Kryptografické systémy a ich aplikácie

doc. RNDr. Jozef Jirásek, PhD.

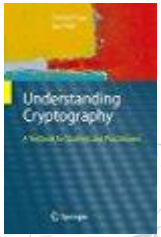
ZS 2023

Témy prednášok

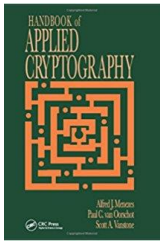
- úvod do kryptografie
- klasická kryptografia
- symetrická kryptografia
  - prúdové šifry
  - blokové šifry
- asymetrická kryptografia
- digitálny podpis
- silná autentifikácia
- správa kľúčov ...

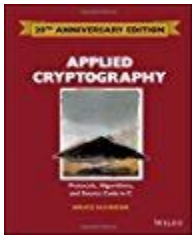
Organizácia semestra

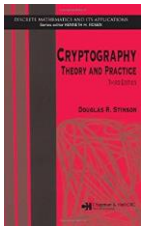
- prednášky v P11 v pondelok 15:20 – 17:50 (vrátane 15 min prestávky)
- úlohy k prednáškam – odovzdať do nasledujúcej prednášky v písomnej forme
- cvičenia v P4 vo štvrtok 11:40 – 13:10 riešenia zložitejších úloh a implementácia algoritmov z prednášok – práca v prostredí Jupyter Notebook s prípadným dokončením doma
- štúdium z literatúry – odporučená učebnica Ch. Paar, J. Pelzl: Understanding Cryptography, Springer-Verlag, 2010, ISBN 9783642041006 (prístupná v Intranete)

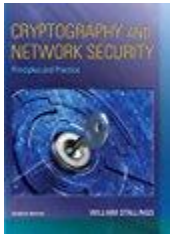


Ďalšia odporúčaná literatúra









- A. Menezes, P. van Oorschot, S. Vanstone: Handbook of Applied Cryptography, CRC Press, 2001 (free!)
- B. Schneier: Applied Cryptography. Protocols, Algorithms and Source Code in C, 2.ed., John Wiley & Sons, 1996 (v študovni)
- D. R. Stinson: Cryptography. Theory and Practie, 2.ed., CRC Press, 2002 (v študovni)
- W. Stallings: Cryptography and Network Security. Principles and Practice, 7.ed., Prentice-Hall, 2016

Hodnotenie

- 40 b – domáce zadania z prednášok
- 30 b – aktívna práca na cvičeniach
- 20 b – polsemestrálny test (1 termín)
- 50 b – záverečný test (3 termíny)

E – minimálne 70 b,
D – minimálne 80 b,
C – min. 90 b,
B – min. 100 b,
A – min. 110 b

Kryptológia

- grécky kryptós (κρυπτός) = ukrytý
  -logia (-λογία) = štúdium kryptológia
  graphein (γράφειν) = písanie kryptografia
  veda o utajovaní správ (komunikácie)
- kryptológia = kryptografia + kryptoanalýza
- kryptografia – štúdium algoritmov (protokolov) pre bezpečnú komunikáciu
- kryptoanalýza – vyhľadávanie bezpečnostných slabín v algoritmoch (protokoloch) a možností ich využitia pri získavaní utajených informácií

Využitie kryptografie

- utajenie prenosu informácie (dôvernosť komunikácie)

Využitie kryptografie

- utajenie prenosu informácie (dôvernosť komunikácie)
- zabezpečenie proti zmenám pri prenose (integrita správ)
- zabezpečenie proti výmene a podhodeniu nepravých správ (pôvodnosť správ)
- zabezpečenie proti maskovaniu sa odosielateľ za iného (nepopierateľnosť pôvodcu správy)
- obmedzenie zahltenia informačného zdroja (dostupnosť správ)
- iné nástroje na dosiahnutie komunikačnej bezpečnosti ...

Utajenie kódovaním

- kódovanie – kto pozná kód (algoritmus kódovania), ten vie správu prečítať

KRYPTOGRAFIA NA UPJS JE SUPER!

- 4b525950544f475241464941204e412055504a532 04a4520535550455221 - ASCII kódovanie
- UPJS的密碼學是偉大的！
- التشفير على أوبس هو عظيم!
- クリプトグラフィア・ナー・アップジズ・ジー・スーパー

Paleografia

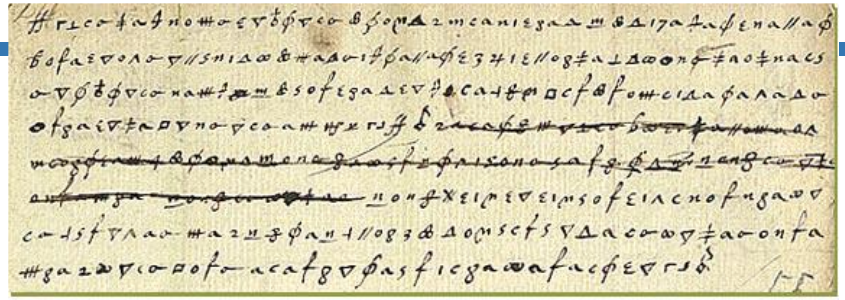
- Faistský disk z Kréty (17. storočie BC) – neznáme písmo ani význam (astronomický dokument, kalendárny záznam, hracia doska ?)

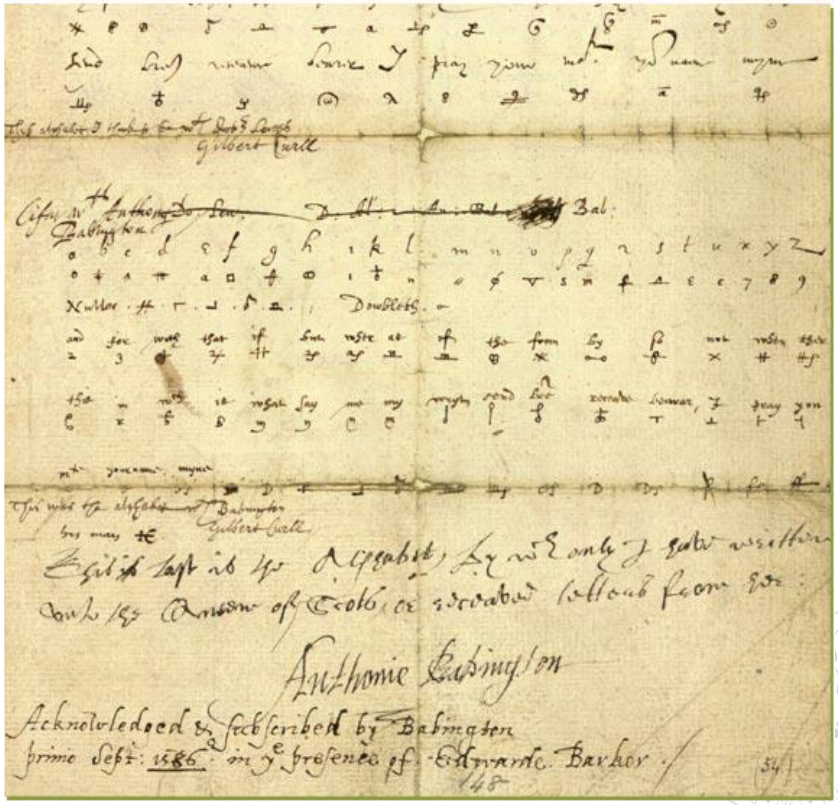
- nerozlúštené harappské písmo (26. až 20. storočie BC)

- zatiaľ nerozlúštené písmo Rongorongo z Veľkonočného ostrova

Kódové knihy

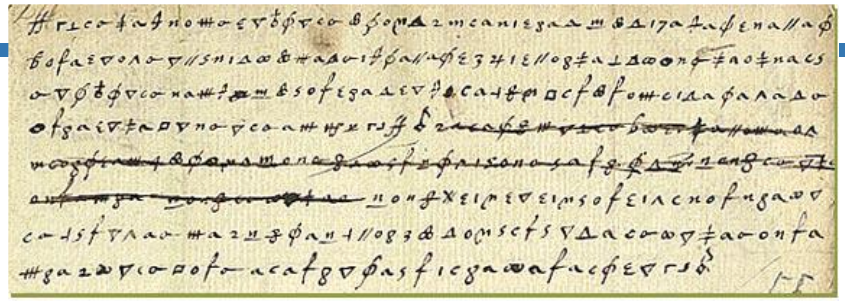
- Mária Stuartová – správy šifrované kódom (nomenklátorom) ju stáli život

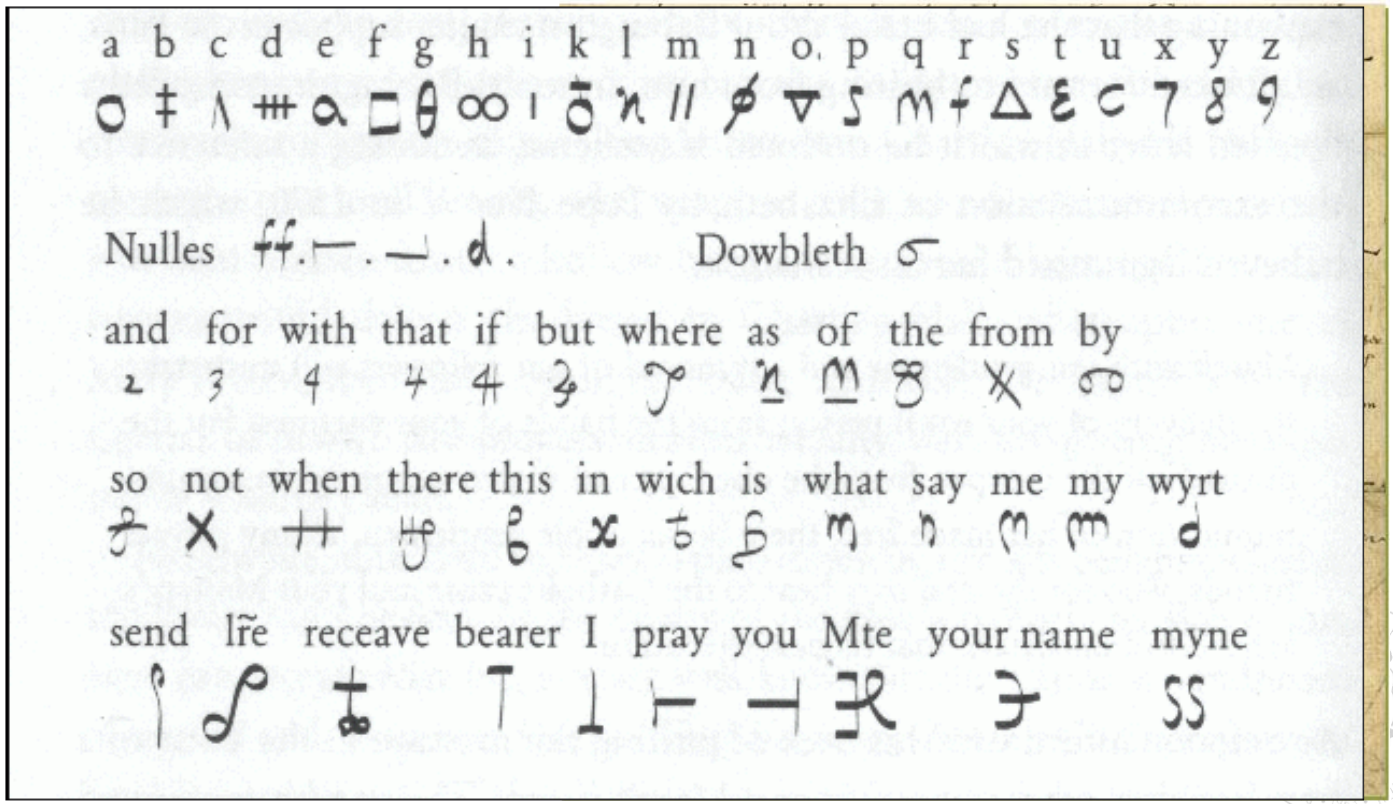




Kódové knihy

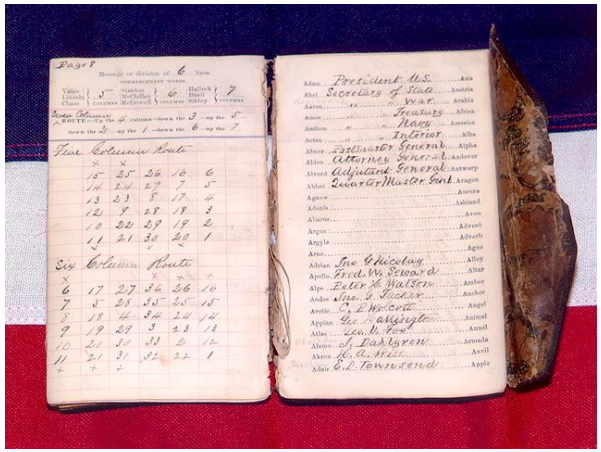
- nomenklátor



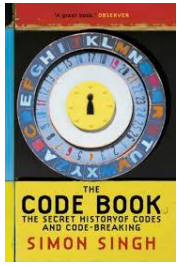


Kódovanie

- kódové knihy v 1. sv. vojne
- jazyk Navajo v 2. sv. vojne



Simon Singh: Kniha kódů a šifer (The Code Book)



Steganografia

ukrývanie správy v texte (inej správe)

- MKJEDKKJFMERMFJEDYJEPSEPJFKSTTJFKSTOFWSAS GMLKOPRJEDTSAMLKPOFYTDHFIJEQWIAMLDKENM LPQOADRTYLUDLPORPAQWLMJMLDKTSLKDPTJLKD PTELKDTSSDPEOTULDKTAPDRLGHETRSALRSELTM

Steganografia

- MKJEDKKJFMERMFJEDYJEPSEPJFKSTTJFKSTOFWSAS GMLKOPRJEDTSAMLKPOFYTDHFIJEQWIAMLDKENM LPQOADRTYLUDLPORPAQWLMJMLDKTSLKDPTJLKD PTELKDTSSDPEOTULDKTAPDRLGHETRSALRSELTM

- MKJED K KJFME R MFJED Y JEPSE P JFKST T JFKST O FWSAS G MLKOP R JEDTS A MLKPO F YTDHF I JEQWI A MLDKE N MLPQO A DRTYL U DLPOR P AQWLM J MLDKT S LKDPT J LKDPT E LKDTS S DPEOT U LDKTA P DRLGH E TRSAL R SELTM

Steganografia

- obrázok vľavo obsahuje pribalený text v ASCII kóde

Steganografia

- obrázok vľavo obsahuje pribalený text v ASCII kóde

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

000BE950  63 FD 51 59 0F C3 43 42 3D 7F C9 D2 C1 F1 02 72  cýQY.ÃCB=.ÉÒÁñ.r
000BE960  3F E2 BA C8 1E 44 A7 09 0A C4 26 8E AD 3C AD A1  ?âºÈ.D§..Ä&Ž.<.¡
000BE970  E2 65 B3 92 AB 2A A9 07 59 88 01 F5 F6 9B C3 1F  âe³'«*©.Y^.õö›Ã.
000BE980  4E FA 7E 20 2A 47 EC FF 00 37 EC EA A3 E2 27 CA  Nú~ *Gìÿ.7ìê£â'Ê
000BE990  BD 48 8E B2 57 9F C9 21 A7 49 9E F2 78 58 3B 14  ½HŽ²WŸÉ!§IžòxX;.
000BE9A0  82 76 09 0A 3B 5C 21 2A 16 E7 FD 7F 77 15 D2 A6  ‚v..;\!*.çý.w.Ò¦
000BE9B0  B5 AA 83 FB 7F CD D7 8F 52 69 6A 64 45 8E 9D A9  µªƒû.Í×.RijdEŽ.©
000BE9C0  A2 58 E3 6A 85 8E CF 19 67 99 E5 92 36 69 98 95  ¢Xãj…ŽÏ.g™å'6i˜•
000BE9D0  22 27 5F A2 8E 7D DD 55 E4 ED 6F 80 75 47 93 49  "'_¢Ž}ÝUäío€uG"I
000BE9E0  55 A1 24 9F F5 7C FA EE 17 8A 3A 69 E9 21 65 8A  U¡$Ÿõ|úî.Š:ié!eŠ
000BE9F0  6A 7A A8 D1 E0 8E 55 48 82 BB 4B 0B 2C 65 97 53  jz¨ÑàŽUH‚»K.,e—S
000BEA00  69 69 3E 80 9F A5 BD DA 60 3C 1F 09 32 69 D3 1E  ii>€Ÿ¥½Ú`<..2iÓ.
000BEA10  11 92 63 10 39 AF 13 FB 7F D5 FE 6E BF FF D9 4B  .'c.9¯.û.Õþn¿ÿÙK
000BEA20  52 59 50 54 4F 47 52 41 46 49 41 20 4E 41 20 55  RYPTOGRAFIA NA U
000BEA30  50 4A 53 20 4A 45 20 53 55 50 45 52              PJS JE SUPER
```

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

000BE950  63 FD 51 59 0F C3 43 42 3D 7F C9 D2 C1 F1 02 72  cýQY.ÃCB=.ÉÒÁñ.r
000BE960  3F E2 BA C8 1E 44 A7 09 0A C4 26 8E AD 3C AD A1  ?âºÈ.D§..Ä&Ž.<.¡
000BE970  E2 65 B3 92 AB 2A A9 07 59 88 01 F5 F6 9B C3 1F  âe³'«*©.Y^.õö›Ã.
000BE980  4E FA 7E 20 2A 47 EC FF 00 37 EC EA A3 E2 27 CA  Nú~ *Gìÿ.7ìê£â'Ê
000BE990  BD 48 8E B2 57 9F C9 21 A7 49 9E F2 78 58 3B 14  ½HŽ²WŸÉ!§IžòxX;.
000BE9A0  82 76 09 0A 3B 5C 21 2A 16 E7 FD 7F 77 15 D2 A6  ‚v..;\!*.çý.w.Ò¦
000BE9B0  B5 AA 83 FB 7F CD D7 8F 52 69 6A 64 45 8E 9D A9  µªƒû.Í×.RijdEŽ.©
000BE9C0  A2 58 E3 6A 85 8E CF 19 67 99 E5 92 36 69 98 95  ¢Xãj…ŽÏ.g™å'6i˜•
000BE9D0  22 27 5F A2 8E 7D DD 55 E4 ED 6F 80 75 47 93 49  "'_¢Ž}ÝUäío€uG"I
000BE9E0  55 A1 24 9F F5 7C FA EE 17 8A 3A 69 E9 21 65 8A  U¡$Ÿõ|úî.Š:ié!eŠ
000BE9F0  6A 7A A8 D1 E0 8E 55 48 82 BB 4B 0B 2C 65 97 53  jz¨ÑàŽUH‚»K.,e—S
000BEA00  69 69 3E 80 9F A5 BD DA 60 3C 1F 09 32 69 D3 1E  ii>€Ÿ¥½Ú`<..2iÓ.
000BEA10  11 92 63 10 39 AF 13 FB 7F D5 FE 6E BF FF D9     .'c.9¯.û.Õþn¿ÿÙ
```

Utajený text ?

H	O	V	M	Q	L	D	O	X	C	F	X		K	X		R	M	G	P		G	B		P	R	M	B	O	!

Utajený text ?

možné významy znakov

H	O	V	M	Q	L	D	O	X	C	F	X		K	X		R	M	G	P		G	B		P	R	M	B	O	!

								A			A			A															!

Caesarova šifra

posunutie v abecede o 3 znaky

H	O	V	M	Q	L	D	O	X	C	F	X		K	X		R	M	G	P		G	B		P	R	M	B	O	!

I	P	W	N	R	M	E	P	Y	D	G	Y		L	Y		S	N	H	Q		H	C		Q	S	N	C	P	!

J	Q	X	O	S	N	F	Q	Z	E	H	Z		M	Z		T	O	I	R		I	D		R	T	O	D	Q	!

K	R	Y	P	T	O	G	R	A	F	I	A		N	A		U	P	J	S		J	E		S	U	P	E	R	!

Posuvná šifra

- abecedný posun o k znakov abecedy
- k je tajomstvo medzi odosielateľom a prijímateľom správy
- 25 možných posunov ...

...	Y	Z	A	B	C	D	...
	⇩	⇩	⇩	⇩	⇩	⇩	
	A	B	C	D	E	F	

Monoalfabetická substitúcia

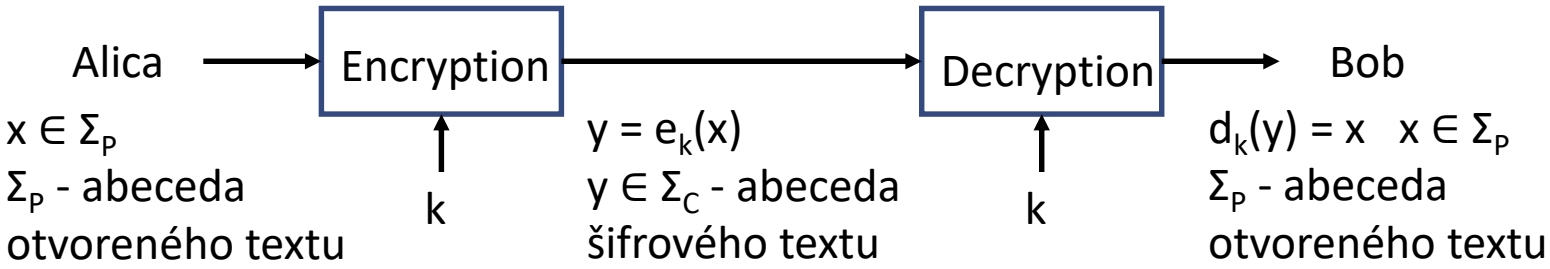
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	P	J	O	C	N	X	A	M	Z	Y	G	S	E	W	T	B	I	R	V	L	F	Q	H	U	K

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

- tajomstvom je zvolená permutácia abecedy
- permutácií je 26 ! = 403 291 461 126 605 635 584 000 000

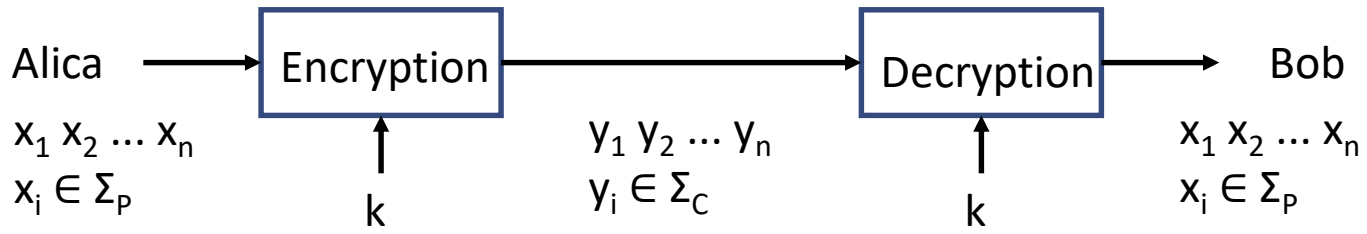
Klasické symetrické šifry

Formálny zápis šifrovania so zdieľaným tajomstvom



- Alica a Bob používajú zápis v abecede otvoreného textu Σ_P (napr. {a, b, ..., z}) a poznajú zdieľané tajomstvo k (secret key)
- šifrovaný text je zaznamenaný v abecede šifrového textu Σ_C (prakticky bývajú obidve abecedy rovnaké – napr. prirodzené čísla)
- šifrovacia funkcia (encryption) $e_k : \Sigma_P \to \Sigma_C$ priradí znaku z abecedy otvoreného textu znak z abecedy šifrového textu v závislosti od zdieľaného tajomstva k
- dešifrovacia funkcia (decryption) $d_k : \Sigma_C \to \Sigma_P$ priradí znaku z abecedy šifrového textu v závislosti od tajomstva k spätne znak z abecedy otvoreného textu
- rozšírime prirodzene toto pravidlo na reťazce znakov nad abecedou Σ_P ($\Sigma_P^* = \{ x_1 x_2 \dots x_n \mid x_i \in \Sigma_P \}$) resp. reťazce znakov nad abecedou Σ_C

Kryptografický systém (symetrický)



Kryptografický systém je pätica (P, C, K, E, D), kde

- P je konečná množina otvorených textov (*plain texts*) nad abecedou Σ_P $\quad P \subseteq \Sigma_P^*$
- C je konečná množina šifrových textov (*cipher texts*) nad abecedou Σ_C $\quad C \subseteq \Sigma_C^*$
- K je konečná množina kľúčov (*keys*)
- pre každé $k \in K$ existuje šifrovacia funkcia $e_k \in E$ a dešifrovacia funkcia $d_k \in D$ také, že pre každý otvorený text $x_1\ x_2 \dots x_n \in P$ platí $d_k(e_k(x_i)) = x_i \quad \forall i \in \{1, 2, \dots, n\}$

Posuvná šifra – formálny zápis

- textovú abecedu reprezentujme číslami 0, 1, ..., 25 (šifrovacie a dešifrovacie funkcie bude možné jednoduchšie zapísať)
- $\Sigma_P = \Sigma_C = K = \{0, 1, ..., 25\}$
- $\forall\, x \in \Sigma_P \;\; \forall\, k \in K \quad e_k(x) = (x + k) \bmod 26$
- $\forall\, y \in \Sigma_C \;\; \forall\, k \in K \quad d_k(y) = (y - k) \bmod 26$
- výpočty v aditívnej grupe $\mathbb{Z}_{26}$

Kryptoanalýza posuvnej šifry

- poznám množinu P
  (číselne zakódované texty v známom jazyku)
- nepoznám kľúč k

- vyskúšam 26 možností posunu šifrového textu
- postupne vylúčim nezmyselné interpretácie

- bezpečnosť ? ... veľkosť množiny kľúčov |K|
- čo ak nepoznám P ?

Monoalfabetická substitúcia

- $\Sigma_P = \Sigma_C = \{0, 1, \ldots, 25\}$
- $K = \{\pi : \Sigma_P \rightarrow \Sigma_C\}$ permutácie množiny $\{0, 1, \ldots, 25\}$
- $e_\pi(x) = \pi(x)$
- $d_\pi(y) = \pi^{-1}(y)$ π^{-1} je inverzná permutácia k π

$|K| = 26!$

Ako si zapamätať kľúč ?

Monoalfabetická substitúcia

- $\Sigma_P = \Sigma_C = \{0, 1, \ldots, 25\}$
- $K = \{\pi : \Sigma_P \rightarrow \Sigma_C\}$ permutácie množiny $\{0, 1, \ldots, 25\}$
- $e_\pi(x) = \pi(x)$
- $d_\pi(y) = \pi^{-1}(y)$ π^{-1} je inverzná permutácia k π

$|K| = 26!$

Ako si zapamätať kľúč ?

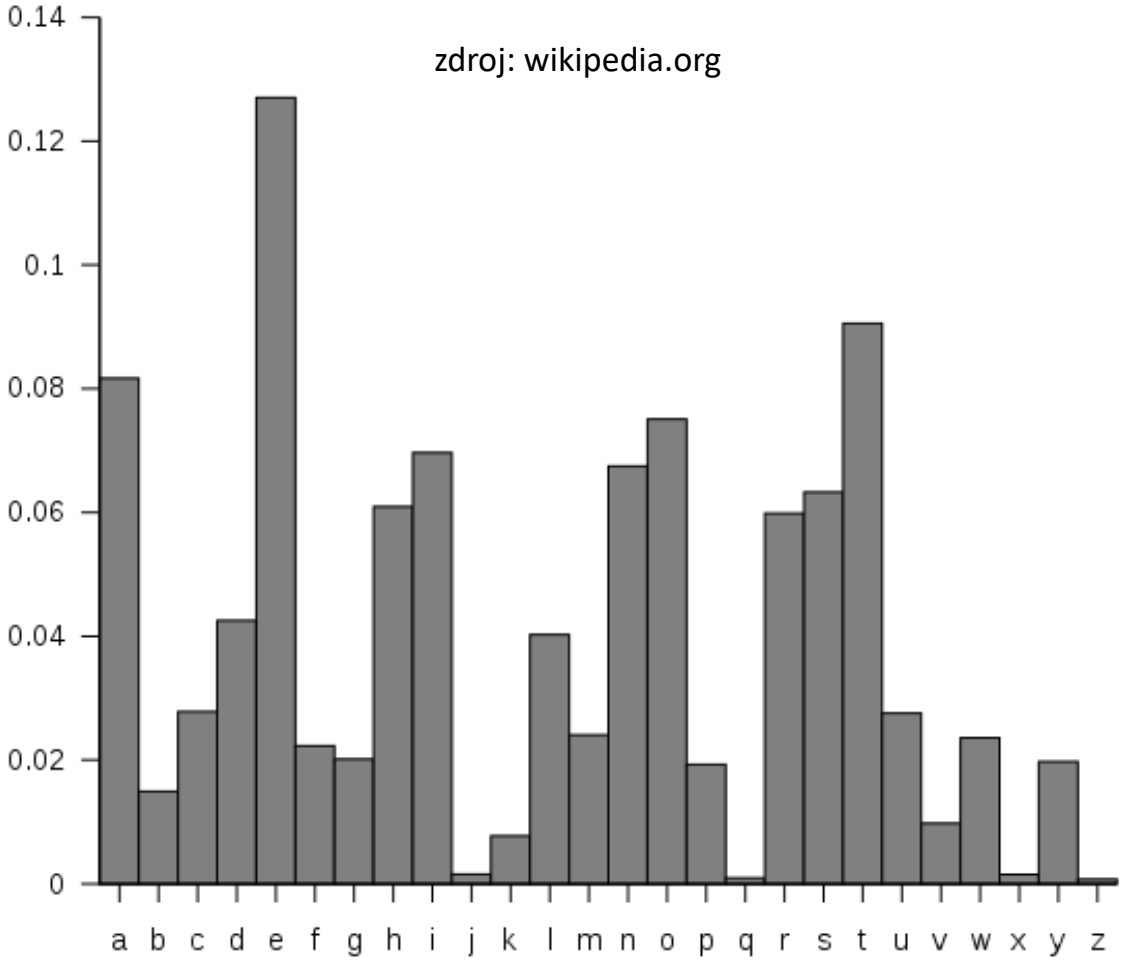
VELMIUTAJNYKCZXWSRQPOHGFDB

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Možnosti kryptoanalýzy monoalfabetickej substitúcie

- jazyk otvoreného textu
- medzery, predložky, spojky ...
- opakované sekvencie, známe časti textu (začiatok, koniec)
- frekvencia výskytu znakov → *frekvenčná analýza*

Frekvencia výskytov znakov v anglickom texte



Frekvenčná analýza - príklad

- Macbeth Act 1, Scene 1

OWLPVNLG MV RVWWO;
DR VQW RTCEV RQMSSCIR VADV OW JGMEX VWXCVACI
DEO JAWYC VACMI DIV. VAC SCIJMGCRR SDJOWEQDGO
QWIVAU VW PC D ICPCG NWI VW VADV
VAC SLGVMTGUMEX FMGGDEMCR WN EDVLIC
OW RQDIS LTWE AMS NIWS VAC QCRVCIE MRGCR
WN YCIER DEO XDGGWQXGDRRCR MR RLTTGMCO
DEO NWIVLEC WE AMR ODSECO BLDIICG RSMGMEX
RAWQO GMYC D ICPCGR QAWIC PLV DGG VWW QCDY
NWI PIDFC SDJPCVA QCGG AC OCRCIFCR VADV EDSC
OMRODMEMEX NWIVLEC QMVA AMR PIDEOMRAO RVCCG
QAMJA RSWYCO QMVA PGWWOU CHCJLVMWE
GMYC FDGWLIR SMEMWE JDIFCO WLV AMR TDRRDXC
VMGG AC NDJCO VAC RGDFC
QAMJA ECCI RAWWY ADEOR EWI PDOC NDICQCGG VW AMS
VMGG AC LERCDSO AMS NIWS VAC EDFC VW VAC JADTR
DEO NMHO AMR ACDO LTWE WLI PDVVGCSCEVR.

Frekvencia v texte		Frekvencia v AJ	
C	64	E	0.12702
V	44	T	0.09056
D	41	A	0.08167
W	41	O	0.07507
R	40	I	0.06966
A	37	N	0.06749
M	37	S	0.06327
G	34	H	0.06094
E	32	R	0.05987
I	30	D	0.04253
O	28	L	0.04025
S	19	C	0.02782
Q	16	U	0.02758
L	16	M	0.02406
N	12	W	0.02360
P	11	F	0.02228
J	11	G	0.02015
X	8	Y	0.01974
T	8	P	0.01929
Y	7	B	0.01492
F	7	V	0.00978
U	3	K	0.00772
H	2	J	0.00153
B	1	X	0.00150
		Q	0.00095
		Z	0.00074

E ↔ C
T ↔ V
A ↔ D
O ↔ W
I ↔ R ?

Frekvenčná analýza príklad

- Macbeth Act 1, Scene 1
- krátke slová
  - VAC -> THE
  - VW -> TO
- využijeme vlastnosti textu
  (nie vždy musia frekvencie
  v texte odpovedať frekvenciám AJ)
- šifrovacia permutácia:

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

Frekvencia v texte	
C	64
V	44
D	41
W	41
R	40
A	37
M	37
G	34
E	32
I	30
O	28
S	19
Q	16
L	16
N	12
P	11
J	11
X	8
T	8
Y	7
F	7
U	3
H	2
B	1

Frekvencia v AJ	
E	0.12702
T	0.09056
A	0.08167
O	0.07507
I	0.06966
N	0.06749
S	0.06327
H	0.06094
R	0.05987
D	0.04253
L	0.04025
C	0.02782
U	0.02758
M	0.02406
W	0.02360
F	0.02228
G	0.02015
Y	0.01974
P	0.01929
B	0.01492
V	0.00978
K	0.00772
J	0.00153
X	0.00150
Q	0.00095
Z	0.00074

E	↔	C
T	↔	V
A	↔	D
O	↔	W
I	↔	M

Príklad substitučnej šifry bez medzier

OWLPVNLG MV RVWWO;
DR VQW RTCEV RQMSSCIR VADV OW JGMEX VWXCVACI
DEO JAWYC VACMI DIV. VAC SCIJMGCRR SDJOWEQDGO
QWIVAU VW PC D ICPCG NWI VW VADV
VAC SLGVMTGUMEX FMGGDEMCR WN EDVLIC
OW RQDIS LTWE AMS NIWS VAC QCRVCIE MRGCR
WN YCIER DEO XDGGWQXGDRRCR MR RLTTGMCO
DEO NWIVLEC WE AMR ODSECO BLDIICG RSMGMEX
RAWQO GMYC D ICPCGR QAWIC PLV DGG VWW QCDY
NWI PIDFC SDJPCVA QCGG AC OCRCIFCR VADV EDSC
OMRODMEMEX NWIVLEC QMVA AMR PIDEOMRAO RVCCG
QAMJA RSWYCO QMVA PGWWOU CHCJLVMWE
GMYC FDGWLIR SMEMWE JDIFCO WLV AMR TDRRDXC
VMGG AC NDJCO VAC RGDFC
QAMJA ECCI RAWWY ADEOR EWI PDOC NDICQCGG VW AMS
VMGG AC LERCDSO AMS NIWS VAC EDFC VW VAC JADTR
DEO NMHO AMR ACDO LTWE WLI PDVVGCSCEVR.

```
OWLPV NLGMV RVWWO DRVQW RTCEV RQMSS
CIRVA DVOWJ GMEXV WXCVA CIDEO JAWYC
VACMI DIVVA CSCIJ MGCRR SDJOW EQDGO
QWIVA UVWPC DICPC GNWIV WVADV VACSL
GVMTG UMEXF MGGDE MCRWN EDVLI COWRQ
DISLT WEAMS NIWSV ACQCR VCIEM RGCRW
NYCIE RDEOX DGGWQ XGDRR CRMRR LTTGM
CODEO NWIVL ECWEA MRODS ECOBL DIICG
RSMGM EXRAW QOGMY CDICP CGRQA WICPL
VDGGV WWQCD YNWIP IDFCS DJPCV AQCGG
ACOCR CIFCR VADVE DSCOM RODME MEXNW
IVLEC QMVAA MRPID EOMRA ORVCC GQAMJ
ARSWY COQMV APGWW OUCHC JLVMW EGMYC
FDGWL IRSME MWEJD IFCOW LVAMR TDRRD
XCVMG GACND JCOVA CRGDF CQAMJ AECCI
RAWWY ADEOR EWIPD OCNDI CQCGG VWAMS
VMGGA CLERC DSOAM SNIWS VACED FCVWV
ACJAD TRDEO NMHOA MRACD OLTWE WLIPD
VVGCS CEVRX
```

Auguste Kerckhoffs (1883)

- Kryptografický systém je bezpečný, ak útočník nie je schopný dešifrovať text ani vtedy, keď dokonale pozná postup šifrovania

Dôvernosť komunikácie je zabezpečená len znalosťou kľúča

Kryptoanalýza hrubou silou (brute-force)

- veľkosť množiny kľúčov |K| a množín |P| a |C|
  čas na testovanie kľúča vs. cena prostriedkov na realizáciu analýzy

Možnosti kryptoanalýzy

- poznám len šifrovaný text, algoritmus šifrovania a charakteristiku otvoreného textu - COA – *ciphertext only attack*
- poznám aspoň jednu dvojicu otvoreného a šifrovaného textu KPA – *known-plaintext attack*
- môžem si nechať niečo zašifrovať CPA – *chosen-plaintext attack*
- môžem si nechať niečo dešifrovať CCA – *chosen-ciphertext attack*
- adaptívne varianty CPA a CCA

Ďalšie možnosti kryptoanalytických útokov

- postranné kanály (*side channels attack*)
- chyby v implementácii
- malware, spyware, ransomware …
- sociálne inžinierstvo, phishing …
- korupčná kryptoanalýza
- pendreková (*rubber-hose*) kryptoanalýza

Eliminácia útokov pomocou frekvenčnej analýzy

- homofónne šifry – monoalfabetické substitúcie, kde sa priradí frekventovaným znakom otvoreného textu náhodne jeden z viacerých znakov šifrovaného textu (napr. $e(E) \in \{X,Y\}$; $e(I) = e(J) = Z$; a pri dešifrovaní sa I a J rozlíši podľa kontextu)
- bigramové šifry – substitúcia po dvojiciach znakov (pri veľmi dlhom texte by mohla kryptoanalýze pomôcť frekvenčná analýza bigramov)
- polygramové a polyalfabetické šifry

Afinný kryptosystém

- $\Sigma_P = \Sigma_C = \{0, 1, \ldots, 25\}$
- K = { (a, b) | $a \in \{1,3,5,7,9,11,15,17,19,21,23,25\}$, $b \in \{0, 1, \ldots, 25\}$ }
- $e_k(x) = (ax + b) \bmod 26$
- $d_k(y) = \left(a'(y - b)\right) \bmod 26$

  kde a' je inverzný prvok k a teda $(a' . a) \bmod 26 = 1$
  to existuje práve vtedy, keď $\gcd(a, 26) = 1$

- 26 x 26 možností ?? - len 26 x 12 = 312

Playfair

- je bigramová šifra (Ch. Wheatstone 1854)
- https://en.wikipedia.org/wiki/Playfair_cipher
- frekvencia najčastejších bigramov v AJ

th 1.52	en 0.55	ng 0.18
he 1.28	ed 0.53	of 0.16
in 0.94	to 0.52	al 0.09
er 0.94	it 0.50	de 0.09
an 0.82	ou 0.50	se 0.08
re 0.68	ea 0.47	le 0.08
nd 0.63	hi 0.46	sa 0.06
at 0.59	is 0.46	si 0.05
on 0.57	or 0.43	ar 0.04
nt 0.56	ti 0.34	ve 0.04
ha 0.56	as 0.33	ra 0.04
es 0.56	te 0.27	ld 0.02
st 0.55	et 0.19	ur 0.02

Hillova šifra

- Lester Hill (1929) – polygramová šifra (m-prvkové vektory kódov znakov, násobenie maticami)

- $\Sigma_P = \Sigma_C = \{ \boldsymbol{x} = \langle x_1\ x_2\ \ldots\ x_m \rangle\ ;\ x_i \in \{0, 1, \ldots, 25\} \}$
- K = { m x m matica s prvkami $\in \mathbb{Z}_{26}$ *invertibilná* }
  (pre $\boldsymbol{k} \in$ K existuje $\boldsymbol{k}^{-1}$, že $(\boldsymbol{k}^{-1}\boldsymbol{k}) \bmod 26 = \mathbf{I}$)
- $e_k(\boldsymbol{x}) = (\boldsymbol{k}\boldsymbol{x}) \bmod 26$
- $d_k(\boldsymbol{y}) = \boldsymbol{k}^{-1}(\boldsymbol{k}\boldsymbol{x}) \bmod 26 = (\boldsymbol{k}^{-1}\boldsymbol{k})\boldsymbol{x} \bmod 26 = \boldsymbol{x}$

Hillova bigramová šifra

pre matice 2 x 2

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (\mathrm{ad} - \mathrm{bc})^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

príklad

$k = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$ HELP $\begin{pmatrix} H \\ E \end{pmatrix}, \begin{pmatrix} L \\ P \end{pmatrix}$ $p = \begin{pmatrix} 7 \\ 4 \end{pmatrix}, \begin{pmatrix} 11 \\ 15 \end{pmatrix}$

$e_k(p) = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 8 \end{pmatrix} \ (mod\ 26)$, $\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 11 \\ 15 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 19 \end{pmatrix} \ (mod\ 26)$

$c = \begin{pmatrix} 7 \\ 8 \end{pmatrix}, \begin{pmatrix} 0 \\ 19 \end{pmatrix}$ $\begin{pmatrix} H \\ I \end{pmatrix}, \begin{pmatrix} A \\ T \end{pmatrix}$ HIAT

$d_k(e_k(p)) = 9^{-1} \begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix} \begin{pmatrix} 7 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 7 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 4 \end{pmatrix} \ (mod\ 26) \quad \ldots \begin{pmatrix} H \\ E \end{pmatrix}$

$\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 15 \end{pmatrix} \ (mod\ 26) \ldots \begin{pmatrix} L \\ P \end{pmatrix}$

Ďakujem za pozornosť.

jozef.jirasek@upjs.sk