Úvod do kryptografie

Milan Radojčić

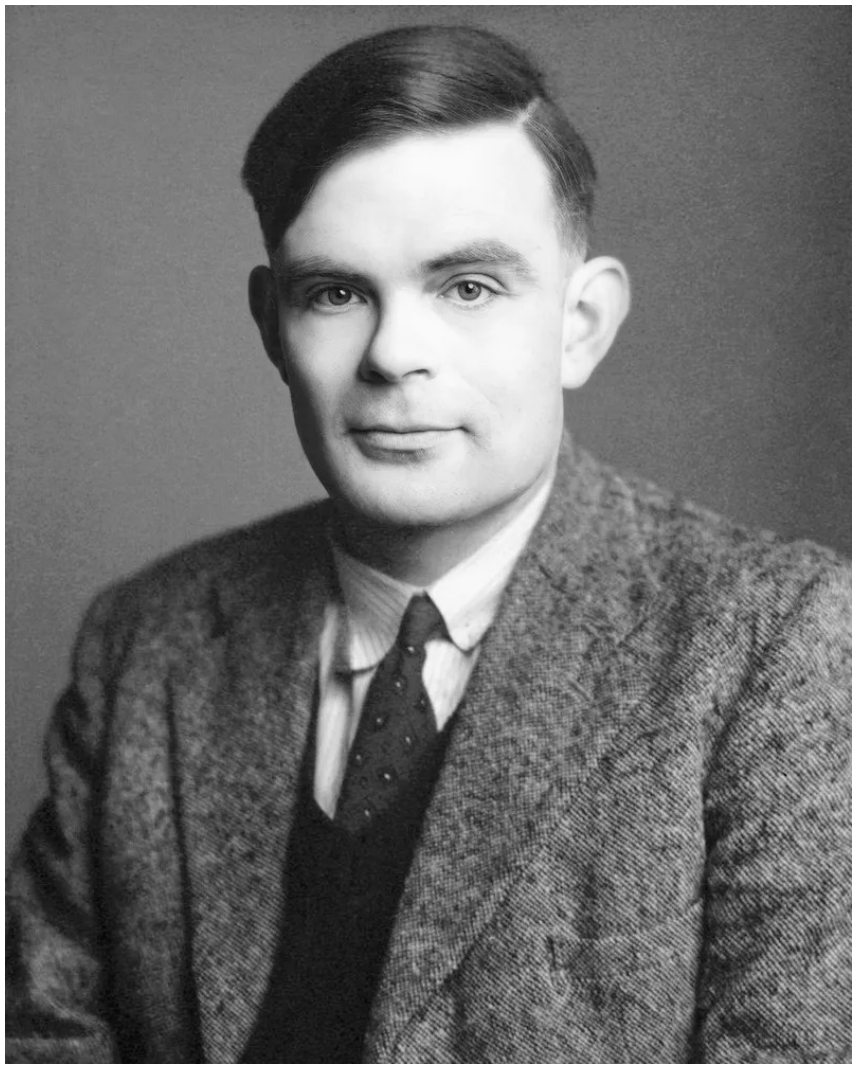
SSPŠaG – KBB

11. listopadu 2025

Hlavní body

Hlavní body


382nd PLATOON U.S.M.C. SAN DIEGO
1942
US MARINES — FIRST TO FIGHT




Klappe
schließen

Stručná historie kryptografie

- Nejstarší známý důkaz „kryptografie“ je z roku 1900 př. n. l. z Egypta.
- Velkou část doby klasické kryptografie jsou známy jen *monoalfabetické* šifry.
  - To změnil Leon Battista Alberti v 15. st.[1]
  - Jeho nápad dokončil Blaise Vigenère a po něm se šifra dnes jmenuje.
- Po celou dobu klasické kryptografie byly známy jen symetrické kryptosystémy.
  - Přelomové je období 70. let 20. století — vzniká Diffie-Hellman a RSA.

[1] Alberti byl příkladem renesančního člověka. Vystudoval práva a poté matematiku a fyziku. Ale dále maloval, skládal hudbu, psal knihy, věnoval se architektuře a prý byl skvělým atletem.

Hlavní body

Základní pojmy

- **Kryptologie/Kryptografie** – věda o utajování zpráv
  - **Kryptoanalýza** – nauka o prolamování šifer
- **Otevřený text/Plaintext (OT)** – text, který je určen k utajení
- **Šifrování** – proces, který převádí Otevřený text na Šifrový text
- **Šifrový text/Ciphertext (ŠT)** – text, ze kterého není zjistitelný OT (bez dalších znalostí)
- **Šifra** – konkrétní metoda, která převádí OT na ŠT
- **Šifrovací systém** – pomocí nějakého algoritmu převádí OT na ŠT

Dělení šifer

- *Historické metody*
  1. **Substituční**
  2. **Transpoziční**
  3. **Kódové knihy**
- *Podle vztahu klíčů*
  1. **Symetrické** – dešifrovací klíč *je odvoditelný* ze šifrovacího
  2. **Asymetrické** – dešifrovací klíč *není odvoditelný* ze šifrovacího

Hlavní body

Substituční šifry

- Substituční šifry provádí tzv. **konfúzi** — snaží se schovat závislost ŠT na OT pomocí *komplikovaného* vztahu s klíčem.
- Příkladem může být Césarova šifra nebo Vigenèrova šifra.
- Bude nás zajímat, jestli je daná šifra *monoalfabetická* nebo *polyalfabetická*.
  - **Monoalfabetická** – Písmena na různých pozicích se *šifrují vždy stejně*; používá *jen jednu* tabulku/„abecedu“ k šifrování.
  - **Polyalfabetická** – Písmena na různých pozicích se *můžou šifrovat různě*; používá *více* tabulek/„abeced“ k šifrování.

Substituční šifry

- Často budeme chtít pracovat s čísly místo textu. Bez újmy na obecnosti se omezíme na anglické texty, pro konvertování budeme používat tuto tabulku:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Césarova šifra

Césarovu šifru můžeme popsat vztahem:

$$c \equiv (p + k) \pmod{26},$$

kde p je plaintext, c je ciphertext a k je klíč.

Pro dešifrování platí

$$p \equiv (c - k) \pmod{26}.$$

- **Symetrická**
- **Monoalfabetická**

Ukázka Césarovy šifry

Začneme zprávou:

SECRET MESSAGE

Rozdělíme si ji do bloků o 5 písmenech. Poslední blok doplníme znakem Z aby se vešel do správné velikosti.

SECRE TMESS AGEZZ

Převedeme na čísla s pomocí tabulky:

18 4 2 17 4 19 12 4 18 18 0 6 4 25 25

Ukázka Césarovy šifry

18 4 2 17 4 19 12 4 18 18 0 6 4 25 25

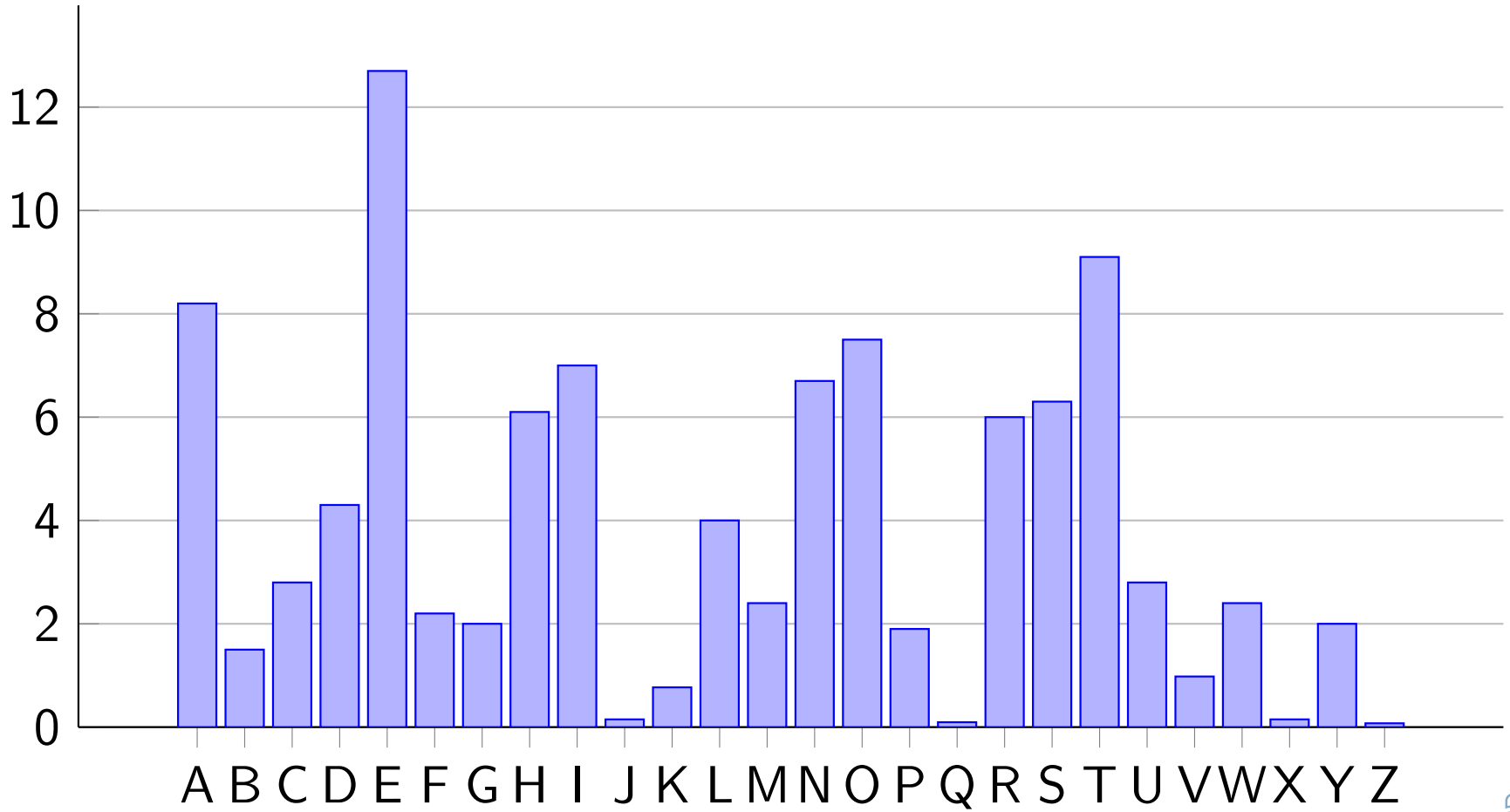
S použitím vztahu $c \equiv (p + k) \mod 26$ a klíče $k = 5$ získáme:

23 9 7 22 9 24 17 9 23 23 5 11 9 4 4

Po převodu zpět na písmena dostáváme:

XJHWJ YRJXX FLJEE

Frekvenční analýza



Četnost písmen v anglickém jazyce

Frekvenční analýza

- Při použití Césarovy se dvě stejná písmena na různých pozicích zašifrují vždy stejně.
- Můžeme analyzovat četnost písmen v šifrovém textu a porovnávat ji s průměrnou četností v normálním textu.
- Pokud třeba zjistíme, že nejčetnější písmeno v šifrovém textu je A a nejčetnější v průměrném anglickém textu je E tak můžeme zjistit klíč jako

$$\begin{aligned} \mathrm{A} &\equiv (\mathrm{E} + k) \mod 26 \\ 0 &\equiv (4 + k) \mod 26 \\ k &\equiv -4 \mod 26 \end{aligned}$$

- Museli jsme znát používaný kryptosystém.
- Museli jsme znát jazyk otevřeného textu.

Afinní šifra

Afinní šifra je dána transformací

$$c \equiv (a \cdot p + b) \pmod{26}.$$

Parametry a a b tvoří klíč.[2]

Pro dešifrování platí

$$p \equiv a^{-1} \cdot (c - b) \pmod{26}.$$

Z tohoto nám plyne podmínka $\gcd(a, 26) = 1$.

- **Symetrická**
- **Monoalfabetická**

[2] Pro $a = 1$ je afinní šifra stejná jako Césarova.

Frekvenční analýza

- Na afinní šifru lze také použít.
- Uvažujme zase případ, že E se zašifrovalo na B.

$$\begin{aligned} \mathrm{B} &\equiv a \cdot \mathrm{E} + b \mod 26 \\ 1 &\equiv a \cdot 4 + b \mod 26 \\ -b &\equiv 4a \mod 26 \end{aligned}$$

- Tato rovnice má více řešení!
- Narazili jsme na problém, jak ho vyřešíme?

Frekvenční analýza

- Máme v rovnici 2 neznámé, potřebujeme tedy alespoň **dvě dvojice písmen**.
- Zkusme tedy situaci, že E se zašifrovalo na B a T se zašifrovalo na C. Máme rovnice

$$\mathrm{B} \equiv a \cdot \mathrm{E} + b \mod 26$$

a

$$\mathrm{C} \equiv a \cdot \mathrm{T} + b \mod 26.$$

- Ty už mají jednoznačné řešení.

Hlavní body

Vigenèrova šifra

U **Vigenèrovy šifry** je klíčem text. Každé písmeno v OT pak zašifrujeme Césarovou šifrou, kde klíčem bude písmeno na stejné pozici v klíči. Pokud je klíč kratší než OT tak jej opakujeme.

„Matematicky“ můžeme zapsat

$$c_i = (p_i + k_i) \mod 26.$$

- **Symetrická**
- **Polyalfabetická!**

Ukázka Vigenèrovy šifry

Vezměme zase zprávu: SECRET MESSAGE a jako klíč vezmeme slovo ORANGE.

Klíč	O	R	A	N	G	E	O	R	A	N	G	E	O
OT	S	E	C	R	E	T	M	E	S	S	A	G	E
ŠT	G	V	C	E	K	X	A	V	S	F	G	K	S

Analýza Vigenèrovy šifry

- Vigenère je **polyalfabetická** šifra, takže FA nejde přímo použít.
- Co když ale známe délku klíče?
  - Když je délka n, tak se dá na šifru koukat jako na n-**krát Césarovu šifru!**

Analýza Vigenèrovy šifry

Pro délku klíče 3:

Klíč	A	B	C	A	B	C	A	B	C	A	B
OT	T	A	J	N	A	Z	P	R	A	V	A
ŠT	T	B	L	N	B	B	P	S	C	V	B

Analýza Vigenèrovy šifry

Pro plaintext s jediným písmenem:

Klíč	A	B	C	A	B	C	A	B	C	A	B
OT	D	D	D	D	D	D	D	D	D	D	D
ŠT	D	E	F	D	E	F	D	E	F	D	E

Analýza Vigenèrovy šifry

- Pokud známe délku klíče, tak lze použít stejný postup jako u Césarovy šifry.
- Pomoc chytré metody jde ale i *odhadnout délka klíče*.
- Tomuto celému postupu se říká **Kasiského test** (angl. *Kasiski examination*)
  - Objevená Babbagem v roce 1846.
  - Později nezávisle publikována Friedrichem Kasiskim v roce 1863.

Kasiského test

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

Šifrový text

Kasiského test

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

Opakování EFIQ

Kasiského test

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

Opakování PSDLP

Kasiského test

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

Opakování WCXYM

Kasiského test

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

Opakování ETRL

Kasiského test

Opakovaný text	Vzdálenost	Možné klíče
EFIQ	95	5, 19
PSDLP	5	5
WCXYM	20	2, 4, 5, 10, 20
ETRL	120	2, 3, 4, 5, 6, 8, 10, 12, 15, 20

- Jakou délku má nejpravděpodobněji klíč?

Kasiského test

Opakovaný text	Vzdálenost	Možné klíče
EFIQ	95	5, 19
PSDLP	5	5
WCXYM	20	2, 4, 5, 10, 20
ETRL	120	2, 3, 4, 5, 6, 8, 10, 12, 15, 20

- Klíč má nejpravděpodobněji délku 5.

Hlavní body

Transpoziční šifry

- Cílem transpozičních šifer je **difúze**, tj. rozptyl informace po celém ŠT.
- Nejjednodušším příkladem transpoziční šifry je **sloupcová transpozice**.

Sloupcová transpozice

Šifrový text si zapíšeme pod sebe do řádků o délce n znaků.[3] Poté text opíšeme po sloupcích.

OT: SECRET MESSAGE

S	E	C
R	E	T
M	E	S
S	A	G
E	Z	Z

$\longrightarrow$

S	R	M	S	E
E	E	E	A	Z
C	T	S	G	Z

ŠT: SRMSEEEEAZCTSGZ

Klíčem je naše číslo n — na kolik sloupců jsme text rozdělili.

[3] Zde musíme využít padding

Šifrování „na plot“ (rail fence)

Klíčem bude počet řádků, které budeme při šifrování používat. Text si vypíšeme do tabulky s tím, že budeme „skákat“ mezi řádky.

OT: SECRET MESSAGE

S				E				S				E
	E		R		T		E		S		G	
		C				M				A		

ŠT: SESEERTESGCMA