

Bezpečnost v informačních technologiích (KIV/BIT)

2. Ochrana informací šifrou, typy šifer, použití, příklady

Ing. Pavel Král, Ph.D.

Katedra informatiky a výpočetní techniky
Západočeská Univerzita

18. února 2015

1 Rozdělení šifer

2 Historické šifry

- Šifra ATBAŠ
- Cézarova šifra
- ...

3 Šifrovací stroje

Rozdělení šifer

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ
Cézarova šifra

...

Šifrovací stroje

- substituční
- transpoziční
- kombinace

- symetrické (jeden klíč pro šifrování i dešifrování)
 - blokové
 - proudové

- asymetrické (jeden klíč pro šifrování , druhý pro dešifrování)

záměna znaku (skupiny znaků) za jiný znak (skupinu znaků)

1 jednoduchá substituční (monoalfabetická šifra)

- jeden znak otevřeného textu → jeden znak šifrového textu

2 homofonní substituční šifra

- jeden znak plaintextu → jeden znak z množiny znaků

3 polygramová subst. šifra

- skupina znaků plaintextu → skupina znaků šifrového textu

4 polyalfabetická substituční šifra

- spojení několika jednoduchých šifer; postupná aplikace

- vznik okolo roku 500 př.n.l.
- písmena hebrejské abecedy použity v substitučním systému násl. způsobem:
 - záměna písmene za písmeno ležící ve stejné vzdálenosti od konce abecedy.
 - (první písmeno je nahrazeno posledním, druhé předposledním atd.)
 - princip v názvu ← **A-T-B-Š** první písmeno hebrejské abecedy (alef), poslední (thav), druhé (bet) a předposlední (šin)

Cézarova šifra

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ
Cézarova šifra

...
Šifrovací stroje

- jedna z nejstarších, jednoduchost
- použití pro vojenskou komunikaci, Julis Caesar, zmatení Galů, popis v Zápiscích o válce galské
- modifikována použita ruskou carskou armádou za 1. sv. války
- nahrazení znaku znakem o tři místa vpravo ($A \rightarrow D$, $B \rightarrow E$, $Z \rightarrow C$)
- abeceda šifrového textu = rotace abecedy plaintextu (\times obecná permutace)
- Příklad: FHCDURYD VLIUD
- v praxi přenos po skupinách znaků, např. 4: FHCD URYD VLIU D
- *zobecnění*: posun o $K =$ klíč \rightarrow 26 různých klíčů (počet písmen abecedy)

Monoalfabetická substituce

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry
Šifra ATBAŠ
Cézarova šifra
...

Šifrovací stroje

- významné vylepšení
- \forall symbol plaintextu \exists šifrový symbol
- Př:
 - A B C D ..
 - X A F R ..
- výrazně více klíčů (počet \forall permutací písmen abecedy) = $26! \approx 4 \times 10^{26}$ klíčů
- tvorba klíče
 - náhodně \rightarrow složité zapamatování \rightarrow složitá distribuce
 - slovo + zbylá písmena abecedy \rightarrow snadné zapamatování a distribuce
- jednoduchost \rightarrow oblíbenost
 - distribuce klíčů bezproblémová (viz výše) a samotné šifrování a dešifrování také jednoduché (\times Vigenèrova šifra)

Bezpečnost monoalfabetické (polygramové) šifry

- praktická nemožnost prolomení algoritmu hrubou silou
 - vyzkouším 10^9 klíčů/s (rychlost PC v GHz) $\rightarrow 4 \times 10^{17}$ sec. \approx 12 miliard let
- snadno rozluštitelná pomocí **frekvenční analýzy**
- nejčastější písmeno v češtině “e”, dále “o” \rightarrow totéž v zašifrovaném textu
- bigramy: nejčtenější “st”, “te”, “ne”
- trigramy: nejčtenější “pro”, “ist”
- samohláska \rightarrow následuje více různých písmen (sohlásky);
sohláska \rightarrow následuje méně různých písmen (samohlásky).
- potřeba šifrovaného textu dostatečné délky (čím více, tím lépe)

\rightarrow použití **nedoporučeno**

Frekvenční analýza - ukázka¹

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

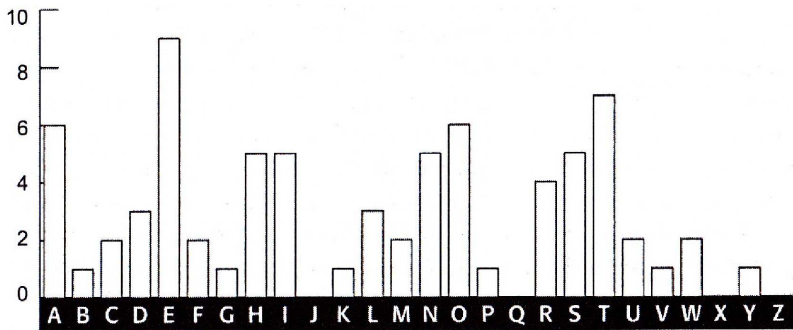
Historické šifry

Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje



¹pro angličtinu

Homofonní substituční šifra

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje

- z řeckého “homos” – stejný a “phonos” – zvuk
- (snadná) rozluštitelnost monoalfabetické šifry pomocí *frekvenční analýzy* → vylepšení kryptografického algoritmu → Homofonní substituční šifra
- písmeno - nahrazení řadou reprezentací
- počet \approx frekvenci výskytu písmene
- → četnost každého písmene v šifrovém textu přibližně stejná
- typ monoalfabetické šifry
 - 1. písmeno n reprezentací \times zpět vždy na jedno písmeno jedné abecedy

Výhody

- jednoduchost
- bezpečnost proti *základní* frekvenční analýze

Homofonní substituční šifra - příklad [1]

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje

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
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

Polyalfabetická substituční šifra

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje

- přidání dalších abeced pro šifrování
 - výběr klíče K pro volbu šifrovací abecedy
 - 1 volba šifrovací abecedy dle klíče K
 - 2 zašifrování daného písmene dle zvolené abecedy
 - 3 posun na další písmeno
 - 4 jít na krok (1)
- Příklad: Albertiho šifra, Vigenèrova šifra

Albertiho šifra

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Kráč, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje

- použití dvou šifrovacích abeced
- 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
- Q W E R T Z U I O P A S D F G H J K L Y X C V B N M
- Y A Q X S W C D E V F R B G T N H Z M J U K I L O P
- při šifrování se abecedy střídají
- hlavní výhoda: jedno písmeno plaintextu → dva různé znaky v zašifrovaném textu
- ztížení kryptoanalýzy (nemožnost použití jednoduché frekvenční analýzy)

Vigenèrova šifra

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje

- použití až 26 šifrových abeced
- základem šifrování se stal tzv. “Vigenèrův čtverec” zápis 26 šifrových abeced

	a	b	c	d	e	f	g	h	i	j	k	l	m	..
a	A	B	C	D	E	F	G	H	I	J	K	L	M	..
b	B	C	D	E	F	G	H	I	J	K	L	M	N	..
c	C	D	E	F	G	H	I	J	K	L	M	N	O	..
..

Šifrování

- klíč = např. slovo libovolné délky.
- (slovo délky jedna → Cézarovu šifra)
- delší klíč → bezpečnější šifra
- Pozn: nevolit slabé klíče, např. “aaaaa”
- dle písmen klíče volíme postupně šifrovací abecedy z Vigenèrova čtverce a zašifrováváme jimi otevřený text zprávy

Dešifrování

- opačným způsobem

Vigenèrova šifra - kryptoanalýza [1]

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje

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

Vigenèrova šifra - kryptoanalýza

Hledání klíče

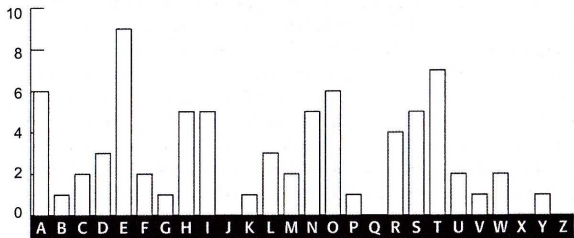
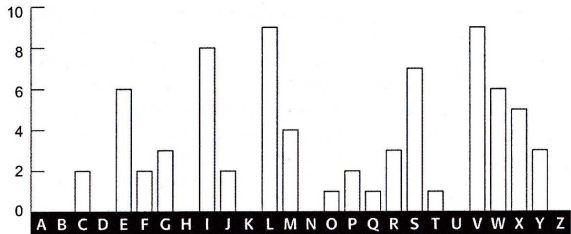
- hledání často se opakujících sekvencí
- délka sekvence > 4 písmena

Opakovaná sekvence	Interval mezi opakováním	Možná délka klíče																			
		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
E-F-I-Q	95				✓															✓	
P-S-D-L-P	5				✓																
W-C-X-Y-M	20	✓		✓	✓					✓										✓	
E-T-R-L	120	✓	✓	✓	✓	✓		✓		✓		✓			✓					✓	

- → pravděpodobně klíč délky 5
- → vzít písmeno č. 1, 6, 11, 16, ... - frekvenční analýza

Vigenèrova šifra - kryptoanalýza

Frekvenční analýza - abeceda č. 1

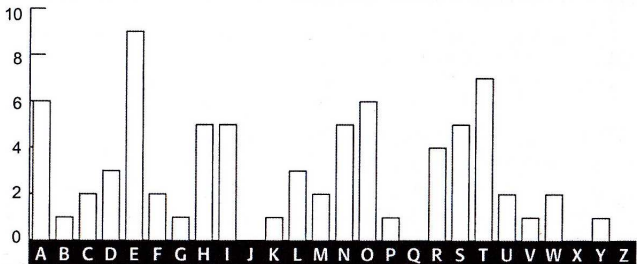
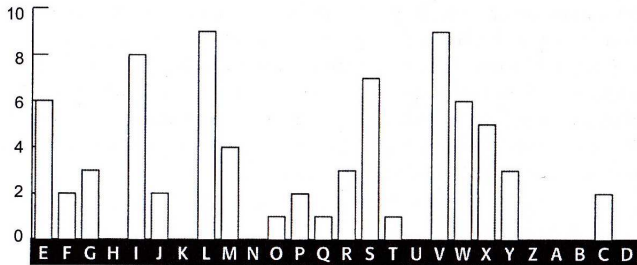


■ referenční abeceda dole

Vigenèrova šifra - kryptoanalýza

Frekvenční analýza - abeceda č. 1

- posun o 4. písmena vlevo (nahore) → 1. písmeno klíče = **E**



Vigenèrova šifra - kryptoanalýza

Frekvenční analýza - abeceda č. 2

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

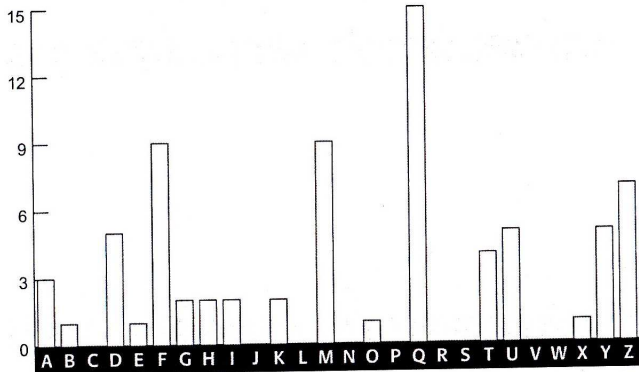
Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje

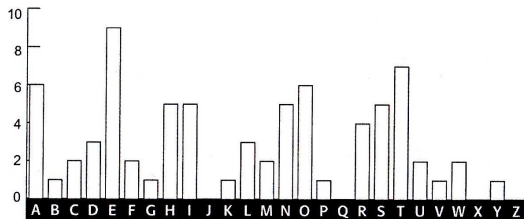
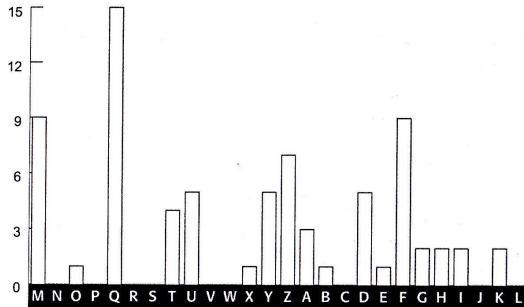
- největší frekvence → písmeno *E*
- nejméně frekventovaná *U – Z*



Vigenèrova šifra - kryptoanalýza

Frekvenční analýza - abeceda č. 2

■ posun o 12. písmen vlevo (nahore) → 2. písmeno klíče = M



Vigenèrova šifra - kryptoanalýza

Řešení

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ
Cézarova šifra

...

Šifrovací stroje

Sit thee down, and have no shame,
Cheek by jowl, and knee by knee:
What care I for any name?
What for order or degree?

Let me screw thee up a peg:
Let me loose thy tongue with wine:
Callest thou that thing a leg?
Which is thinnest? thine or mine?

Thou shalt not be saved by works:
Thou hast been a sinner too:
Ruined trunks on withered forks,
Empty scarecrows, I and you!

Fill the cup, and fill the can:
Have a rouse before the morn:
Every moment dies a man,
Every moment one is born.

Vylepšení substitučních šifer

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ
Cézarova šifra

...

Šifrovací stroje

- delší jednotka pro zakódování
 - znak → skupina znaků (bigramy, trigramy, ...)
 - + stejná písmena zašifrována v různých bigramech jinak → znemožnění jednoduché kryptoanalýzy
 - – zachována frekvence bigramů
- prodloužení klíče
 - Př. Vermanova šifra - délka klíče = délka zprávy
 - + nerozluštitelnost
 - – distribuce klíče
 - tzv. *jednorázový klíč*

Vermanova šifra

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

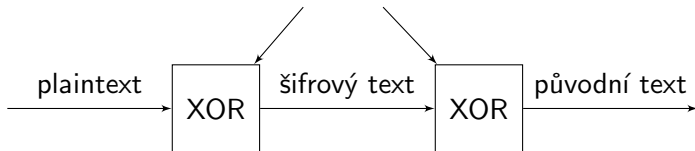
Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje

dlouhá *rand.* posloupnost (perioda = ∞)



Transpoziční šifry

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ
Cézarova šifra

...

Šifrovací stroje

- Princip = změna pořadí jednotlivých znaků textu (permutace) na základě daného algoritmu
- + jednoduchost – není obvykle třeba jakákoliv znalost matematiky.
- – relativně jednoduché dešifrování pomocí frekvenční analýzy (znaky zůstávají totožné, mění se jen jejich pořadí).

Realizace

- sloupcová transpozice
- šifrovací mřížka

Sloupcová transpozice

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje

Princip šifrování

- volba klíčového slova $K \rightarrow$ pořadí písmen (podle abecedy) určuje pořadí při šifrování
- přepsání šifrovaného textu do tabulky o počtu sloupců který je roven počtu písmen v klíčovém slově
- zašifrování dle klíče

Př:

- | | |
|-------------------------|--------|
| ■ text: co jsem napsal? | ■ cojs |
| ■ klic (=klíčové slovo) | ■ emna |
| ■ 3421 | ■ psal |
- \rightarrow (po čtveřicích) sjco anem laps \rightarrow (výsledek) sjcoanemlaps

Dešifrování

- rozdělit písmena do sloupců podle délky klíče
- seřadit dle pořadí v klíči (sjco - pořadí písmen 3421 \rightarrow cojs)

- obvykle papírová karta s proraženými otvory (okénky)
- přiložení mřížky na papír, zápis textu zprávy do okének (po písmenech, slabikách, slovech)
- doplnění textu na prázdné místo → přenášená zpráva je skryta v textu (=steganografie)
- dešifrování přiložením shodné mřížky

Otočná mřížka

- přiložení mřížky na papír a vyplnění všech okének
- otočení mřížky o 90° (návrh tak, aby po otočení bylo ve všech okénkách prázdné místo)
- postupné vystřídání 4 pozic
- počet znaků zprávy $> \#rows \times \#lines$ (mřížky) → rozdělení zprávy do více tabulek
- dešifrování přiložením shodné mřížky $4 \times$

Příklad otočné šifrovací mřížky

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

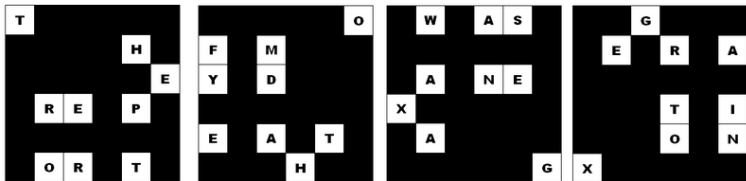
Historické šifry

Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje



T	W	G	A	S	O
F	E	M	R	H	A
Y	A	D	N	E	E
X	R	E	T	P	I
E	A	A	O	T	N
X	O	R	H	T	G

Příklad otočné šifrovací mřížky

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

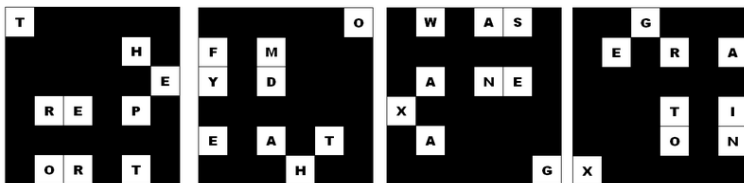
Historické šifry

Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje



T	W	G	A	S	O
F	E	M	R	H	A
Y	A	D	N	E	E
X	R	E	T	P	I
E	A	A	O	T	N
X	O	R	H	T	G

Řešení:

- The report of my death was an exaggeration x.

Šifra PLAYFAIR

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ
Cézarova šifra

...

Šifrovací stroje

- vznik: 1854 - vědec Charles Wheatstone
- účinné prosazování přítelem (baron Lyon Playfair) pro přijetí britskou vládou → název

Šifrování:

- 1 odstranění diakritiky a interpunkce, náhrada $J \rightarrow I$
 - 2 rozdělení písmen do párů
 - 3 zdvojená písmena → oddělení písmenem X nebo Z (střídat)
 - 4 lichý počet písmen → doplnění X nebo Z na konec
-
- 1 dvojice ve stejném řádku → šifruj písmenem vpravo (cyklicky)
 - 2 dvojice ve stejném sloupci → šifruj písmenem pod ($-||-$)
 - 3 neplatí (1) ani (2) →
 - $C = \text{průsečík řádek prvního} \times \text{sloupec druhého písmene dvojice}$
 - $C = \text{průsečík řádek druhého} \times \text{sloupec prvního písmene dvojice}$

Dešifrování: opačně

Šifra PLAYFAIR - příklad

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ
Cézarova šifra

...

Šifrovací stroje

Tabulka (klíč):

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

Šifra:

- OSFHED_FXGGNMPGMFMOENHTNCFIEMF

Text zprávy:

- ???

Šifra PLAYFAIR - příklad - řešení

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ
Cézarova šifra

...

Šifrovací stroje

Tabulka (klíč):

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

Šifra:

- OSFHED_FXGGNMPGMFMOENHTNCFIEMF

Text zprávy:

- BREAKING OF THE ENIGMA MACHINE

Šifrovací stroje

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

Šifra ATBAŠ

Cézarova šifra

...

Šifrovací stroje

- základem:
 - klávesnice
 - otočné rotory (na jedné ose)
 - elektromechanický princip
- nejznámější **Enigma** (německý vynálezce Arthur Scherbius)
- tři nebo čtyři rotory
- rotor kontakty na obou stranách, různé mapování

→ velký rozvoj šifrování



Enigma [2]

Bezpečnost v
informačních
technologiích
(KIV/BIT)

Ing. Pavel
Král, Ph.D.

Rozdělení šifer

Historické šifry

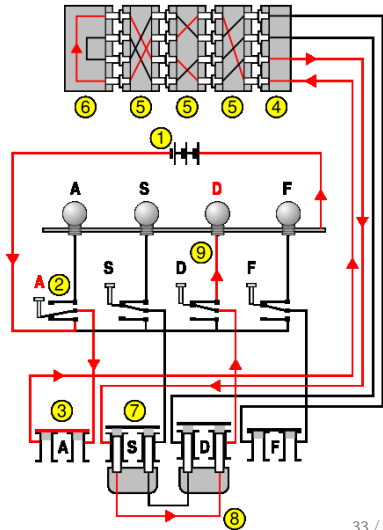
Šifra ATBAŠ
Cézarova šifra

...
Šifrovací stroje

- 1 baterie
- 2 klávesy
- 3 propojovací deska
- 4 rozvodové kolo
- 5 rotory (permutace)
- 6 deflektor
- 7 zástrčka
- 8 propojovací kabel
- 9 žárovka

■ **A → D**

- pro rozluštění potřeba známý otevřený text





Simon Singh,
Kniha kódů a šifer,
Dokořán a Argo, 2003.



Jak pracuje Enigma,
<http://enigma.eleferno.cz/index.php?text=13-jak-pracuje-enigma>,
2005.