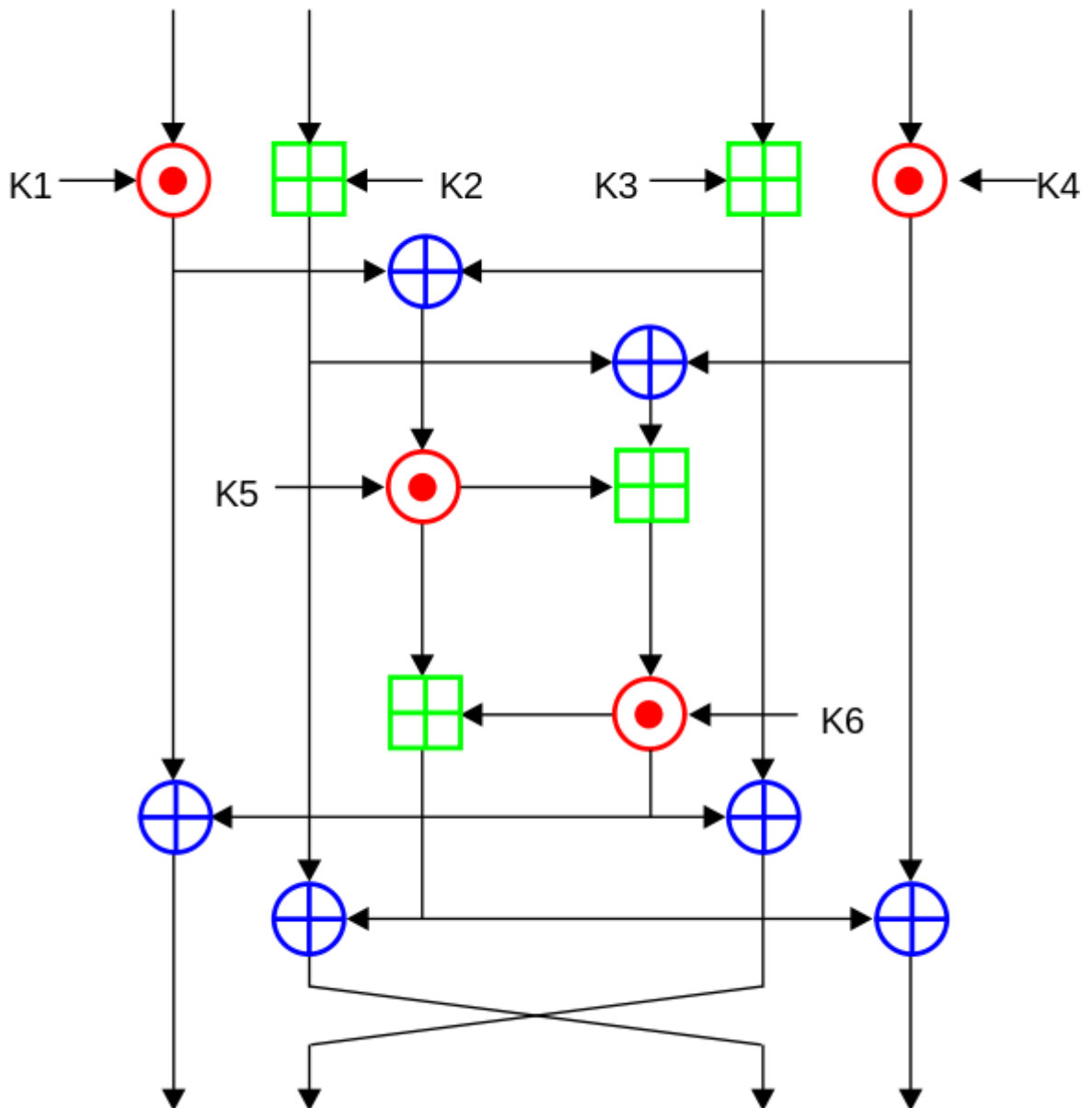


Obrázek 10: Schéma systému 3DES

[1] [2]

### 2.3.4 Šifra IDEA

Symetrická bloková šifra uvedena v roce 1992. Vstupní text/data rozdělena na bloky o velikosti 64 bitů, používá 128 bitový klíč. Proces výpočtu má 8 kol (rund). Používá 52 sub-klíčů generovaných z hlavního klíče, 6 sub-klíčů na kolo. 4 klíče použity na výstupní transformaci. V každé rundě se používají 4 16-bitové bloky s operacemi XOR, sečtení bloků, sečtení blok + klíč. Vytvoření subklíčů: 128 bitový hlavní klíč je rozdělen na 8 16 bitových klíčů. Následuje posunutí o 25 bitů doleva a další rozdělení na 8 16-b klíčů. Princip se opakuje dokud není vytvořeno 52 sub-klíčů.

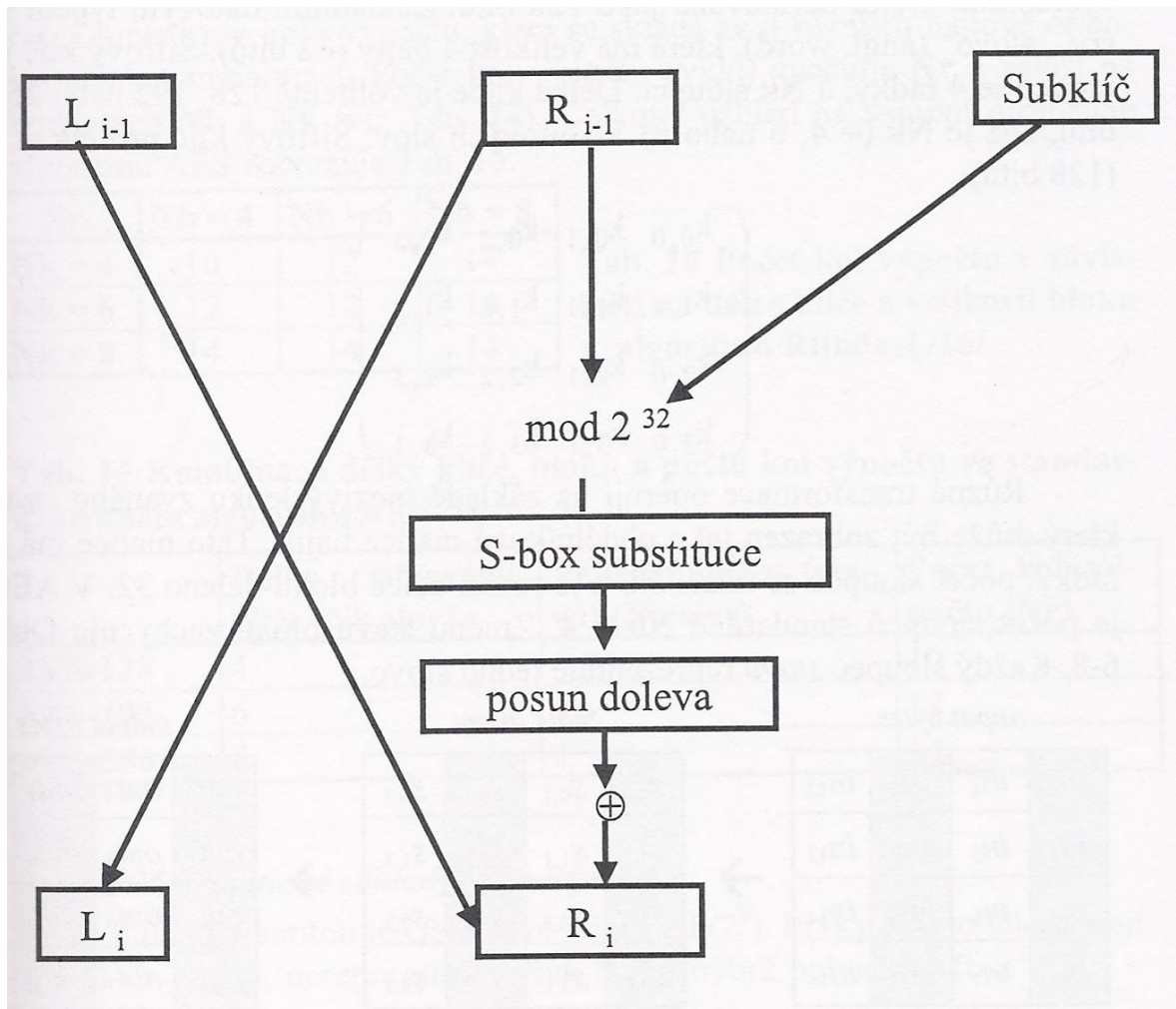


Obrázek 11: Vnitřní struktura kola výpočtu šifry IDEA

[1] [2]

### 2.3.5 Šifra GOST

Šifra vlád sovětského bloku, vytvořena v 70. letech 20. století – značen jako TOP SECRET (přísně tajné), 1990 stále používaná, ale již s nižším stupněm utajení SECRET (tajné), 1994 zveřejněna veřejnosti. Používá 256 bitový klíč, vstupní text/data rozdělen do bloků o velikosti 64 bitů. Používá 32 kol výpočtu (rund), bezpečnost byla založena na utajení S-boxů.



Obrázek 12: Vnitřní struktura kola výpočtu šifry GOST

[1] [2]

### 2.3.6 El Gammal

Podobný algoritmu RSA, používá se i pro digitální podpisy.

Postup algoritmu: Zvolí se prvočíslo  $p$ ; zvolí se náhodná čísla  $q$  a  $x$  menší jak  $p$ ; vypočítá se  $y = q^x \bmod p$ ;  $x$  představuje soukromý klíč, zatímco  $y, p, q$  představují veřejný klíč. Dále se volí  $k$  nesoudělné s  $(p-1)$ .

šifrování zprávy:  $a = q^k \bmod p$   $b = y^k \bmod p$

dešifrování zprávy:  $Z = b/a^x \bmod p$

[1] [2]

### 2.3.7 DSA

Vyvinut Davidem W. Kravitzem pracujícím v NSA. Vychází z algoritmu El Gammal. Využívá hashování funkce SHA-1 (v současných verzích SHA-2). Používá se jako podpisový algoritmus.

Postup:-volí dva parametry pro klíče  $L, N$  (1024-3072;160-256)

- volí se  $q$ -  $N$  bitové prvočíslo (délka musí být alespoň taková jako výstupu hashe)
- volí se  $p$ -  $L$  bitové prvočíslo, že  $p-1$  je násobkem  $q$
- vybere se  $g$  ( $y=h^{((p-1)/q)} \bmod p$ )  $1 < h < p-1$   $h$  se většinou volí jako 2
- vybere se  $x$  z rozsahu  $0 < x < q$
- vypočítá se  $y = q^x \bmod p$
- veřejný klíč  $(p, q, g, y)$ , soukromý klíč  $(x)$

[1] [2] [5]

### 2.3.8 AES – Endvanced Encryption standart

O standart soutěžili následné šifry: Rijndael, Twofish; Serpent; RC6; MARS

Jako AES byla vybrána roku 2001 šifra Rijndael. Symetrická bloková šifra publikována roku 1998. Vstupní text/data je rozdělen na 128 bitové bloky, používá klíč o velikostech 128/192/256 bitů. Výpočet má 10/12/14 kol (rund) (dle klíče se určuje počet rund).

Popis algoritmu:-rozšíření klíče

- kolo výpočtu:-záměna bitů
  - prohození řádků
  - kombinace sloupců
  - přidání sub-klíče
- finální kolo: -záměna bitů
  - prohození řádků
  - přidání subklíčů

[1] [2] [5]

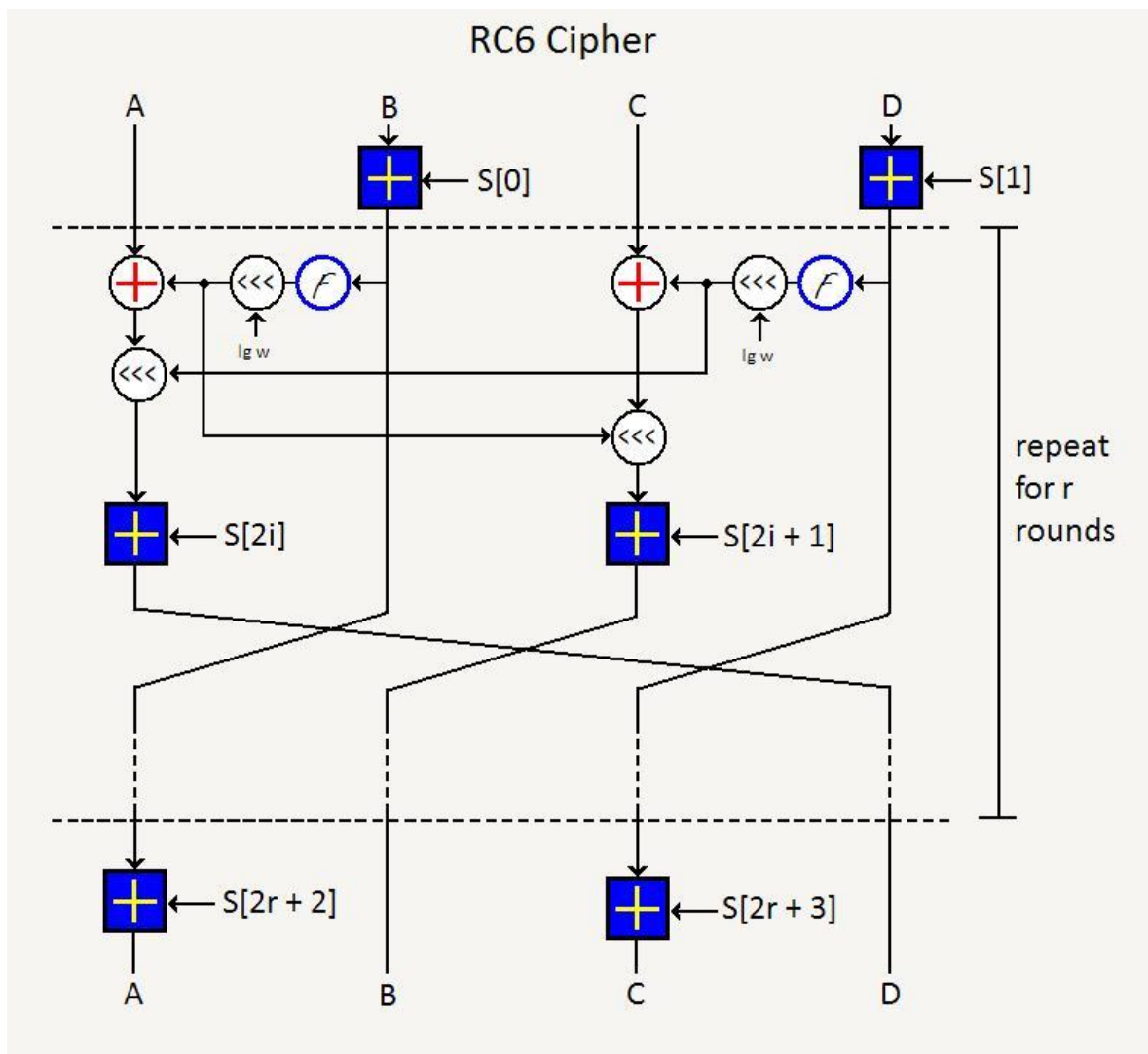
### 2.3.9 Rijndael

Na rozdíl od AES standartu nemá pevně dané velikosti bloků, můžeme volit bloky jako násobky 32.

[1] [2]

### 2.3.10 RC6

Symetrická bloková šifra vychází z šifry RC 5, vytvořena roku 1998 R. Rivestem, M. Robshaw, R. Sidney, Y. Lisa Yin. Podporuje klíče délky 128, 192 a 256 bitů, vstupní text/data rozdělen na bloky o velikosti 128 bitů. Lze považovat RC 6 jako dva paralelní RC5. Vnitřní struktura je Feistelova síť.



Obrázek 13: Vnitřní struktura bloku šifry RC6

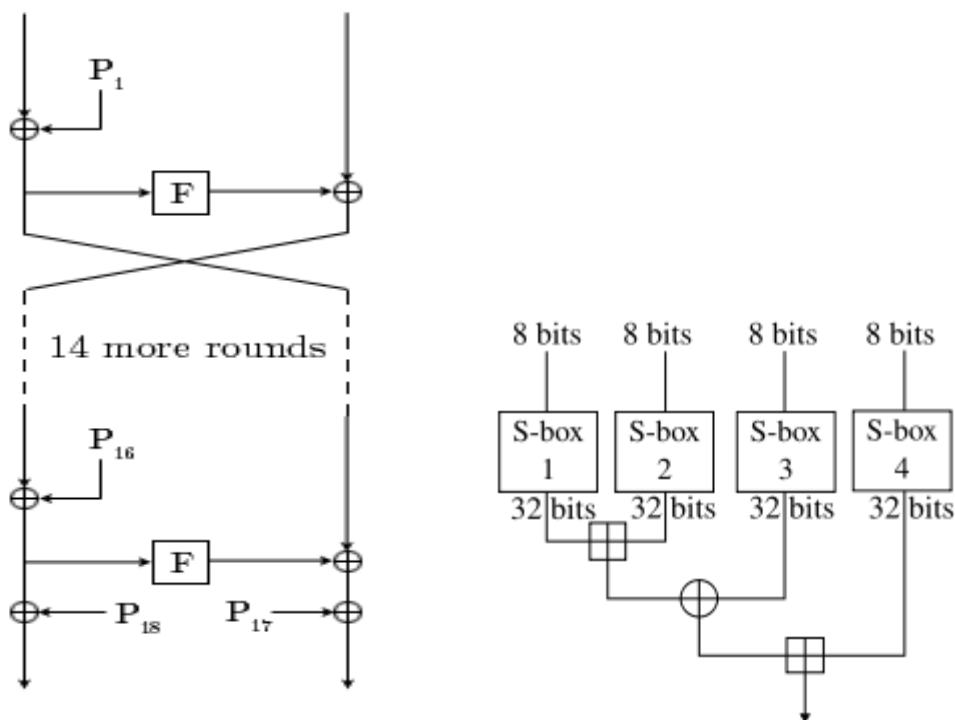
### 2.3.11 MARS

Bloková symetrická šifra vytvořena firmou IBM roku 1999. Využívá velikost bloků 128 bitů. Podporované délky klíče jsou veškeré násobky 32 bitů v rozmezí 128 a 448bitů. Využívá 32 kol výpočtu pomocí Feistelovy sítě.

[2]

### 2.3.12 Blowfish

Symetrická blokovaná šifra vytvořena roku 1993 Brucem Schneierem. Vstupní text/data rozdělen na bloky o velikosti 64 bitů, klíče jsou v rozmezí 32 – 448 bitů, používá 16 kol výpočtu. Vnitřní struktura je Feistelova síť.



Obrázek 14: Struktura funkce Blowfish

Obrázek 15: Struktura kola výpočtu Blowfish

### 2.3.13 Serpent

Symetrická blokovaná šifra vytvořena roku 1998 R.Andersonem, E.Bihmem a L.Knudsenem.

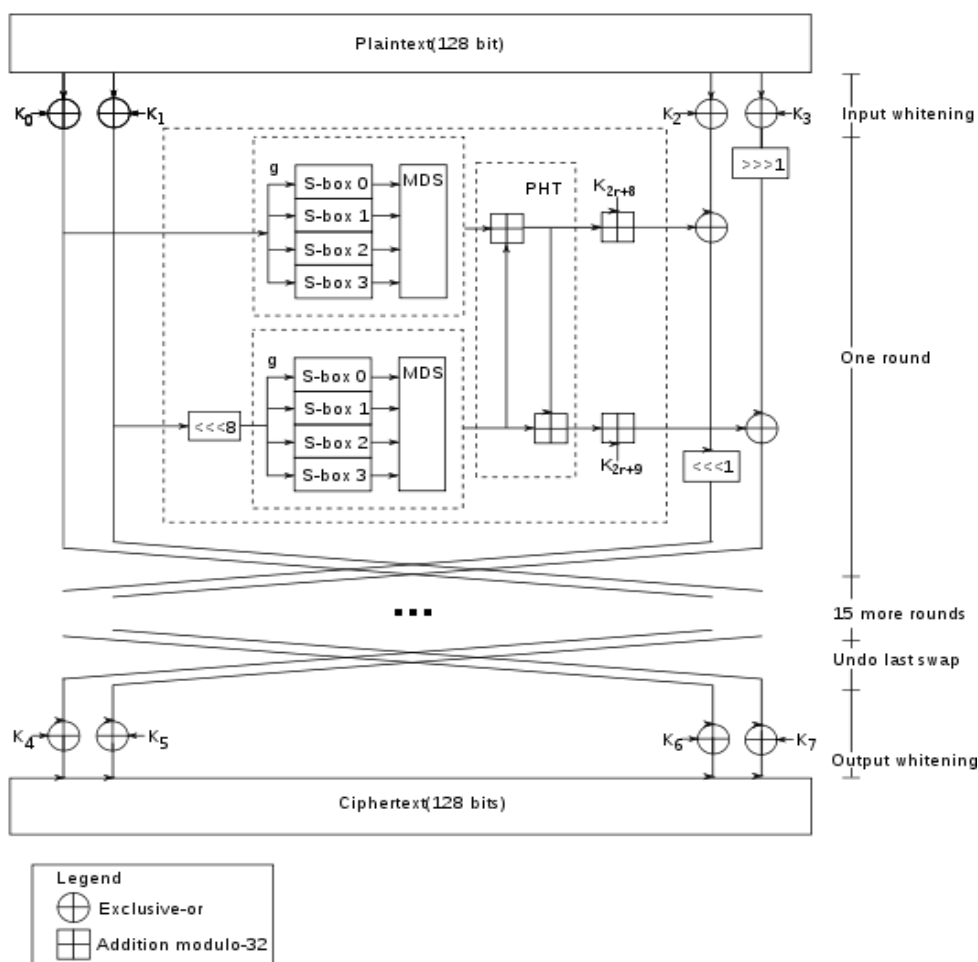
Používá klíč délky 128, 1925 a 256, vstupní text/data jsou rozděleny na bloky velikosti 128 bitů, využívá 32 kol výpočtu pomocí substitučně permutační sítě pracující s 32bitovými sub-bloky.

[2]

### 2.3.14 Twofish

Symetrická bloková šifra vycházející z šifry blowfish. Vytvořena roku 1998 Bruceem Schneierem, J. Kelsey, D. Whiting, C. Hall a N. Ferguson

Šifra implementována do systému OpenPGP, algoritmus je volně zdarma šiřitelný bez jakýchkoliv omezení. Používá 128, 192 a 256 bitové klíče, vstupní text/data jsou rozděleny na bloky velikosti 128 bitů, používá 16 kol výpočtu. Vnitřní struktura je Feistelova síť.



Obrázek 16: Struktura výpočtu šifry Twofish

[2]

### 2.3.15 Threefish

Bloková šifra vytvořena roku 2008. Je to část hashování funkce Skein. Používá klíče a bloky o stejné velikosti (256 - 1024), počet kol výpočtu je 72 (pro 1024 bit klíč je to 80).

### 2.3.16 RSA

Asymetrická šifra s veřejným klíčem, vytvořena roku 1977 R. Rivestem, A. Shamirem a L. Adlemanem z MIT. Založena na předpokladu složitosti faktorizace velkých čísel (1024 bitový klíč a více). V současné době je bezpečný, ale pouze za předpokladu velmi silného klíče, používá klíče o velikosti 1024 – 4096 bitů.

Postup: -zvolí se 2 náhodná prvočísla  $p$  a  $q$

-spočítá se jejich součin  $n = p * q$

-vypočítá se Eulerova funkce  $\phi(n) = (p-1)*(q-1)$

-zvolí se číslo  $e$ , menší jak  $\phi(n)$ , ale nesoudělné

-nalezne se číslo  $d$ , s podmínkou  $d * e = 1 \pmod{\phi(n)}$

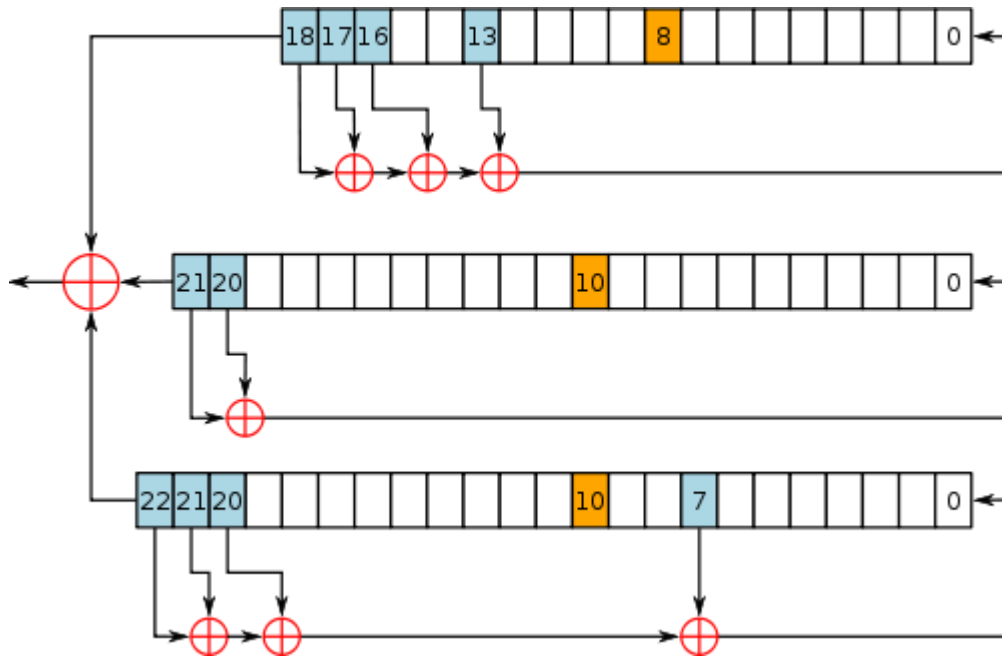
Šifrování:  $c = m^e \pmod{n}$

Dešifrování:  $m = c^d \pmod{n}$

[1][5]

### 2.3.17 A5/1

Vytvořena v roce 1987, algoritmus byl zveřejněn v roce 1994, 1995 získán jeho zdrojový kód. Jedná se o proudovou šifru, používající 64 bitový klíč. Výstupní data jsou 114 bitová (což je blok dat, které se odesílají z mobilního telefonu do sítě). Základem je kombinace tří lineárních zpětnovazebních posuvných registrů.



Obrázek 17: Vnitřní struktura šifry A5/1

### 2.3.18 A5/2

Vytvořena roku 1989, zveřejněna v roce 1994. 1999 byl kód publikován veřejnosti. Od roku 2006 mobilní telefony tuhle šifru nadále nepodporují. Od roku 2007 je přísný zákaz implementace téhle šifry do další zařízení. Princip založen na 4 lineárních zpětnovazebních posuvných registrech a nelineárním slučovači (sčítač)

### 2.3.19 A5/3

Známa taky pod názvem KASUMI. Vytvořena primárně pro 3GPP síť (síť třetí generace – umožňující připojení i do internetu). Je to bloková šifra s 128 bitovým klíčem, 64 bitovým vstupem i výstupem. Jádrem je Feistelova síť s 8 koly výpočtu, každé kolo používá 16 bitový subklíč derivovaný z hlavního klíče.

[14][18]

## 2.4 Hashovací funkce/algoritmy

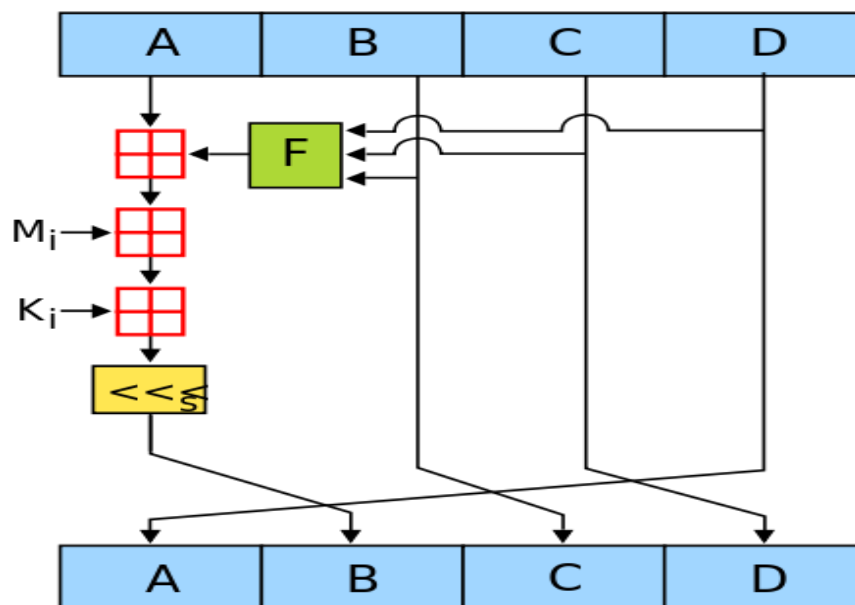
Jednosměrné funkce, používají se v některých cifrách jako S-boxy. Samostatně mimo šifrovací algoritmy se používají pro ověření neporušení souborů.

### 2.4.1 MD2

Algoritmus vytvořen roku 1989 Ronem Rivestem pro 8bitové počítače. I když není bezpečný používá se ještě jako část generování klíčů. Otisk má velikost 128 bitů a výpočet má 18 kol

### 2.4.2 MD4

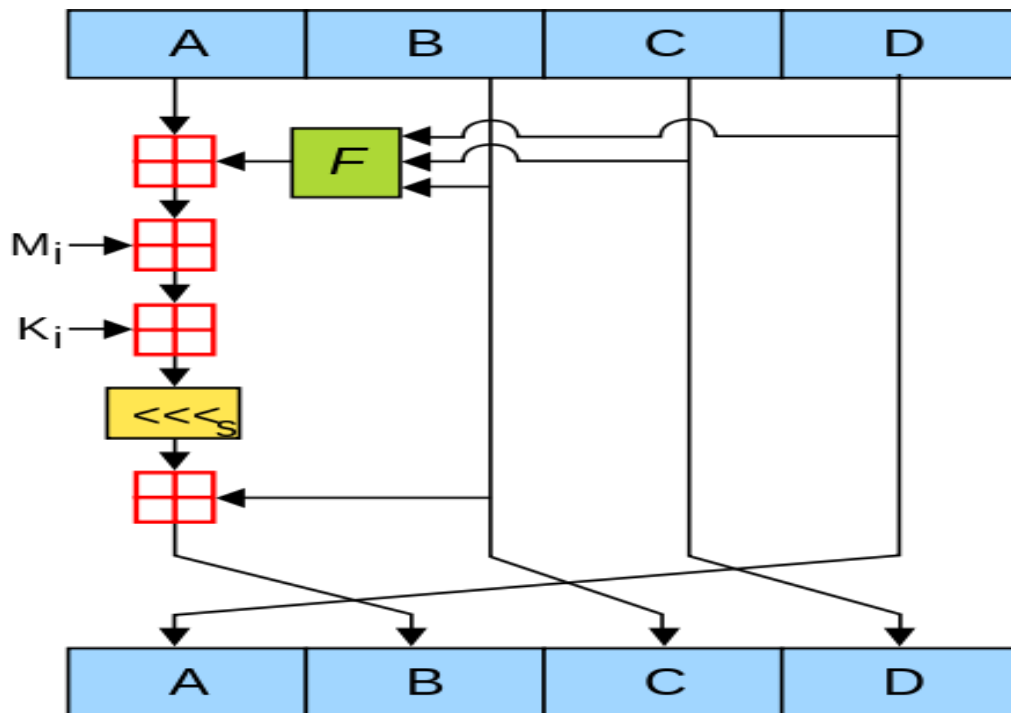
Algoritmus vytvořen R. Rivestem roku 1990. Používá se v systémech Windows NT, XP, Vista a 7 pro hash otisk hesla pro přihlašování do systému. Otisk má velikost 128 bitů, provádí se 3 kola výpočtu (16 operací za kolo).



Obrázek 18: Vnitřní struktura hashovací funkce MD4

### 2.4.3 MD5

Vytvořen roku 1991 R. Rivestem. Otisk má velikost 128 bitů, provádí se 4 kola výpočtu (16 operací za kolo).



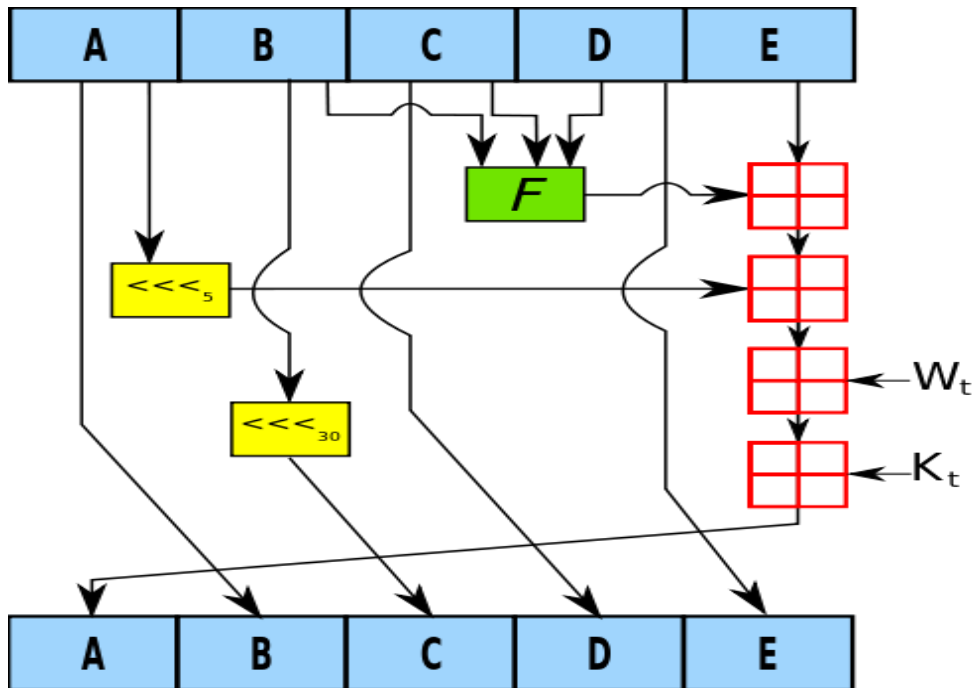
Obrázek 19: Vnitřní struktura hashování funkce MD5

#### 2.4.4 MD6

Vytvořen roku 2008. Velikost otisku se pohybuje v rozmezí 0 – 512 bitů. Počet kol výpočtu je v rozmezí 40 – 168.

#### 2.4.5 SHA-1

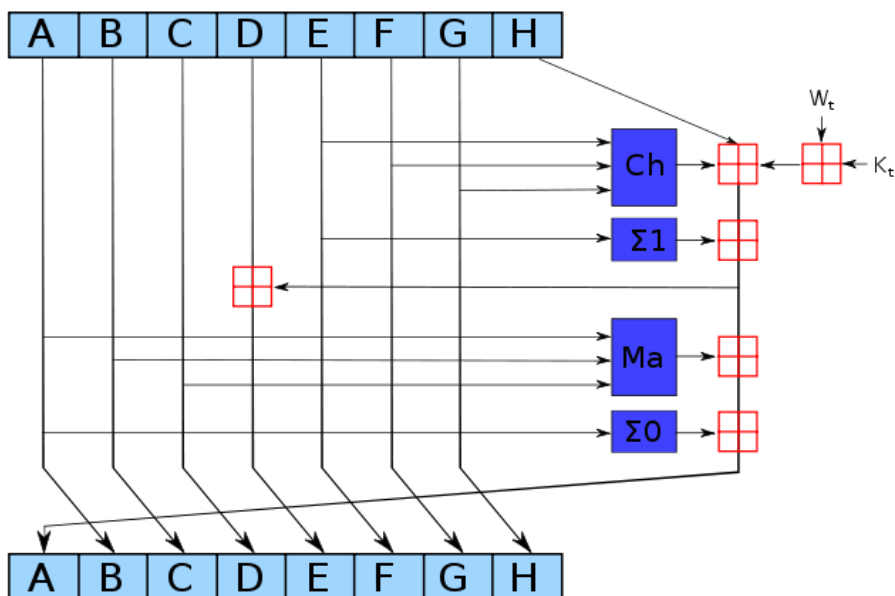
Algoritmus vytvořen agenturou NSA v roce 1993 (prototyp SHA-0). Roku 1995 vytvořen algoritmus SHA-1. Velikost otisku je 160 bitů, provádí 80 kol výpočtu. Vnitřní velikost bloků je 512 bitů. Omezení vstupu na  $2^{64}$  bitů. Vpodobnou strukturu jako MD4/5. V současnosti používán na heslování kancelářských souborů z balíku Microsoft Office 2007 a součást některých šifer.



Obrázek 20: Vnitřní struktura hashování funkce SHA1

### 2.4.6 SHA-2

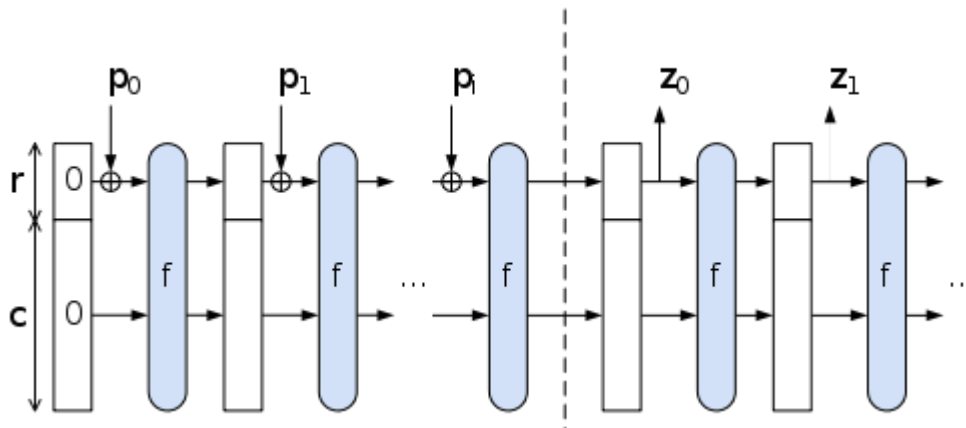
Vytvořen agenturou NSA roku 2001. Existuje více verzí SHA-224, SHA-256, SHA-384 a SHA-512). Používá 64 nebo 80 kol výpočtu, vnitřní velikost bloků je 512 bitů. Využívá Merkle-Damgardova konstrukce. Používá se v TLS, SSL, PGP, SSH, BitCoin a pro kontrolu souborů.



Obrázek 21: Vnitřní struktura hashování funkce SHA2

### 2.4.7 SHA-3

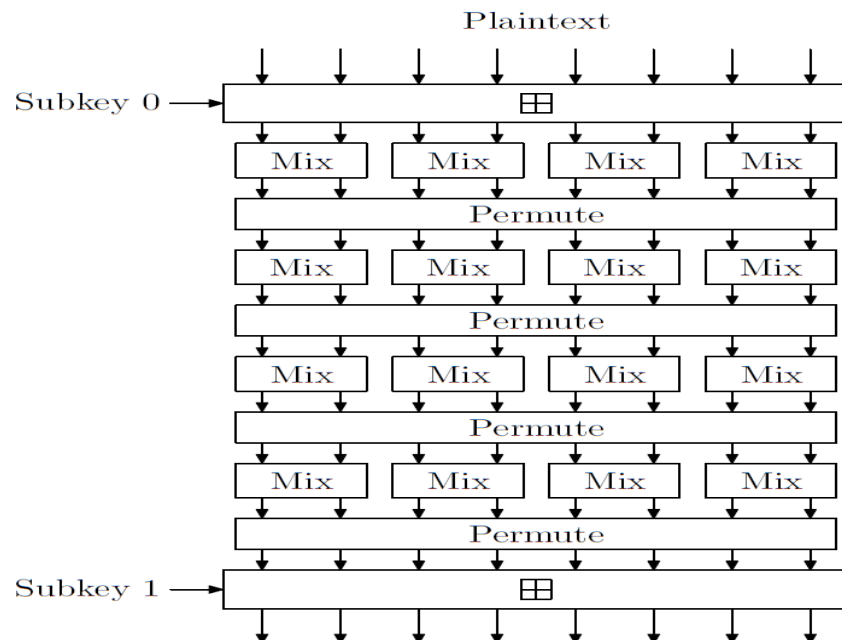
Původně znám jako Keccak. V roce 2012 vítězem NIST soutěže hash funkcí. Využívá takzvané „houbovitě konstrukce“



Obrázek 22: Vnitřní struktura hashování funkce SHA3

#### 2.4.7.1 Skein

Odvozen od šifry Threefish, finalista NIST soutěže hash funkcí. Používá 72 nebo 80 kol výpočtu, délka bloku je 256, 512 a 1024 bitů. Délka otisku je volitelná.



Obrázek 23: Vnitřní struktura hashování funkce Skein

## **II. PRAKTICKÁ ČÁST**

### 3 DEMONSTRATIVNÍ UKÁZKY ŠIFROVACÍCH METOD

Pro demonstraci byli vytvořeny programy – šifry ve vývojových prostředích Wolfram Mathematica a Eclipse IDE pro JAVA a Javascript pro webové stránky. Jedná se o následující šifry a hashe: Transpozice, Substituce, Vernamova šifra, Viegnerova šifra, DES, RSA, RC4, SHA-1, MD-5

#### **Transpoziční šifra**

Vytvořena v prostředích Javascript a Wolfram Mathematica.

#### **Substituční šifra**

Vytvořena v prostředích Javascript a Wolfram Mathematica.

#### **Viegnerova šifra**

Vytvořena v prostředí Wolfram Mathematica.

#### **Vernamova šifra**

Vytvořena v prostředích Javascript a Wolfram Mathematica.

#### **DES**

Vytvořena v prostředích Java..

#### **RSA**

Vytvořena v prostředí Wolfram Mathematica.

#### **RC4**

Vytvořena v prostředí Java.

#### **SHA-1**

Vytvořena v prostředí Java.

#### **MD5**

Vytvořena v prostředí Java

## 3.1 Porovnání současných metod zabezpečení

Šifra	Délka klíče	délka bloku	počet kol výpočtu	typ	prolomena	možnost útoků	rychlost
Rinjadel (AES)	128		10	Blokovaná		útok	75 MB/s
	192	128	12	Subs.	ne	postraními	-
	256		14	Permut. síť		kanály (8 kol)	-
Twofish	128			Blokovaná		zkrácená	-
	192	128	16	Feistelova síť	ne	diferenciální kryptoanalýza	63 MB/s
Blowfish	256			Blokovaná		diferenciální	-
	32 - 448 (64)	64	16	Feistelova síť	ne	kryptoanalýza	-
Serpent				Blokovaná		lineární	
	448	64	-	Subs. Permut. síť	ne	kryptoanalýza	58 MB/s
RC2	8 - 128			Blokovaná		Related key attack	-
RC4		64	16+2	Feist. síť	ano		-
	40-2048	2064	256	proudová	ano	-	-
IDEA	128	64	8,5	Blokovaná Add-Rotate-xor	ne	Related key attack	-
3DES	128			Blokovaná			
	168 - 192	64	48	Feistelova síť	ne	-	20 MB/s
DES	56	64	16	-//-	1997	Brute force	21 MB/s
A5/3	128	64	8	Blokovaná Feist. síť	2010	Related key attack	-
Vernamova	-	-	1	Substituční	nikdy	?	XoR ~2TB/s
Substitute	-	-	1	Substituční	15. století	Frekvenční analýza, bruteforce	-
Transpozice	-	-	1	Transpoziční	15. století	Bruteforce	-

Tabulka 2: Přehled šifer a jejich vlastností

Porovnávat jednotlivé šifry společně nejde, ale obecně platí, že čím rychlejší šifra, tím je více náchylná vůči kryptoanalýze. Z hlediska bezpečnosti je nelepší používat co nejdelší klíče co algoritmus dovoluje. Jako obecně nejlepší volba se jeví šifra Rinjadel (AES). Pro aplikace, kde není důležitá rychlost se může použít 3DES, která je 3x pomalejší jak AES.

## 4 MULTIMEDIÁLNÍ POMŮCKA PRO VÝUKU NA FAI

### 4.1 Základní pohled na stránky

Pro vytvoření stránek bylo použito technologií CSS a Javascript. Jedná se o stránky statické. Při návrhu stránek byl hlavní důraz kladen na snadnou orientaci. Stránka je rozdělena do dvou sloupců a menu nad ním. Menu zůstává neustále stejné. V levém sloupci je proměnný rozcestník - submenu. Dolní část stránek je tvořena footerem. Na design stránky je použita technologie CSS. Stránky jsou optimalizovány převážně pro prohlížeč Mozilla Firefox.



Obrázek 24: Náhled první webové stránky

## **4.2 Popis odkazů menu**

### **4.2.1 Úvod**

Stránka nastavená jako domovská. Sloužící jako první náhled o co se jedná v Kryptologii, jaké je její základní rozdělení. V levé části je rozcestník – submenu z kterého se dostaneme do jednotlivých rozdělených částí.

### **4.2.2 Základní pojmy**

Slouží k ujasnění pojmů, které se v kryptologie obecně používají a vyskytují se i na stránkách. V submenu je možno najít některé základní pojmy i v anglickém jazyce. (překlad z anglického jazyka do českého)

### **4.2.3 Historie – vývoj**

Tahle část se zabývá vývojem kryptologie od jejího počátku až po současnou dobu. Je rozdělena na tři kategorie. První kategorie je od počátků po 19. století. Do druhé kategorie patří období od počátku 20. století po konec 2. světové války. Třetí kategorie je od konce 2. světové války po současnost. V submenu je každá kategorie ještě rozdělena na časové úseky. Většinou popsán i princip jednotlivých šifer.

### **4.2.4 Rozdělení**

Na téhle stránce se nachází základní rozdělení šifer a jejich krátký popis.

### **4.2.5 Principy**

Stránka obsahuje vysvětlení principů šifer, které nebyli zmíněny v sekci Historie - vývoj

### **4.2.6 Příklady šifer**

Stránka slouží jako informační rozcestník pro jednotlivé šifrovací jazyky. Na jednotlivé šifrovací jazyky se dostane i ze submenu.

### **4.2.7 Programy**

Tato část patří krátkému rozdělení současných šifrovacích programů. Rozděluje je do několika kategorií podle funkce. Udává taky zástupce z jednotlivých kategorií.

#### 4.2.8 Zdroje

Stránka se v menu nenachází, je dostupná pouze z linku footeru. Jedná se o tabulku se zdroji obrázků.

## ZÁVĚR

V první části rešerše byly zmíněny základní pojmy z oboru kryptologie a jejího rozdělení. Následující definice jednotlivých částí a čím se zabývají a jejich další rozdělení. Dále byly zmíněny základní pojmy oboru a krátké připomenutí historie kryptologie.

V druhé teoretické části se nachází krátké rozdělení současné kryptologie. Dále následují oblasti současného života, kde se s kryptologií setkáváme. Poté následuje krátký popis jednotlivých šifer.

V praktické části byly vytvořeny demonstrativní ukázky vybraných šifer. Byly vytvořeny v různých programovacích jazycích. Následně byli porovnány jednotlivé metody zabezpečení dat – šifrování.

Vytvořené webové stránky jsou zcela funkční. Na jejich vývoji se v budoucnu bude neustále pracovat. Budou sloužit také k výuce Kryptologie na Univerzitě Tomáše Bati ve Zlíně

## ZÁVĚR V ANGLIČTINĚ

In the first part of the research were discussed basic concepts in the field of cryptology and its distribution. The following definitions of individual parts and what they do and their subdivisions. Were also mentioned basic concepts of the field and a short reminder of the history of cryptology.

The second theoretical part is a short distribution of current cryptology. Then there are areas of our life where we meet with cryptography. This is followed by a brief description of each cipher.

In the practical part were created illustrative examples of selected ciphers. They were created in different programming languages. Then they compared different methods of data security - encryption. Created website is fully functional. Their development will continue also in the future. The website will also serve to teach Cryptology at Tomas Bata University in Zlin

**SEZNAM POUŽITÉ LITERATURY**

- [1] ZELENKA, Josef, Jan ČAPEK, Jiří FRANCEK a Hana JANÁKOVÁ. *Ochrana dat: kryptologie*. Vyd. 1. Hradec Králové: Gaudeamus, 2003, 198 s. ISBN 80-704-1737-4.
- [2] BITTO, Ondřej. *Šifrování a biometrika aneb tajemné bity a dotyky*. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-866-8648-5.
- [3] ČANDÍK, Marek. *Základy informační bezpečnosti*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 107 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 80-731-8218-1.
- [4] VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. 1. vyd. Praha: Albatros, 2006, 340 s. Oko. ISBN 80-00-01888-8.
- [5] KATZ, Jonathan a Yehuda LINDELL. *Introduction to modern cryptography*. Boca Raton: Chapman, 2008, xviii, 534 s. ISBN 978-1-58488-551-1.
- [6] PIPER, F a Sean MURPHY. *Kryptografie*. 1. vyd. v českém jazyce. Překlad Pavel Mondschein. Praha: Dokořán, 2006, 157 s. ISBN 80-736-3074-5.
- [7] FM 34-40-2 Basic Cryptanalysis [online]. [cit. 2013-06-12]. Dostupné z: <http://www.umich.edu/~umich/fm-34-40-2/>
- [8] ZELINKA, Ivan. Vyuka [online]. [cit. 2013-06-12]. Dostupné z: <http://www.ivanzelinka.eu/hp/Vyuka.html>
- [9] Kvantová kryptografie pro bezpečnou distribuci klíčů - Lupa.cz. [online]. [cit. 2013-06-12]. Dostupné z: <http://www.lupa.cz/clanky/kvantova-kryptografie-pro-bezpecnou-distribuci-klicu/>
- [10] WEP-/WPA-Keygen. [online]. [cit. 2013-06-12]. Dostupné z: <http://darkvoice.dyndns.org/wlankeygen/>
- [11] Bezdrátové sítě. [online]. [cit. 2013-06-12]. Dostupné z: <http://www.barts.cz/index.php/pocitace/site/29-bezdratovesite.html>
- [12] Weakness in Passphrase Choice in WPA Interface - Wi-Fi Networking News. [online]. [cit. 2013-06-12]. Dostupné z: [http://wifinetnews.com/archives/2003/11/weakness\\_in\\_passphrase\\_choice\\_in\\_wpa\\_interface.html](http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html)

- [13] Understanding WEP Weaknesses - For Dummies. [online]. [cit. 2013-06-12].  
Dostupné z: <http://eu.dummies.com/WileyCDA/how-to/content/understanding-wep-weaknesses.html>
- [14] WebCite query result. [online]. [cit. 2013-06-12]. Dostupné z:  
<http://www.webcitation.org/64FzqeRV8>
- [15] RFC 6101 - The Secure Sockets Layer (SSL) Protocol Version 3.0. [online]. [cit. 2013-06-12]. Dostupné z: <https://tools.ietf.org/html/rfc6101>
- [16] RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2. [online]. [cit. 2013-06-12]. Dostupné z: <https://tools.ietf.org/html/rfc5246>
- [17] Bitcoin - Open source P2P digital currency [online]. [cit. 2013-06-12]. Dostupné z:  
<http://bitcoin.org/en/>
- [18] Security in the GSM network - security\_in\_the\_gsm\_network.pdf. In: [online]. [cit. 2013-06-12].  
Dostupné z:  
[http://ipsec.pl/files/ipsec/security\\_in\\_the\\_gsm\\_network.pdf](http://ipsec.pl/files/ipsec/security_in_the_gsm_network.pdf)
- [19] Hash Functions and Block Ciphers. In: [online]. [cit. 2013-06-12]. Dostupné z:  
<http://burtleburtle.net/bob/hash/index.html>
- [20] Understanding Cryptography, A Textbook for Students and Practitioners - with a Foreword by Bart Preneel [online]. [cit. 2013-06-12]. Dostupné z:  
<http://wiki.crypto.rub.de/Buch/movies.php>
- [21] Cryptographic hash function - Wikipedia, the free encyclopedia. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-06-12]. Dostupné z:  
[https://en.wikipedia.org/wiki/Cryptographic\\_hash\\_function](https://en.wikipedia.org/wiki/Cryptographic_hash_function)

## SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3DES	3x Data Encryption Standard – symetrický šifrovací algoritmus
AES	- symetrická bloková šifra
CPU	Central Procesor Unit - procesor počítače
CSS	Kaskádové styly
DES	Data Encryption Standard – symetrický šifrovací algoritmus
DSA	Digital Signature Algorithm – Algoritmus digitálního podpisu
EDE	šifrování dešifrování šifrování
EEE	šifrování šifrování šifrování
FTP	File Transfer Protocol
GSM	Globální Systém pro Mobilní komunikaci
HIFS	metoda fraktální kryptologie
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBM	Mezinárodní počítačová firma
IDEA	International Data Encryption Algorithm
IFS	metoda fraktální kryptologie
IMAP	Internet Message Access Protocol
IRC	Internet Relay Chat
MD5	Message-Digest algorithm - hashovací funkce
MIT	Massachusetts Institute of Technology - Massachusettský technický institut
NIST	Národní institut standardů a technologie
NSA	National Security Agency- <i>Národní bezpečnostní agentura Spojených států</i>
P2P	Peer to peer - typ připojení počítačů
PC	osobní počítač
POP3	Post Office Protocol
PSK	Pre shared key předsdílený klíč
RC2	bloková šifra
RC4	bloková šifra
RSA	šifrovací algoritmus
SHA	Secure Hash Algorithm - Hashovací funkce
SSH	Secure Shell
SSL	Secure Sockets Layer
TEA	metoda fraktální kryptologie
TLS	Transport Layer Security
TOR	Název síť
VPN	Virtuální privátní síť – druh počítačové sítě
WEP	Wired Equivalent Privacy soukromí ekvivalentní drátovým sítím
WIFI	bezdrátová síť
WPA	Wi-Fi Protected Access chráněný přístup k Wi-Fi
XOR	Exlusive OR součet

**SEZNAM OBRÁZKŮ**

Obrázek 1: Rozdělení kryptologie .....	12
Obrázek 2: Rozdělení šifer .....	17
Obrázek 3: Transpoziční šifra .....	18
Obrázek 4: Substituční šifra.....	18
Obrázek 5: Kódová kniha .....	19
Obrázek 6: Hashovací funkce Zdroj: Prednasky předmětu Kryptologie, FAI, UTB Zlín .....	23
Obrázek 7: SSL Handshake .....	28
Obrázek 8: Schéma digitálního podpisu .....	32
Obrázek 9: Počáteční a finální kolo výpočtu šifry DES.....	34
Obrázek 10: Schéma systému 3DES.....	35
Obrázek 11: Vnitřní struktura kola výpočtu šifry IDEA.....	36
Obrázek 12: Vnitřní struktura kola výpočtu šifry GOST .....	37
Obrázek 13: Vnitřní struktura bloku šifry RC6 .....	39
Obrázek 14: Struktura funkce Blowfish .....	40
Obrázek 15: Struktura kola výpočtu Blowfish.....	40
Obrázek 16: Struktura výpočtu šifry Twofish .....	41
Obrázek 17: Vnitřní struktura šifry A5/1 .....	43
Obrázek 18: Vnitřní struktura hashování funkce MD4.....	44
Obrázek 19: Vnitřní struktura hashování funkce MD5 .....	45
Obrázek 20: Vnitřní struktura hashování funkce SHA1 .....	46
Obrázek 21: Vnitřní struktura hashování funkce SHA2.....	46
Obrázek 22: Vnitřní struktura hashování funkce SHA3.....	47
Obrázek 23: Vnitřní struktura hashování funkce Skein .....	47
Obrázek 24: Náhled první webové stránky .....	51

**SEZNAM TABULEK**

Tabulka 1: Charakteristické rysy etap rozvoje kryptologie Zdroj:Ochrana dat.

Kryptologie .....	20
Tabulka 2: Přehled šifer a jejich vlastností.....	50

## SEZNAM PŘÍLOH

Zdrojové kódy od webové prezentace a šifer přiloženy na CD.