Informatika – Ochrana dat

Radim Farana

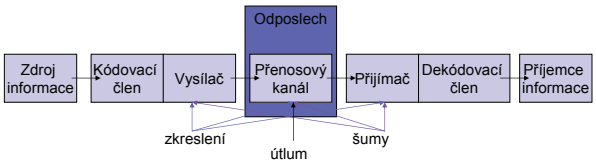
Podklady předmětu Informatika
pro akademický rok 2007/2008

Obsah

- Kryptologie.
- Kryptografické systémy,
  - klasifikace systémů,
  - bezpečnost systémů.
- Systémy s tajným klíčem,
  - transpoziční systémy,
  - transkripční systémy.

Kryptologie

- Kryptografie - tvorba kryptografických systémů
- Kryptoanalýza - narušování kryptografických systémů



Kryptografické systémy

- Tajný inkoust, tajný kanál, utajený přenos (Steganografie)
- Transpoziční systémy (skytala, …, šifrovací mřížka)
- Transkripční systémy (homofonní šifra, …, DES, AES)
  - S tajným klíčem
  - S veřejným klíčem

Utajený přenos

Sir Francis Bacon

* 22. 1. 1561 London
+ 9. 4. 1626
http://bacon.thefreelibrary.com/

Mi*l*ý p*ř*íte*l*i, d*o*r*u*č*i*te*l* t*o*hoto d*o*pi*s*u
je *m*i zvlášť milý.

11001 00000 10101 01001 01000 00111
01110 11111 11111 1

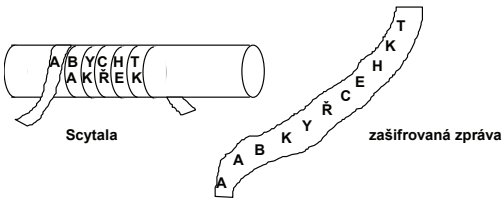
Příklad přiřazení znaků Baconovy šifry :

a	00000	b	00001	c	00010	d	00011
e	00100	f	00101	g	00110	h	00111
i	01000	j	01001	k	01010	l	01011
m	01100	n	01101	o	01110	p	01111
q	10000	r	10001	s	10010	t	10011
u	10100	v	10101	w	10110	x	10111
y	11000	z	11001.				

Celkem takto lze vyjádřit $2^5 = 32$ různé znaky.

Transpoziční systémy

Scytale (Skytalé, Skytala)



Jednoduchá transpozice

heslo	**Z**	**L**	**A**	**T**	**A**	**B**	**R**	**A**	**N**	**A**
pořadí	**10**	**6**	**1**	**9**	**2**	**5**	**8**	**3**	**7**	**4**
otevřená zpráva	K	L	O	K	A	N	P	R	I	L
	E	T	I	V	P	R	O	S	I	N
	C	I	X	X	X	X	X	X	X	X

Šifrovaná zpráva se obvykle rozděluje do pětipísmenných skupin a zní :
OARLN LIPKK IPSNR TIRVE XXXXX IXXXC

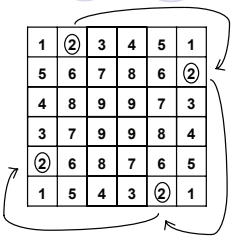
Šifra Porta

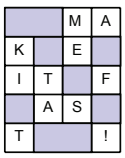
heslo	**Z**	**L**	**A**	**T**	**A**	**B**	**R**	**A**	**N**	**A**
pořadí	**10**	**6**	**1**	**9**	**2**	**5**	**8**	**3**	**7**	**4**
otevřená zpráva	K	L	O	K	A	N	P	R	I	L
	E	T	I	V	P	R	O	S	I	N
	C	I								

Šifrovaný text zní :
OIAPR SLNNR LTIII POKVK EC

italský fyzik Gian Babtista della Porta (1563)

Šifrovací mřížka





Fleissnerova otočná mřížka

Hieronimo Cardano

* 24. 9. 1501 Pavia
+ 21. 9. 1576 Rome
http://www-groups.dcs.st-and.ac.uk/~history/PictDisplay/Cardan.html

mřížka 4 x 4 dává 4^4 = 256 možností,
mřížka 6 x 6 dává 4^9 = 262 144 možností,
mřížka 8 x 8 dává 4^{16} = 4 294 967 296 možností,
mřížka 10 x 10 dává 4^{25} = 1 125 899 906 843 000 možností.

Transkripční systémy

- Cézarovské šifry

Gaius Julius Caesar

* 12. 7. 100 BC ? Rome
+ 15. 3. 44 BC Rome
http://en.wikipedia.org/wiki/Julius_Caesar

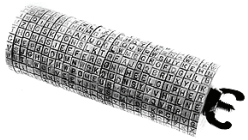
$C_k: Z_N \rightarrow Z_N$, $C_k(n)$ $(n + k) \bmod N$,

kde je n - znak původní zprávy,
$C_k(n)$ - znak šifrované zprávy,
k - klíč šifry, posunutí v abecedě,
N - počet znaků abecedy.

Monoalfabetická šifra obecná

26! = 403 291 461 126 605 635 584 000 000.

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

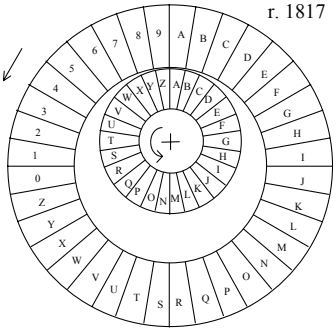


Jeffersonův válec

A B C D E F G ....znaky původní zprávy
↓ ↓ ↓ ↓ ↓ ↓ ↓ ...
D A S O F T B ...znaky šifrované zprávy

Nestejné kotouče

r. 1817



Decius Wadsworth
1768-1821

Charles Wheatstone, Sir
1802-1875

Vigenérovské šifry

použití množiny Cézarovských šifer

Např pomocí hesla: **AHOJ** šifrujeme text:
NEMOHU PRIJIT následovně

N + A mod 26 = N	P + O mod 26 = D
E + H mod 26 = L	R + J mod 26 = A
M + O mod 26 =A	I + A mod 26 = I
O + J mod 26 =X	J + H mod 26 = Q
H + A mod 26 = H	I + O mod 26 = W
U + H mod 26 = B	T + J mod 26 = C

A dostáváme šifrovanou zprávu:
NLAXHB DAIQWC

Blaise de Vigenère

+ 5. 4. 1523 – 1596

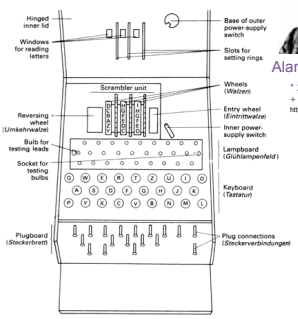
http://fr.wikipedia.org/wiki/Blaise_de_Vigenere

1586 kniha o šifrování
Autor systému:
Giovanni Battista Bellaso

Vigenérův čtverec

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

Šifrovací stroj ENIGMA



Alan Mathison Turing

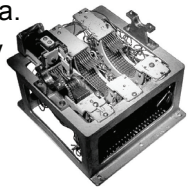
* 23. 6. 1912. London
+ 7. 6. 1954 Wilmslow
http://ei.cs.vt.edu/~history/Turing.html

Japonský „purpurový kód“

William Frederick Friedman

* 24. 9. 1891 Kishinev
+ 12. 12. 1969
http://en.wikipedia.org/wiki/William_F._Friedman

- Uveden do provozu 1939.
- Stroj nepoužívá rotory, ale krokové voliče jako automatické telefonní ústředny.
- Na konci roku 1940 prolomena.
- Zpráva o vypovězení smlouvy s USA byla rozluštěna jen několik hodin před útokem na Pearl Harbor.



Nekonečný klíč

Klíčová kniha - určení slova pro heslem míchanou abecedu

1 2 0 8 9, kde je:
12 - strana v knize,
08 - řádek na stránce,
9 - pozice slova na řádku.

Dokumentarfilme

Krok 1:

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

Krok 2:

2 7 4 0 5 3 6 9 1 8
D O K U M E N T A R
B C F G H I J L P Q
S V W X Y Z .

Očíslování podle pořadí v abecedě

- část 2

Krok 3:

2 7 4 0 5 3 6 9 1 8
4 D O K U M E N T A R
6 B C F G H I J L P Q
1 S V W X Y Z .

Očíslování řádků (např. ze sloupce 3, 7, 9)

Krok 4:

A B C D E F G H I J
14 26 76 24 34 46 06 56 36 66
K L M N O P Q R S T
44 96 54 64 74 16 86 84 21 94
U V W X Y Z .
04 71 41 01 51 31 61

Písmena zakódována číslem sloupce a řádku

- část 3

Oznámení: "Die Leibstandarte Adolf Hitler ist in Warschau eingetroffen." ("Tělesná standarta Adolfa Hitlera dorazila do Varšavy.")
Pro radiodepeši text zkrátíme a zakódujeme do čísel dle 4.

Krok 5: H I T L E R S T A N D A R T E
56 36 94 96 34 84 21 94 14 64 24 14 84 94 34
I N W A R S C H A U
36 64 41 14 84 21 76 56 14 04

Získaná čísla seřadíme do pětimístných skupin.

Krok 6: 56369 49634 84219 41464 24148
49434 36644 11484 21765 61404

- část 4

Krok 7:

A	B	C	D	E	F	G	H	I	J
1	**2**	**7**	**2**	**3**	**4**	**0**	**5**	**3**	**6**
K	L	M	N	O	P	Q	R	S	T
4	**9**	**5**	**6**	**7**	**1**	**8**	**8**	**2**	**9**
U	V	W	X	Y	Z	.			
0	**7**	**4**	**0**	**5**	**3**	**6**			

Písmena převedeme na čísla (sloupců)

Zakódujeme klíčový text

Krok 8:

D	O	K	U	M	E	N	T	A	R	F	I	L	M	E
2	**7**	**4**	**0**	**5**	**3**	**6**	**9**	**1**	**8**	**4**	**3**	**9**	**5**	**3**
S	I	N	D	B	E	L	E	G	T	W	E	R	D	E	N
2	**3**	**6**	**2**	**2**	**3**	**9**	**3**	**0**	**9**	**4**	**3**	**8**	**2**	**3**	**6**
A	B	E	R	R	A	S	C	H	W	I	E	D	E	R	F	R	E	I
1	**2**	**3**	**8**	**8**	**1**	**2**	**7**	**5**	**4**	**3**	**3**	**2**	**3**	**8**	**4**	**8**	**3**	**3**

- část 5

Sečteme (modulo 10) zprávu a pomocný text

zpráva z kroku 6:	56369	49634	84219	41464	24148
zpráva z kroku 8:	27405	36918	43953	23622	39309
znění telegramu	**73764**	**75542**	**27162**	**64086**	**53447**
zpráva z kroku 6:	49434	36644	11484	21765	61404
zpráva z kroku 8:	43823	61238	81275	43323	84833
znění telegramu	**82257**	**97872**	**92659**	**64088**	**45237**

Na dohodnuté místo vložíme skupinu označující heslo **12089**

Proudová šifra

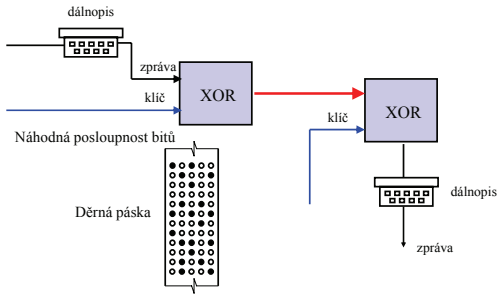
Mezinárodní telegrafní abeceda CCITT-2

CCITT	znak	kód	CCITT	znak	kód
1	A _	11000	17	Q 1	11101
2	B ?	10011	18	R 4	01010
3	C :	01110	19	S !	10100
4	D vz	10010	20	T 5	00001
5	E 3	10000	21	U 7	11100
6	F	10110	22	V =	01111
7	G	01011	23	W 2	11001
8	H	00101	24	X /	10111
9	I 8	01100	25	Y 6	10101
10	J zv	11010	26	Z +	10001
11	K (	11110	27	návrat válce	00010
12	L)	01001	28	posun řádku	01000
13	M .	00111	29	číslicová změna	11011
14	N ,	00110	30	písmenová změna	11111
15	O 9	00011	31	mezera	00100
16	P 0	01101	32		00000

Vernamův systém

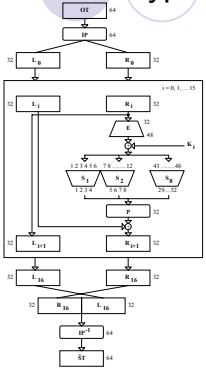
Gilbert Sandford Vernam
1890-1960

- Prokazatelně nerozluštitelný systém

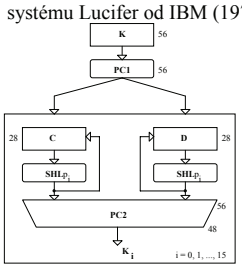


Data Encryption Standard

Horst Feistel
* 30. 1. 1915 Berlin
+ 14. 11. 1990



patentován 24. 2. 1975 na základě systému Lucifer od IBM (1970)



Advanced Encryption Standard

Joan Daemen

* 1965 Achel, Limburg, Belgie

Vincent Rijmen

* 16. 101970 Leuven, Belgie

http://en.wikipedia.org/wiki/Vincent_Rijmen

- **Veřejná soutěž vyhlášena**: 2. 1. 1997
- **Vyhlašovatel**: National Institute of Standards and Technology (NIST - http://www.nist.gov/)
- **Soutěž ukončena**: 2. 10. 2000
- **Vítěz**: Rijndael (čti: rájndol), Belgie.
- **Platnost**: předpokládá se použití pro 2000 – 2030.
- **Autoři**: **Dr. Joan Daemen** (Yo'-ahn Dah'-mun) of Proton World International a **Dr. Vincent Rijmen** (Rye'-mun), a postdoctoral researcher in the Electrical Engineering Department (ESAT) of Katholieke Universiteit Leuven.
- **Typ**: bloková šifra, blok 128 bitů, délka klíče 128, 192 a 256 bitů (4, 6, 8 32bitových slov), vícerundová, počet rund 10, 12 a 14 závisí na délce klíče.
- **Princip**: pracuje se s prvky Galoisova tělesa GF(2^8) a s polynomy, jejichž koeficienty jsou prvky z tohoto tělesa. Prvky v Galoisově tělese mají osm bitů, ale reprezentují polynomy $b_7x_7 + b_6x_6 + \ldots + b_0$. Základní operace jsou realizovány v okruhu polynomů modulo $m(x) = x^8 + x^4 + x^3 + x^1 + 1$.

AES – postup šifrování

1. Před šifrováním se vypočítá 4 + N_r*4 rundovních klíčů (32bitových slov). První 4 se naxorují na otevřený text („whitening") a umístí po sloupcích do matice $\boldsymbol{A}$.

$$\boldsymbol{A}=\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}$$

2. Proběhne N_r rund, v každé se použijí 4 rundovní klíče. Jedna runda probíhá

```
Round (State, RoundKey)
{
ByteSub (State)
ShiftRow (State)
MixColumn (State)      kromě poslední rundy
AddRoundKey (State, RoundKey)
}
```

ByteSub

bajtová substituce $a \rightarrow b$:

vypočítá se multiplikativní inverze prvku a: $c = a^{-1}$ mod $m(x)$, poté se bajt c transformuje na b substitucí:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix} + \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix}$$

ShiftRow

cyklická rotace prvků matice $\boldsymbol{A}$ v jednotlivých řádcích doleva, první řádek beze změny, druhý o jeden prvek, třetí o dva atd.

MixColumn

zesložitění prvků v rámci každého sloupce matice $\boldsymbol{A}$:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

např. $b_0 = '02' * a_0 \oplus '03' * a_1 \oplus '01' * a_2 \oplus '01' * a_3$

AddRoundKey

Naxorování bajtů klíče na prvky matice $\boldsymbol{A}$ po sloupcích.

AES – zpracování klíče

Šifrovací klíč k o N_k 32bitových slovech (4, 6 nebo 8) se naplní na počátek pomocného pole $\boldsymbol{W}[0 \ldots N_{k-1}]$. Toto pole následně expanduje:

```
for i = Nk to 4*Nr + 3 do
    {
    temp = W[i-1];
    if (i mod Nk = 0)
        temp = SubByte(RotByte(temp)) ⊕ Const[i/Nk];
    if ((i mod Nk = 4) AND (Nk = 8))
        temp = SubByte(temp);
    W[i] = W [i – Nk] ⊕ temp;
}
```

Využívají se operace:

RotByte – cyklický posun bajtů doprava,
SubByte – substituce bytů stejná jako u šifrování, aplikovaná na všechny bajty proměnné **temp**

a pole konstant **Const**[]