

# Prednáška č. 1

Bruce Schneier: Applied cryptography

- 2 druhy kryptografie - silná a slabá

- kryptologie - kryptografia - veda o vytváraní sifr. alg.

kryptanalyza - veda o rozbijaní sifr. alg.

- na tomto predmete - kryptológia = kryptografia

- 700 pml. - Grécko - skribal

- malica s mavinubým koženým prásom

- 360 pml. - na ulajovanie práv

- Česárová sifra - ABC

X Y Z

C D E F ...

A B

David Kahn: The codebreakers

- štúdium matemat. technik na <sup>ulajovanie</sup> ukryvanie inf.

- abeceda - 2 snaková (0,1), 26 (A...Z), 256

- mad non operácie (+) (-)

- záistenie integrity dát - po prenose dát nesmie nastaviť ich zmena

- autentifikácia, digitálny podpis

- identifikácia

- zdieľavé klúčov

- elektronické peniaze

- veda ako ukryť inf. do iných súborov - steganografia (časť kryptografie)

Kryptosystém

- usporiadana sústava ( $x, m, c, \tau$ )

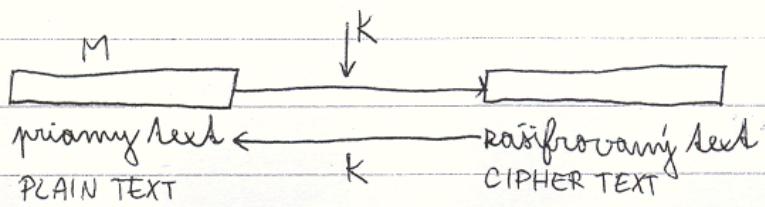
$x$  - množina klúčov

$m$  - množina priamych textov

$c$  - množina kódovaných textov

$\tau$  - kódovanie  $\tau: x * m \rightarrow c$

$x \in x, m \in m : \tau(x, m) \in c$



$$E_k(M) = C \quad E_k^{-1}(C) = D_k(C)$$

kašifrovanie kľúčom k správnej M

- symetrická krypt. - 1 kľúč na sifr. a na dešifr.

- nesymetrická krypt. - 1 na sifr. (verejny) a 1 na dešifr. (sajmy)

$$E_{k_1}(M) = C$$

$$E_{k_2}(C) = M$$

Útoky na kryptosystém - postup, ktorý môžeme odhaliť kašifroval. kľúč

### BRUTE FORCE ATTACK

$$x_1, x_2, \dots \in \mathcal{X} \quad D_{x_1}(C) = ? \in \mathcal{M}$$

- najsilnejší útok, dá sa mu zabrániť veľkou množinou kľúčov

- systém DES - 56 bitových kľúčov  $|2^{\text{bit}}| = 2^{56}$

### CIPHER TEXT ONLY ATTACK

- máme len kašifrovaný text

### KNOWN PLAINTEXT ATTACK

- vieme kúsok priameho textu a korespondujúcu časť kašifrov. textu

- napr. formuláre - vieme, kde má byť meno, priezisko, ...

### CHOSEN PLAINTEXT ATTACK

- podstrekávanie šifrovaním slov priame texty a sledovať, ako ich sifruje

### Substitučný systém

- každý znak nahradzuje iným znakom

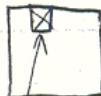
### Transpozičný systém

- prehadzuje znaky

- čítajú sa napr. pomocou tabuľky

- normy počet znakov

nesmiem vyzerať



vyrezané

## Kerckhoff (1835-1903)

- rádoby pre dobrý kryptosystém (platica náleží):

1. Prezrazenie alg. šifrovania nesmie ohrozit bezpečnosť sústavu.
2. Bezpečnosť spočíva iba v utajení kľúča.

## Cézarová sifra

$$A = \{ a_1, a_2, \dots, a_q \}$$

0	1	q-1
		$\epsilon^{2q}$

$$r = a \oplus k \quad E_k(a) = a \oplus k$$

$$D_k(r) = r \oplus k = r \oplus (-k)$$

$$\mathcal{K} = \{1, 2, \dots, q-1\} \quad 0 - \text{slabý kľúč}$$

## Afínna sifra

$$r = a \oplus k_1 + k_2$$

$$r \oplus k_2 = a \oplus k_1 \mid k_1^{-1}$$

$$(r \oplus k_2) \oplus k_1^{-1} = a_2$$

- musí existovať inverzný prvek k  $k_1$

$$2q \quad q=26$$

$k_1$  - môže byť: 0, 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24

-  $k_2$  - 12 kľúčov;  $k_1 - 26$  kľ.

$$r_1 = a_1 k_1 + k_2 \quad \epsilon^{26}$$

$$r_2 = a_2 k_1 + k_2 \quad \text{vyrieši sústavu a získame } k_1, a_1, k_2$$

## Všeobecná monoalfabetická sifra

$$\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|} \hline A & B & C & \dots & P & \dots & X & Y & Z & a \\ \hline Q & R & B & Z & & M & & A & P & Y & \dots & \end{array}$$

libovoľná permutácia  $26! \approx 10^{28} \approx 2^{93}$

$$E_\pi(a) = \pi(a)$$

$$D_\pi(c) = \pi^{-1}(c)$$

$$(\mathcal{X}, \mathcal{M}, \mathcal{C}, \mathcal{T})$$



$$P(x_1, x_2, \dots, x_n)$$

vlásmosti:

$$\sum_{(x_1, \dots, x_n) \in \mathcal{A}^m} P(x_1, \dots, x_n) = 1$$

$$P(x_1, \dots, x_n) = \sum_{(y_1, \dots, y_m) \in \mathcal{A}^m} P(x_1, \dots, x_n, y_1, \dots, y_m)$$

prázdneho slova  $(y_1, \dots, y_m) \in \mathcal{A}^m$

$$P(\emptyset) = 1$$

rodový inf.

$$P_m(x_1 \dots x_m) = \sum_{(y_1 \dots y_{m-1}) \in A^{m-1}} P(y_1 \dots y_{m-1} | x_1 x_2 \dots x_m)$$

↑  
ab p.s. mezi vším m - stacionárny zdroj

$$P_m(x_1 \dots x_n) = P(x_1) \cdot P(x_2) \cdot \dots \cdot P(x_n)$$

mezi všichy zdroj

$$I(a_i) = -\log_2 P(a_i) \quad A = \{a_1 \dots a_q\}$$

$$H_2 = \sum_{i=1}^q p_i \log_2 p_i = -\sum_{i=1}^q P(a_i) \cdot \log_2 P(a_i) \text{ - sredná inf. pre jednoznačkové slovo}$$

H<sub>2</sub>

$$H_2 = \sum_{x_1 \in A} \sum_{x_2 \in A} P(x_1, x_2) \cdot \log_2 P(x_1, x_2) \quad \frac{H_2}{2}$$

$$H_m = \sum_{x_1 \in A} \sum_{x_2 \in A} \dots \sum_{x_m \in A} P(x_1 \dots x_m) \cdot \log_2 P(x_1 \dots x_m)$$

$$\frac{1}{m} H_m$$

$\lim_{m \rightarrow \infty} \frac{1}{m} H_m$  entropia zdroja

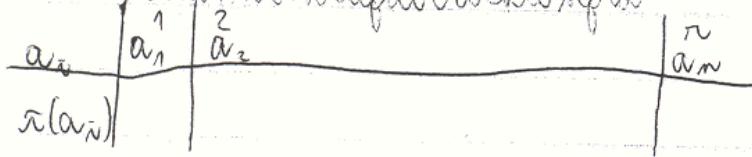
- entropia S) = 1,57 b na znak

8 b skomprimujeme na 1,57 b

15.10.

## Prednáška č. 2

Kriptogram monovalfabetického sifra



$i$  je pravdepodobnosť znaku  $a_i$  v kľúču  
 $f_k$  je frekvencia znaku  $a_i$

$$x_{ip} = \begin{cases} 1 & \text{ak } \pi(i) = p \\ 0 & \text{inak} \end{cases}$$

$$\sum_{n=1}^k x_{ip} = 1 \quad \text{pre } p = 1, 2, \dots, n$$

$$\sum_{p=1}^n x_{ip} = 1 \quad \text{pre } i = 1, 2, \dots, k$$

$$x_{ip} \in \{0, 1\}$$

$$\sum x_{ip} (p_i - f_k)^2 \rightarrow \min$$

Naďrekvenčovanie siedmich znakov prípadu 1. znak (medziem al. A)

$$\sum_{i,j,p,q} x_{ip} x_{jq} (f_{qj} - p_{ij})^2 \rightarrow \min \quad \text{- nelineárna kriteriálna funkcia}$$

- monovalfabetický sifring - šifruje meno znak po znaku

Polyalfabetické (blokové) sifry

- šifruje celý blok textu

Kasiskerovská sifra

vhodné kódované heslo

HESLO HESLO

PRIAMY TEXT

↓↓

H+P E+R S+I L+A O+N

- ak je rozdelenie hesla, ktoré rozlišiť je ľahké

- slabá sifra

## Index koincidencie

26 A, B, ..., Z  $p(a_1) = p(a_2) = \dots = p(a_q) = \frac{1}{q}$  ideálny stav - ale neplatí

$a_1, a_2, \dots, a_q$

- odchýlka od ideálneho stavu  $\sum_{n=1}^q (p(a_n) - \frac{1}{q})^2$

- metóda najmenších čtvercov - na základních

$$\sum_{i=1}^q (p(a_i) - \frac{1}{q})^2 = \sum_{i=1}^q (p^2(a_i) - 2p(a_i)\frac{1}{q} + \frac{1}{q^2}) = \sum_{i=1}^q p^2(a_i) - 2\frac{1}{q} \sum_{i=1}^q p(a_i) + \frac{1}{q^2} \sum_{i=1}^q 1 =$$

$$= \sum_{i=1}^q p^2(a_i) - 2\frac{1}{q}$$

miera nerovnomernosti - index koincidencie  $\chi^2$

- pravdep. že 2 náhodne vybrané znaky budú rovnake

$$p(a_1), p(a_1) + p(a_2), p(a_1) + p(a_3), p(a_3) + \dots + p(a_q), p(a_q)$$

$$p^2(a_1) + p^2(a_2) + p^2(a_3) + \dots + p^2(a_q) - \text{index koinc.}$$

$$q_f = 26$$

$$\frac{1}{q} = \frac{1}{26} = 0,03846$$

$$\chi^2 = 0,06027 \text{ pre } S_j$$

- odhad koincidencie v ňecte

$n$  - počet znakov v ňecte

$n_i$  - počet znakov  $a_i$

$n_1 = 11 - a_2$

$\vdots$

$n_q = 11 - a_q$

Počet dvojic znakov  $a_i$  (bez ohľadu na poradie)  $\frac{1}{2} n_i(n_i - 1)$

Počet všetkých znakov  $= 11 - \frac{1}{2} n(n - 1)$

$$\chi^2 = \frac{\frac{1}{2} \sum n_i(n_i - 1)}{\frac{1}{2} n(n - 1)} = \frac{\sum n_i(n_i - 1)}{n(n - 1)}$$

$x_1, x_2, \dots, x_m$

$\frac{1}{n}$  priameho ňectu

$\pi(x_1), \pi(x_2), \dots, \pi(x_n)$

$\frac{1}{n}$  roztočeného ňectu

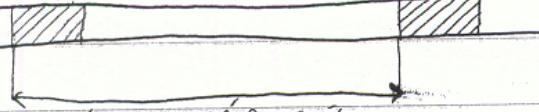
- pri monoalfab. sifre je ind. koinc. invariant - nemení sa

- ak sa sa blíži k 0,06, mohla byť použitá monoalf. šifra
- pri polyalf. šifre je ťe rozšfr. Ťechn rapidne klesne
- $\lambda$  - miera rovnenia rozdelenia priameho ťehu

Atrécie dléky kľúča - metódy:

1. určenie dĺžky kľúča klasičného metóda

- po sebe idúce n-tice znakov

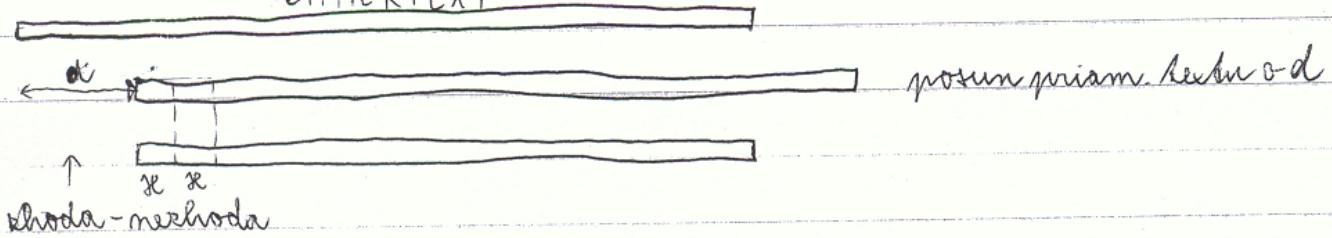


másobok dĺžky kľúča

- nájsť najväčšieho spoločného deliteľa

2. metóda indirektná koinciencia

CIPHERTEXT



pri posune o másobok kľúča skôrne počet rhôd =  $\lambda$

relatívny počet rhôd  $\approx \frac{1}{n}$

3. Friedmanov test

- predpoklad - dĺžka kľúča je k

$s_1$	$s_2$	$s_m$	
1	2		$k$
$s_1$	$s_2$		$s_k$
$s_{k+1}$	$s_{k+2}$		$s_{2k}$
$\vdots$			
$x_1$			

ak hesto nebude másobkom dĺžky kľúča, ťe sa bude lísiť od inol. kôm.

AOEI - najčasťejšie znaky

$$\{z_1, z_2, \dots, z_m\}$$

$$N_1 = \{z_1 - A, z_2 - A, \dots, z_m - A\}$$

$$N_2 = \{z_1 - 0, z_2 - 0, \dots, z_m - 0\}$$

$$\vdots$$

$$N_4 =$$

## MODPRIAMY TEXT

### TEXT ZNEJAKÉJK - kľúč

$k_1 \ k_2 \ \dots \ k_n$

lenak nesie 1,57 b inf.

$x_1 \ x_2 \ \dots \ x_n$

-11-

$$y_i = x_i + k_i$$

8 b > 3,14

- slov. text ťifrujem slov. textom

- relativity počet skôd by bol rovný ind. koin.

### Hillovská ťifra

- 1929 L.S. HILL

- ráčina byt silná

$A$  - konečným polom, ak  $A = \mathbb{Z}_p$   $p$  - prvočíslo

$$p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 \dots$$

$q = 256$   $\mathbb{F}_{2^8}$   $\mathbb{F}_{p^n}$   $p$  - prvočíslo  
existuje

$A = \mathbb{Z}_q$  - polyalfabetická ťifra

$$\text{kľúč } K = \begin{pmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & \dots & k_{nn} \end{pmatrix}$$

$$K^{-1} K = K \cdot K^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$$

↑ jednotková matica

$$X =$$

Príamy text  $x_1 \ x_2 \ \dots \ x_n \ x_{n+1} \ x_{n+2} \ \dots \ x_{n+m} \ \dots \ x_{n+kn}$

$$\#_1 \quad \#_2 \quad \dots \quad \#_n$$

$$E_k(x) = K \cdot x = y$$

$$k_{11}x_1 + k_{12}x_2 + \dots + k_{1n}x_n = y_1$$

$$k_{21}x_1 + k_{22}x_2 + \dots + k_{2n}x_n = y_2$$

⋮

$$k_{n1}x_1 + k_{n2}x_2 + \dots + k_{nn}x_n = y_n$$

$$x_i = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

$$D_k(y) = K^{-1}y$$

$$K^{-1}(K(x)) = (K \cdot K^{-1}) \cdot x = x$$

$$K \cdot E \sim (E | K^{-1})$$

- problém, ak matice bude singulárna (nie regulárna)

## KNOWN PLAINTEXT ATTACK

$$X_n \leftrightarrow Y_n \quad n=1, 2, \dots, m$$

$$\begin{array}{|c|c|} \hline x_{1n} & y_{1n} \\ \hline x_{2n} & y_{2n} \\ \hline \vdots & \vdots \\ \hline x_{mn} & y_{mn} \\ \hline \end{array}$$

$$K \cdot X_n = Y_n$$

$$X = (x_1, x_2, \dots, x_m) =$$

$$\begin{array}{cccc} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \vdots & \vdots & & \vdots \\ x_{mn} & x_{m2} & \cdots & x_{mm} \end{array}$$

$X$  analogicky  $Y$

$$K \cdot X = Y \quad \text{poznám } X, Y$$

$$(X | E) \sim (E | K^{-1}) \quad \text{riskam } K^{-1}$$

$$K \cdot X = Y \quad | \cdot K^{-1}$$

$$\underbrace{K(X \cdot K^{-1})}_{E} = Y \cdot K^{-1}$$

$$K \cdot E = Y \cdot K^{-1}$$

$$\boxed{K = Y \cdot K^{-1}}$$

Afíenna Hillovská sifra

$$E(x) = K \cdot x + b = x$$

$$D(x) =$$

$$D(x) = K^{-1}(y - b)$$

klíč  $K$ , vektor  $b$

## Hillovská šifra

$$\begin{array}{c|c|c|c} x_1 & x_2 & \dots & x_n \\ \hline & & \dots & \\ & & & x_N \end{array}$$

$$K \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

$$K \cdot x = y \quad x = K^{-1} \cdot y$$

- bloková šifra

- zaisťuje difúznu inf.

- ľavý riadok  $y_1, \dots, y_m$  rávna máx.  $x_i \rightarrow$  záverečné (difuzné) frekv. analýzy

$$X = \begin{pmatrix} x_{11} \\ x_{12} \\ \vdots \\ x_{1m} \end{pmatrix} = (x_1 \ x_2 \ \dots \ x_n) \quad Y = (y_1 \ y_2 \ \dots \ y_n)$$

$$K \cdot X = Y \quad / \cdot X^{-1}$$

$$K \cdot X \cdot X^{-1} = Y \cdot X^{-1}$$

$$K = Y \cdot X^{-1}$$

## Transpozičná šifra (permutačná)

$$\begin{array}{c|c|c|c} x_1 & x_2 & \dots & x_n \\ \hline & & \dots & \\ & & & x_{\pi_1(x)} \ x_{\pi_2(x)} \ \dots \ x_{\pi_n(x)} \end{array}$$

v jednotlivých blokoch poprechádzajú znaky

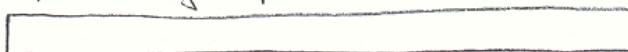
- treba určiť dĺžku bloku

- najčastejšie trojice znakov: OST, YCH, PRE, STI, OVA, ...

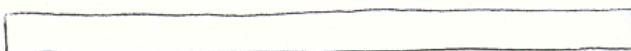


vedľaj. rovná másočku dĺžky bloku

- speciálny prípad Hill-S.



- CIPHERTEXT



→ riadok na kódovanie

0 1 0 1

- počet riadkov rastie, ak je druhý

sek posunutý o dĺžku bloku

$$K_{\pi} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_1 \\ x_2 \\ x_4 \end{pmatrix}$$

$$Z_{2^6} \quad y = x + k \\ x \text{ XOR } k$$

XOR

XOR		xor
XOR	0	1
0	0	1
1	1	0

$$E_k(x) = x \oplus k = y \quad D_k(y) = y \oplus k = (x \oplus k) \oplus k = x \oplus (k \oplus k) \\ = x \oplus 0 = x$$

- k - šifrovací a dešifrovací klíč

HESLO

AHOJ PETER

HOA EOH SOD

Vigenere

$k_1 \ k_2 \ \dots \ k_n \quad 1,57 \text{ b}$

$x_1 \ x_2 \ \dots \ x_n \quad 1,57 \text{ b}$

$$y_i = x_i \oplus k_i$$

- šifrovat jeden sestav sestavou k soho istého rečia je slabé

- ak budú klíče absolútne náhodné (k má mať informácie), potom

$k_i \oplus x_i$  nemá priestor na dodatočné inf. o x

$$P(k_i = 1) = \frac{1}{2} \rightarrow \text{k každý klíč nesie inf. 1b}$$

$P(k_i = 0) = \frac{1}{2}$  ONE TIME PAD - Vernamova šifra

$$y_i = E_{k_i}(x_i) \quad \text{priestová šifra} \quad y_i = x_i \oplus k_i$$

- bezpečnosť sári si od klíča

- jediná šifra absolútne sári si od klíča

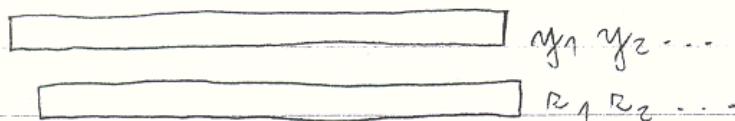
- nebezpečie:  $y_i = a_i \oplus k_i$  ak sa použije príslušný kľúč 2-krát  
 $r_i = b_i \oplus k_i$

$$y_i \oplus r_i = (a_i \oplus k_i) \oplus (b_i \oplus k_i) = a_i \oplus k_i \oplus b_i \oplus k_i = a_i \oplus b_i$$

1 priamy test zašifrovaný 2.

velmi skôr (riska sa väčšia inf.)

- preto sa príslušný kľúč smie použiť len raz na sif. a 1 na desif.



- návrat, keďže bol záčiatok; bol použitý ten istý príslušný kľúč

- otázka: Ako ich dostať do synchronizácie?

- riešenie: budem posúvať a sledovať počet rôzod

$$a_i \oplus b_j \oplus k_i \oplus k_j$$

- ak je počet rôzod > ako  $\frac{1}{2}$ , pravdepodobne sú správy eosynchronizované

$$p(k_1) = p(k_2) = \dots = p(k_n) = \frac{1}{2}$$

- Akuba viedie

- otázka: Ako rizikať kľúče?

- gen. moh. čísel nie sú vhodné pre kryptogr.

### Generátory náhodných čísel

- lin. kongruenčný gen.

$$x_m = (a x_{m-1} + b) \bmod m$$

- rýchlosť

- ak sa kvôli dobré a, b, majú veľkú periodu

- dobré súst. vlastnosti

- perioda  $\leq m-1$

- pre krypt. nerhodné (1977 J. Reeds)

$$X_m = (a X_{m-1}^2 + b X_{m-1} + c) \bmod m$$

- rôzny

- Joan Boyar Plunstein - dokázala, že je nerhodný pre krypt.

- pre krypt. - fyzikálne gen. náh. ē.
- 0,1 nemusia byť rovnomerne rozptýlené  
Treba sorynesiť

- metódy: (najvýrovnávanie počtu 0 a 1)

① -  $k_1, k_2, \dots, k_n$

$$K_1 = k_1 \oplus k_2 \quad \text{- aká je pravdepodobnosť } K_1 = 0$$

$$K_2 = k_3 \oplus k_4 \quad P(K_1 = 0) = P(k_1 = 0) \cdot P(k_2 = 0) + P(k_1 = 1) \cdot P(k_2 = 1)$$

$$\frac{1}{2} - \varepsilon \qquad \qquad \qquad \frac{1}{2} + \varepsilon^2$$

$$(\frac{1}{2} - \varepsilon)^2 + (\frac{1}{2} + \varepsilon)^2$$

$$\frac{1}{4} - \varepsilon + \varepsilon^2 + \frac{1}{4} + \varepsilon + \varepsilon^2 = \boxed{\frac{1}{2} + 2\varepsilon^2}$$

$$\varepsilon = 0,2 \quad 2 \cdot \varepsilon^2 = 2 \cdot 0,04 = 0,08$$

$$\text{ak } p_1 = 0,3 \quad p_2 = 0,7$$

$$0,58 \quad 0,42$$

②	00	00	11	11	10	10	01
			1	1	0		

- 2 rovnaké zahodim

- ak je star. niezdroj, dôsa posúvať hľadanie

## RC4

- 1987 - Ron Rivest

- pridložená ťifra

- bola krypta do 1994 - na internete sa objavil popis

$s[0], s[1], \dots, s[255]$  - 256 čísel v rozmedzi 0 .. 255

- tiež č. obsahujú permutáciu  
čísel 0 .. 255

- máme  $i, j$  - smerovky  $i \in \langle 0, 255 \rangle$

$\text{rand}()$

$j \in \langle 0, 255 \rangle$

$i = i + 1 \bmod 256$

$j = j + s[i] \bmod 256$

$\text{swap}(s[i], s[j])$  - vymenia sa obsahy biniek

$t = (s[i] + s[j]) \bmod 256$  - výsledok

$k = s[t]$

return  $s[t], k$

- klíč - libovolné dleší, až  $256 \times 8$  bitov



2[0] & 2[1]

$s[i] = i$  prefixe 0, 1, ..., 255

$$j = 0$$

for i=0 to 255

$j = (j + s[i] + k[i]) \bmod 256$

swap( $s[i], s[j]$ )    end

i = 0      portion alg. rand() ...

potom alg. rand()..

- rovnaký kľúč pre ťifr. aj dešifr.

- nedostane sa do rovnakej stavy po krátkej dobe, ak je dobré nastaviť.

- rozszerzenie RC4-VMPC - s[;]- 16 bitové nie 8

$$- \text{noční slávov } 256! - 256 \cdot 256 = 2^{1700}$$

poor flavor

poor flavor is by

- miesto slabé stránky (menášiel sa ziadny útok)

BLUM-MICALLI generator

$$x_{i+1} = g^{x_i} \bmod p$$

$$l_{-n} = 1 \text{ ak } x_i < \frac{n-1}{2} \quad -n-\text{big bit}$$

"0 inak

- vlastnosti rávnia na  $\mathbb{Q}$  a  $\mathbb{R}$

- odolny wobec kryzysu i stokom

RSAgen.

Yin-  
Wei

Mig - moe-

$$N = p_1 \cdot q_1 \quad \text{e - residuel } A(p_1-1), (q_1-1)$$

$$x_{i+1} = x_i \bmod N$$

$b_n = \text{ostatni} \text{ } \text{bit} \text{ } x_n$

## One Time Pad

$$k_1 k_2 k_3 \dots k_m$$

$$x_1 x_2 x_3 \dots x_m$$

$$y_1 y_2 y_3 \dots y_m \quad y_i = x_i \oplus k_i \quad x_i = y_i \oplus k_i$$

$$P(k_i=1) = P(k_i=0) = \frac{1}{2}$$

- nevzlištiteľná sifra

- nebezpečensťovo - ak použijem 2-krát ten istý kľúč

Lin. kongr. gen.

$$k_{m+1} = (ak_m + b) \bmod m$$

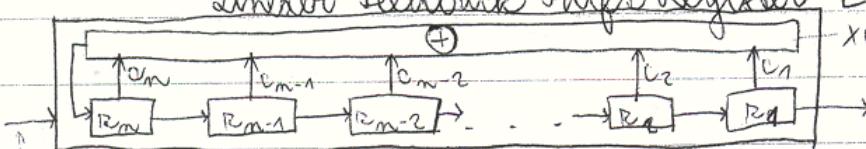
- nevhodný pre krypt. - dôsa ľahko existujú  $a, b, m$

R C4 alg.

- relativne bezpečný

## Lineárne posuvné registre

## Linear Feedback Shift Register LFSR



vodivový impulz

$$\text{XOR výstavka } \sum_{i=1}^m r_i = R_{m+1} \text{ - nový výstav } \\ c_i \in \{0, 1\} - \text{výstav signál}$$

do súťažky

$2^m - 1$  stavov - períoda

$$1 + c_m x + c_{m-1} x^{m-1} + \dots + c_1 x^m - \text{polynóm nad } \mathbb{Z}_2$$

od kohož polynómu závisia vlastnosti LFSR

- LFSR má max. períodu, ak jeho polynóm je primitívny:

- irreduibilný - nedá sa napsať ako súčin 2 polyn.

- delí polynóm  $x^{2^{n-1}} + 1$

- nedeli polynóm  $x^d + 1$  pre ťažné d také, že d delí  $2^n - 1$

(32, 7, 5, 3, 2, 1, 0) - primit. polyn.

$$x^{32} + x^7 + x^5 + x^3 + x^2 + x + 1$$

(1, 0) prim. polyn.

(2, 1, 0)

(3, 1, 0)

$$(9689, 8, 4, 0) \rightarrow \text{periód} 2^{9689} - 1$$

- príkladov sa časne opakovat až po veľkých periódach

$$c_1 R_1 + c_2 R_2 + \dots + c_m R_m = R_{m+1}$$

$$c_1 R_2 + c_2 R_3 + \dots + c_m R_{m+1} = R_{m+2}$$

:

$$c_1 R_m + c_2 R_{m+1} + \dots + c_m R_{2m-1} = R_{2m}$$

$$\begin{pmatrix} R_1 & R_2 & \dots & R_m \\ R_2 & R_3 & \dots & R_{m+1} \\ \vdots & & & \\ R_m & R_{m+1} & \dots & R_{2m-1} \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix} = \begin{pmatrix} R_{m+1} \\ R_{m+2} \\ \vdots \\ R_{2m} \end{pmatrix}$$

- co je klin?  $\Rightarrow c_i$

$$Z \cdot \vec{c} = \vec{z}$$

$$\vec{c} = Z^{-1} \vec{z}$$

- ak máme 2-másobok periody, existuje  $c_i$

$$R_1 R_2 R_3 R_4 R_5 R_6 R_7 R_8$$

$$0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$Z^{-1}$  řešba

$$(Z|E) \sim (E|Z)$$

$$\left( \begin{array}{c|ccccc} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{array} \right) \sim \left( \begin{array}{c|ccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{array} \right) \sim \left( \begin{array}{c|ccccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array} \right)$$

$$Z^{-1}$$

$$Z^{-1} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix}$$

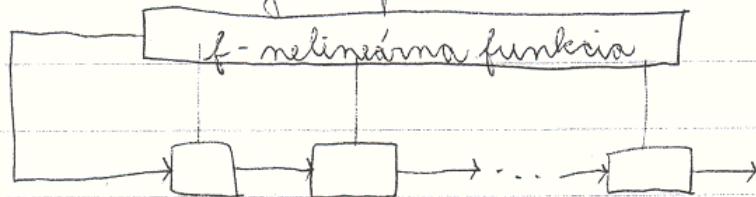
$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$



- nevhodné

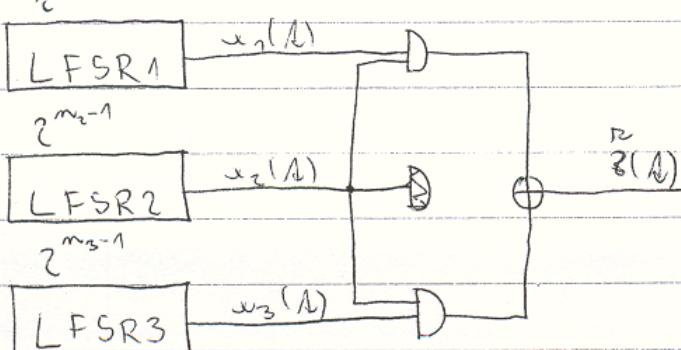
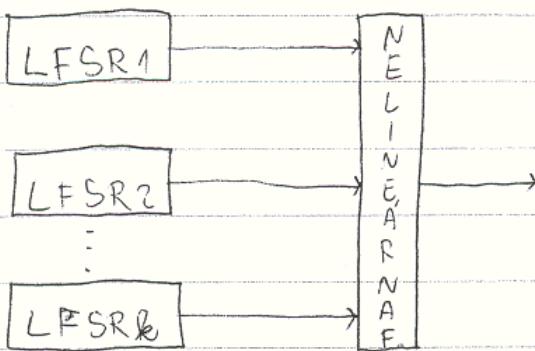
# Pokusy o klesanie LFSR

1.



$$r_{m+1} = f(r_1, r_2, \dots, r_m)$$

2.



$$R(A) = x_1(A) \cdot x_2(A) \oplus (1 + x_2(A)) \cdot x_3(A)$$

- kľúč - protiahožník na stavenie registrov

$x_1$	$x_2$	$x_3$	$e$	$\bar{x} = x_1$	$\bar{e} = x_3$	$R = x_2$
0	0	0	0	+	+	+
0	0	1	1	-	+	-
0	1	0	0	+	+	-
0	1	1	0	+	-	-
1	0	0	0	+	+	-
1	0	1	0	+	+	+
1	1	0	1	+	-	+
1	1	1	1	+	+	+

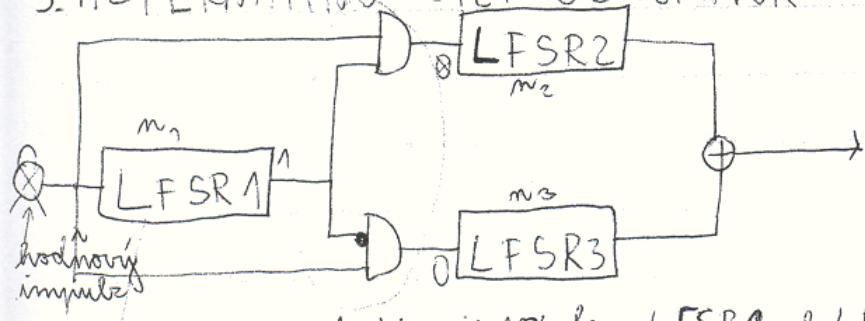
$$\frac{6}{8} = \frac{3}{4} = P(R=x_1) \quad P(R=x_3) = \frac{3}{4}$$

$r_1, r_2, r_3, \dots$  korelačný útok

$m_1, m_2, m_3, \dots$

- ak počet e-hôd by mal byť  $\frac{3}{4}$ , viem, že bol nastavený rovnaký očko/keras  
 $(2^{m_1-1})(2^{m_2-1})(2^{m_3-1})$

### 3. ALTERNATING STEP GENERATOR



posuny sa len LFSR2 a LFSR3

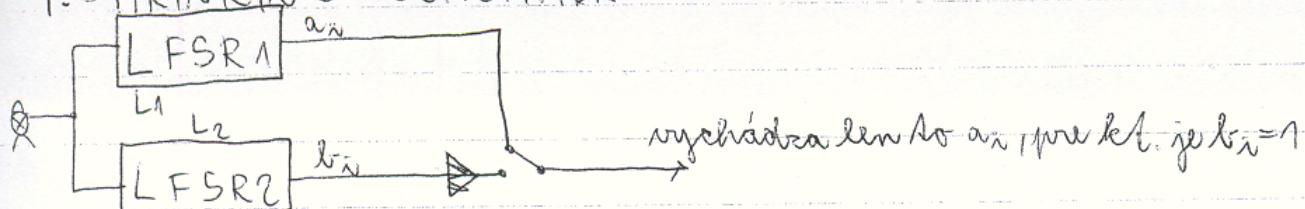
-  $L_1, L_2, L_3$  nesúvisiace, približne rovake

$$2^{m_1} (2^{L_2} - 1) (2^{L_3} - 1) \quad L_1, L_2, L_3 \text{ nesúvisiace, približne rovake}$$

vyrovnený funk., že po  $m-1$  mlnach vyste ešte 1 mln

- + bezpečnosť

### 4. SHRINKING GENERATOR



$L_1, L_2$  - nesúvisi.

$$(2^{L_1} - 1)(2^{L_2} - 1)$$

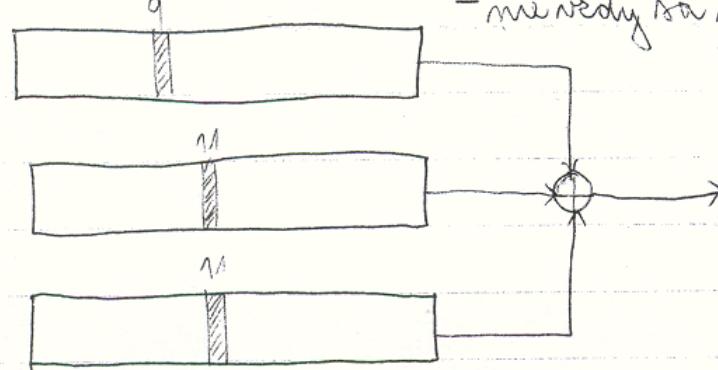
### 5. n-mobiloch GSM algoritmus A5

(19, 818, 17, 14, 8) - dĺžky posuvných registror

(122, 21, 17, 13, 0)

(23, 22, 19, 18, 0)

- nie vedia sú posuvajúce registrory



posun i-eho reg.  $b_i$

$$b_2 \oplus T(b_1, b_2, b_3)$$

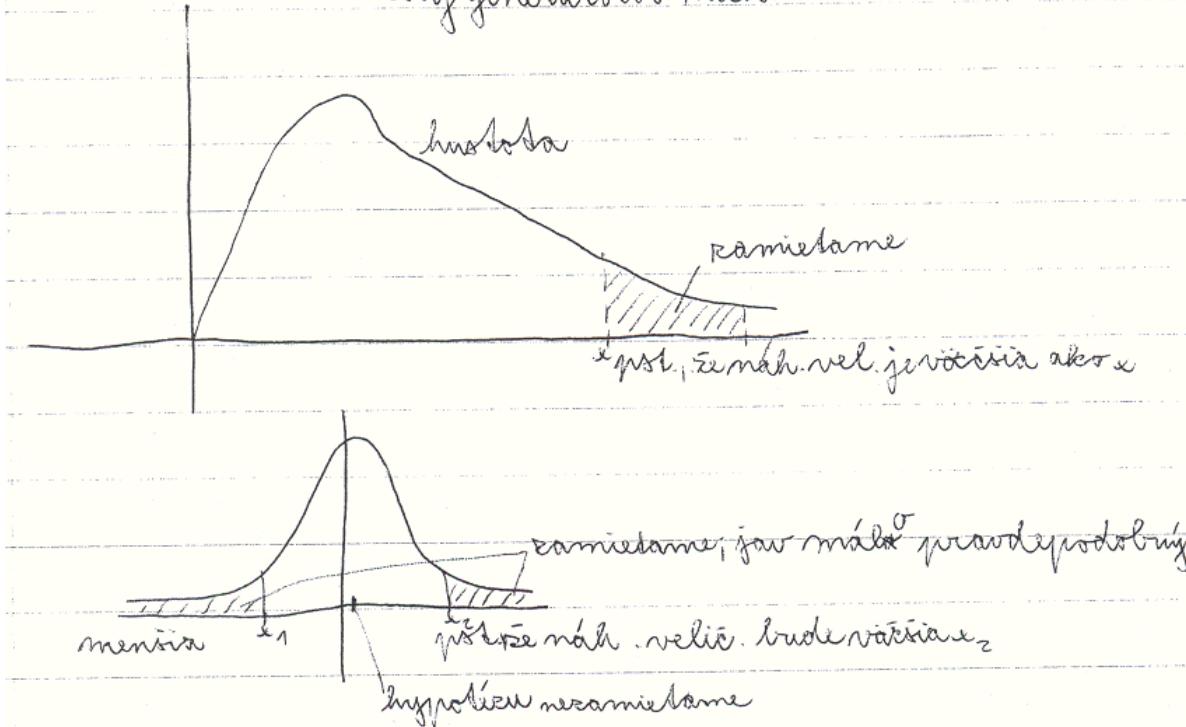
$$b_3 \oplus T(b_1, b_2, b_3)$$

- hlasovacia f. -  $T(110)=1 \quad T(000)=0$

$$T(101)=1$$

$$T(111)=0$$

# Testy generátorov náh. čísel



## 1. frekvenométrický test

$m_0$  - počet nulových bitov       $m = m_0 + m_1$

$m_1$  - počet jednotkových bitov

$$X_1 = \frac{(m_0 - m_1)^2}{m} \approx \chi^2(1)$$

z hypotézy  $X_1 = 0$

počet 0 = počet 1

## 2. TWO BIT TEST - SERIAL TEST

$m_0$  - počet 0b

$m_1$  - počet 1b

$m_{00}$

$m_{01}$

$m_{10}$

$m_{11}$

počet dvojic - rovnomerne rozložené - hypotéza

$$m_{00} + m_{01} + m_{10} + m_{11} = m - 1$$

$$X_2 = \frac{4}{m-1} (m_{00}^2 + m_{01}^2 + m_{10}^2 + m_{11}^2) - \frac{2}{m} (m_0^2 + m_1^2) + 1 \approx \chi^2(2)$$

pre  $n > 21$

## 3. POKER TEST

$m$	$m$	$m$		$m$	$k$	$k \leq m \leq n$
1	2	3			$k$	$k \geq 5 \cdot 2^m$

$i = 0, 1, 2, \dots, 2^m - 1$        $m_i$  - počet výskytov čísla  $2^i$

$$X_3 = \chi^2 \sum_{i=0}^{2^m-1} m_i^2 - k \approx \chi^2(2^m - 1)$$

#### 4. RUNS TEST

blok - posloupn.  $0 \frac{1}{n} \dots 1,0$ , nedá se v ně dálji rozšiřovat

gap - posloupn.  $1,00 \dots 0,1$

$$e_i = \frac{n-i+3}{2^{i+2}} \text{ očekávaný počet blokov délky } i \text{ v posloupnosti n libor}$$

$b_i$  - počet blokov délky  $i$

$$g_i = \sum_{j=1}^k \frac{(b_j - e_j)^2}{e_j} + \sum_{j=1}^k \frac{(g_j - e_j)^2}{e_j} \quad \text{pro } e_i \geq 5$$

$$\approx \chi^2(2k-2)$$

#### 5. autokorelační test

$s_1, s_2, s_3, \dots, s_n$

$$d \quad 1 \leq d < \frac{n}{2}$$

$$A(d) = \sum_{n=1}^{n-d} s_n \oplus s_{n+d}$$

$$X_d = 2 \frac{A(d) - \frac{n-d}{2}}{\sqrt{n-d}} \quad \approx N(0,1)$$

- počet  $s_a$  by mal být rovnaký

- počet libor rozcorovaných s posloupností samého sebe

- vzorce netreba, len princip pochyt

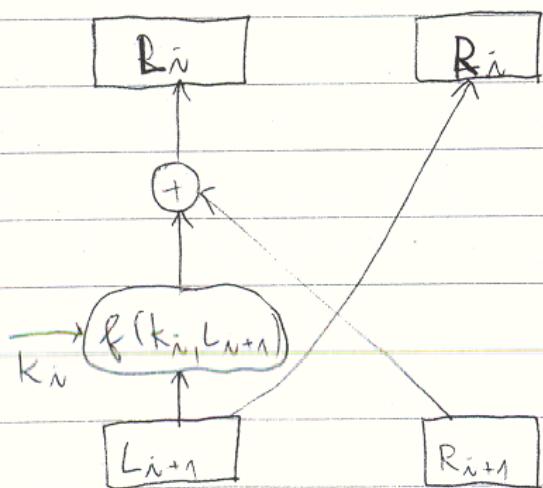
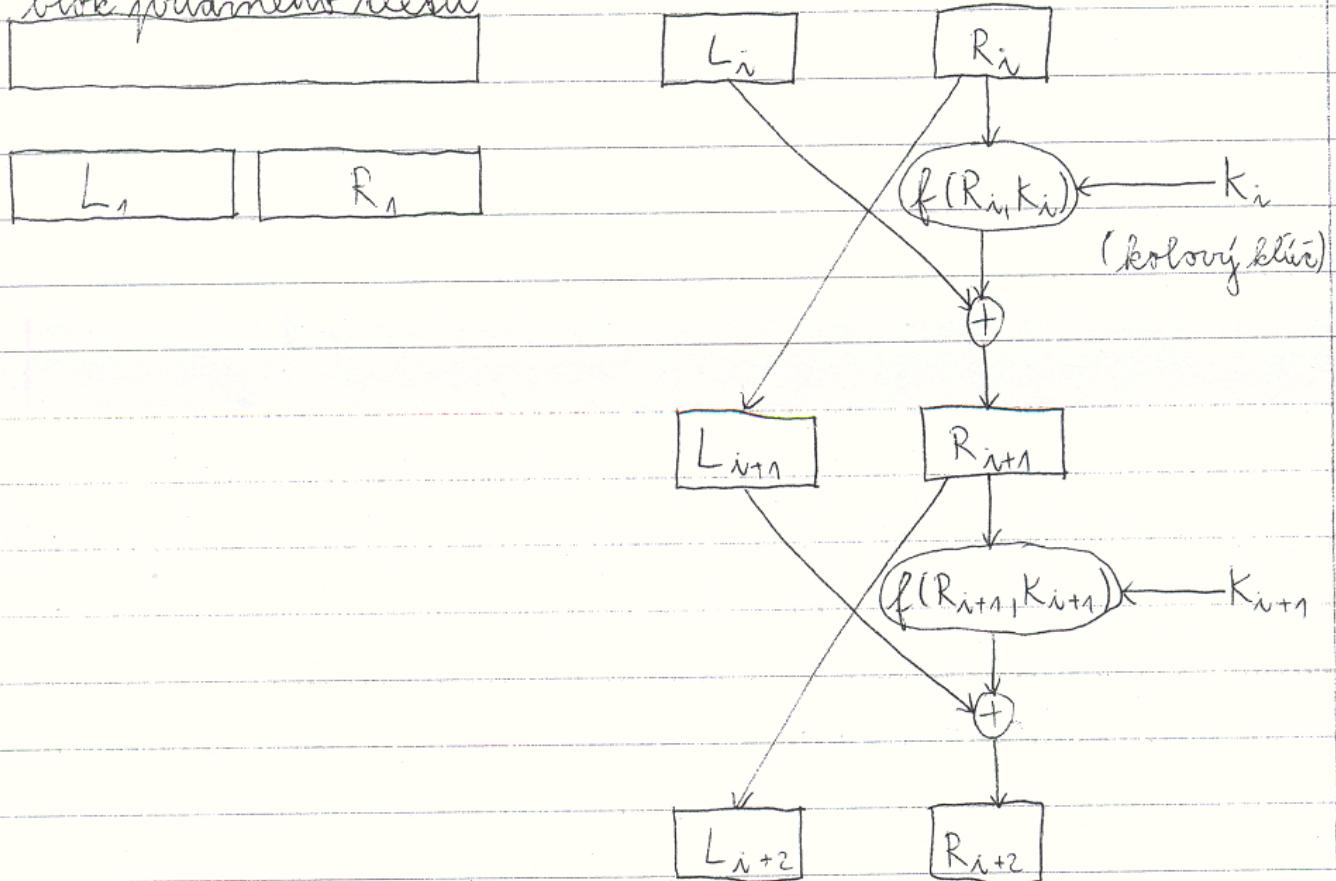
#### 6. FIPS 140-1 (pro 20 000 b)

## Symetrická kryptografia

1. A, B - dve ľudia / inštancie, dohodnutí kryptografie
2. A, B - dohodnutý kľúč K - súpravný
3. A, resp. B šifruje  $E_K(x) = y$
4. B, resp. A dešifruje  $D_K(y) = x$

## Kryptosystém Feistellovho typu

blok priameho zložu



- dešifrovanie:

- kľúče dávaj v opačnom poradí

- nymení stramy

$$f(k_i, R_i) \oplus R_{i+1} = L_i$$

$$f(k_i, R_i) \oplus L_i$$

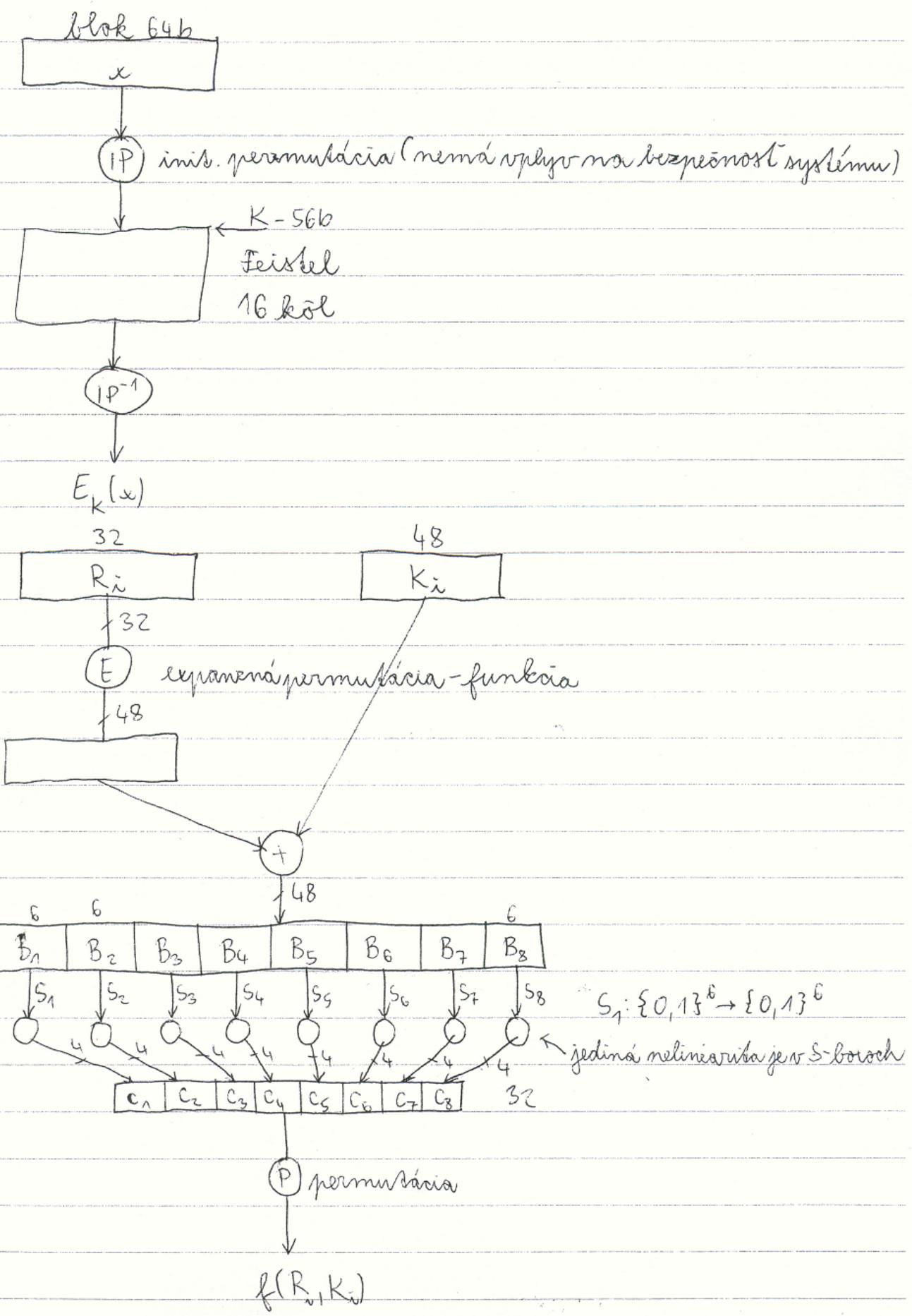
- odvlné voči smerom

# DES - Data Encryption System

- IBM - 1975

- blok - 64b

- kľúč - 56b



- S-boxy

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
6	18	14	8	143	86	82	811	15	12	89	97	83	10	15	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

- Šloby

$b_1, b_2, b_3, b_4, b_5, b_6$

$b_1, b_2$  - riadok

$b_2, b_3, b_4, b_5, b_6$  - slípce

011101

01-1



01110-14

0011

- každý riadok - permutácia 0-15

- nie je lineárna ani afínna ...

expansívna funkcia E

B	32	1	2	3	4	5
	4	5	6	7	8	9
	8	9	10	11	12	13
	12	13	14	15	16	17
	16	17	18	19	20	21
	20	21	22	23	24	25
	24	25	26	27	28	29
	28	29	30	31	32	1

-  $C_1$  - má 4 b, ale rávňa sa 6 b vstupu; aby sa dosiahla difúzia inf.

permutácia P

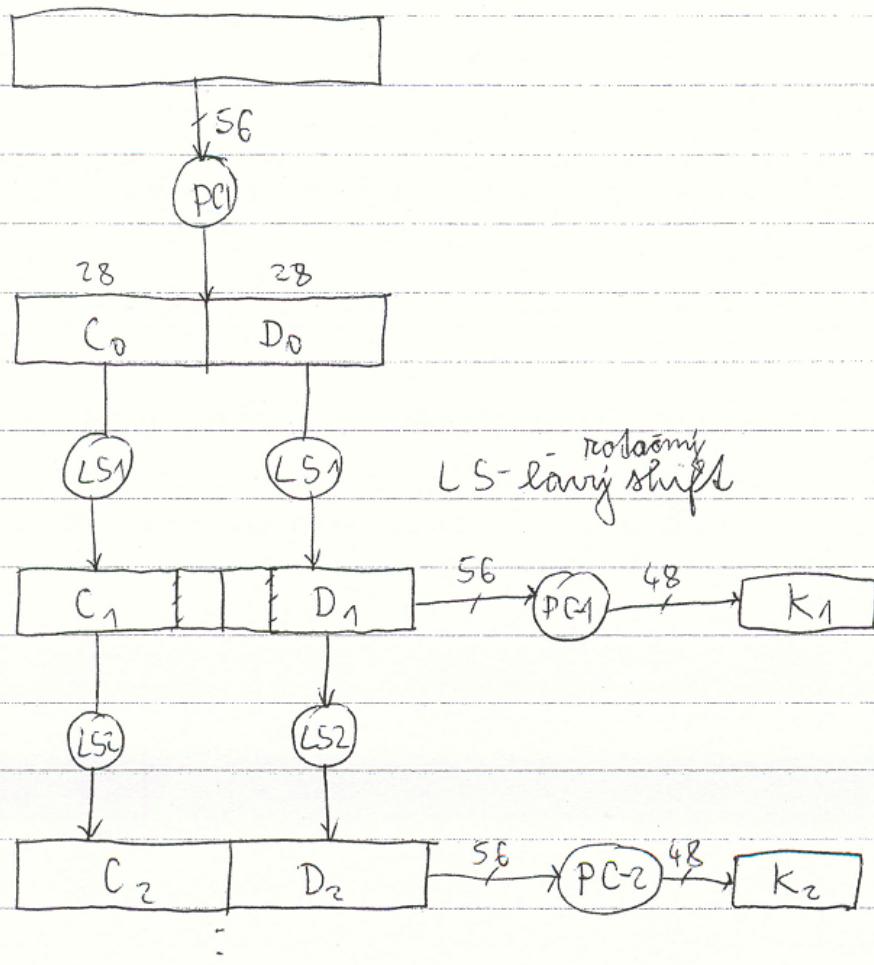
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

- nízok rizikovosť difúzie

kľúč - 56b



- 64b - 2 kohy 8 paritných



LS<sub>i</sub> - 1, 2, 9, 16 a 16

inak o 2b

PC-2

14	17	11	24	5	1
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

- slabé kľúče - súme 00, so 01

- súme 11, 10

- útoky - CHOSEN PLAIN TEXT ATTACK

- diferenciálna kryptanalyza - odolný (ale ak ~~odolný~~ obserueme 2 kola, nám je taký odolný)

- lineárna kryptanalyza - nám je odolný

$x_1 \dots x_{64}$  - plain text

$y_1 \dots y_{64}$  - príslušný káisfr. text

$$x_{17} \oplus y_3 \oplus y_8 \oplus y_{14} \oplus y_{25} = (K_i)_{26} \quad \text{A pravdep. } P = \frac{1}{2} - \frac{5}{16}$$

$2^{47}$  plain textov  $\rightarrow$  2 útoky

$2^{43}$  ~ 11 - 50 dní

- najväčšia slabosť systém - 56 b kľúč -  $2^{56}$  možnosť

- ďalšie nebezpečenstvo - dĺžka bloku

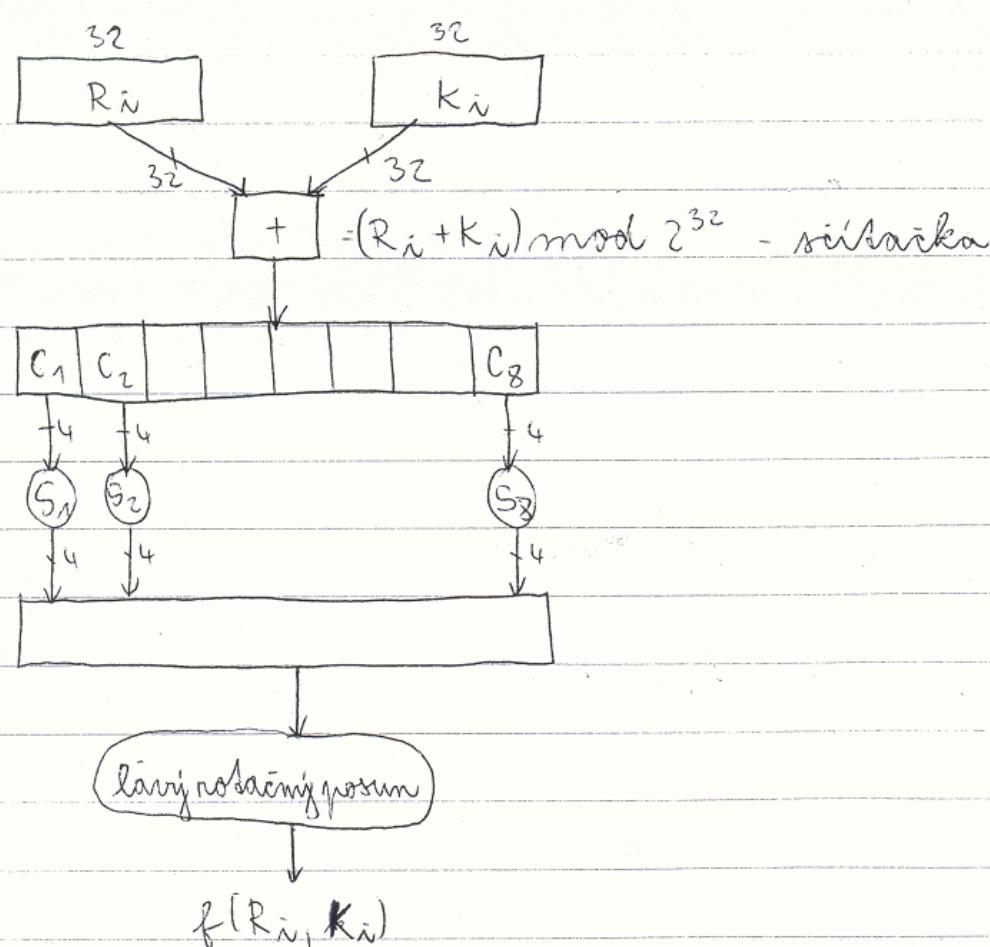
- veľké poučenie - pred šifrovaním skomprimovať text

## GOST

- 256 b kľúč

- Feistel - 32 kôl

- 64 b blok



- útok hruškovou sibou nemysliteľný

$256b = 8 \cdot 32b$  blokov



$K_1 \ K_2 \ K_3 \dots \ K_8$

1-8

1-8

:

8-1

0	1	2	$S_1$	15
4	10	9	2	13 8 0 14 6 11 1 12 7 15 5 3

- neboli inčenj pre širokú verejnosc - šifrovací systém
- slabina v dĺžke bloku ostáva

$$C = (c_1, c_2, c_3, c_4) = \sum a_i c_i \quad - \text{nonlineárna}$$

Operačné módy pre blokové šifry

$x_1, x_2, x_3, \dots$  - bloky priameho textu

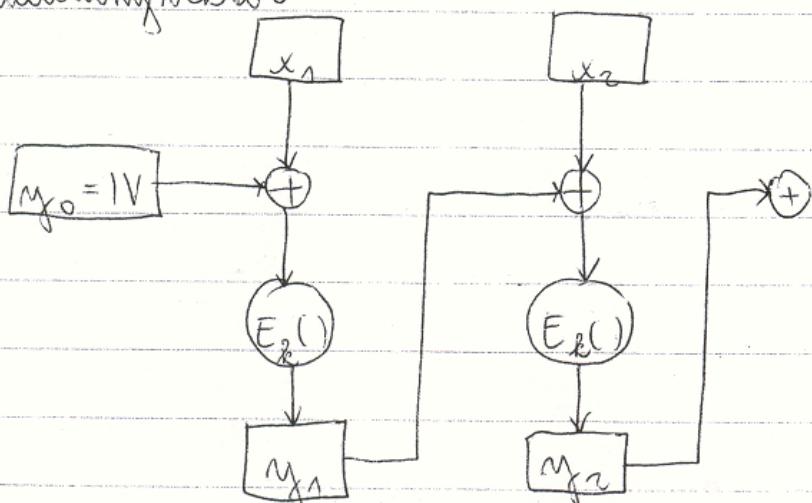
ECB - Electronic code book

$$y_1 = E_k(x_1), y_2 = E_k(x_2), \dots, y_i = E_k(x_i)$$

CBC - Cipher block chaining mode

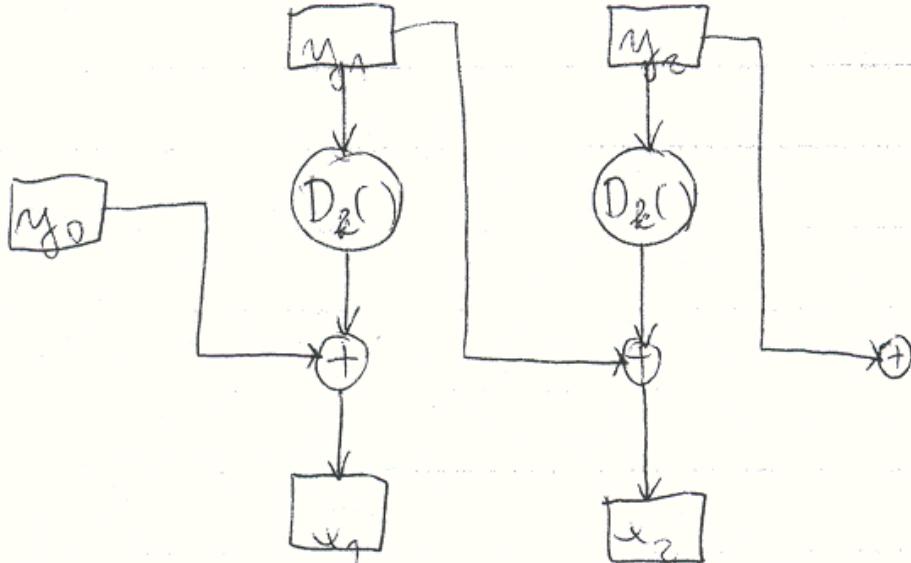
$$y_0 = IV$$

inicIALIZACIj vektor



$$y_i = E_k(y_{i-1} \oplus x_i)$$

IV - môže byť rôzny, ale vždy iný  $\Rightarrow$  rovnaká správa inak řeši.



$$x_i = y_{i-1} \oplus E_k(y_i)$$

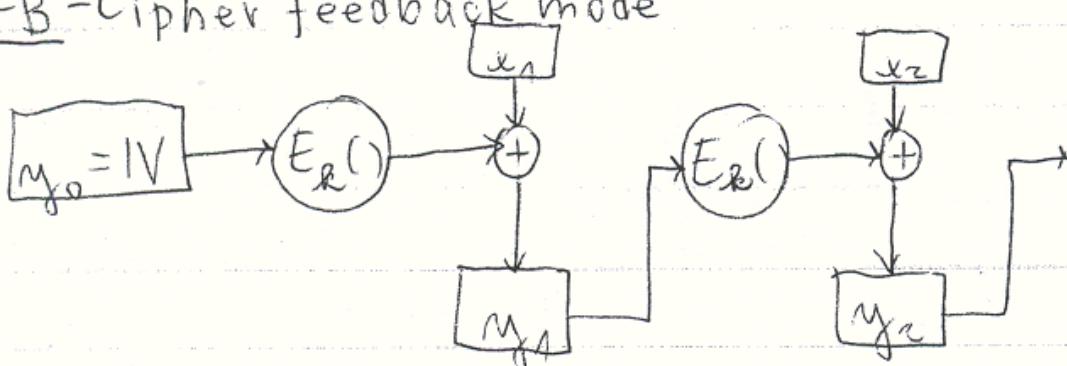
OFB - Output feedback mode



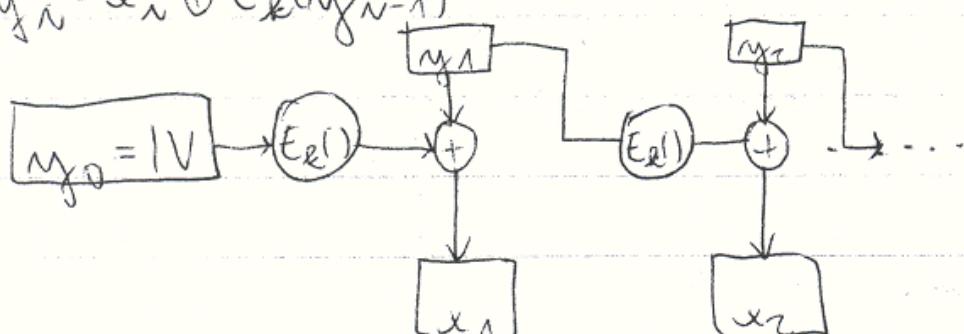
$$y_i = r_i \oplus x_i$$

$$x_i = y_i \oplus r_i$$

CFB - Cipher feedback mode



$$y_i = x_i \oplus E_k(y_{i-1})$$



$$x_i = y_i \oplus E_k(y_{i-1})$$

12.11.

Prednáška Č. 6

## DES

$$E_{k_2}(E_{k_1}(x)) = E_{k_3}(x) \quad \text{klúč - dvojica } (k_1, k_2) - 2 \times 56b = 112b$$

- otázka: či tieto súhrnenia tvoria grupu?  $E_{k_2} \circ E_{k_1}$  časovana
- časovská súhra vzhľadom na skladanie tvorí grupu elositosť

 $G_0$ 

$$\forall a, b \in G \quad \exists c \in G$$

$$c = a \circ b$$

$$o(\text{lin. operácia}): (a \circ b) \circ c = a \circ (b + c)$$

$$\exists x \in G \quad x \circ b \circ a = a \circ x = a$$

$$\forall a \in G \quad \exists a^{-1} \quad a \circ a^{-1} = e$$

$\downarrow$

$$E_{k_2} \circ E_{k_1} \quad \forall k_1, k_2 \quad \exists k_3 \quad E_{k_2} \circ E_{k_1} = E_{k_3}$$

- otázka: Je DES grupa?

- ukážalo sa, že asi nie

MEET IN THE MIDDLE - útok

$$C = E_{k_2}[E_{k_1}(P)]$$

$$D_{k_2}(C) = E_{k_1}(P)$$

$k$	$E_k(P)$
$k_1$	
$k_2$	
$\vdots$	
$k_{56}$	

Tab. bude mať  $2^n$  položiek

$D_2(C)$

- složitosť  $\approx 2 \cdot 2^{56} \cdot 56$  (ak máme 2 klúče)

$$C = E_{k_1}(D_{k_2}(E_{k_1}(P))) - 3\text{-DES}$$

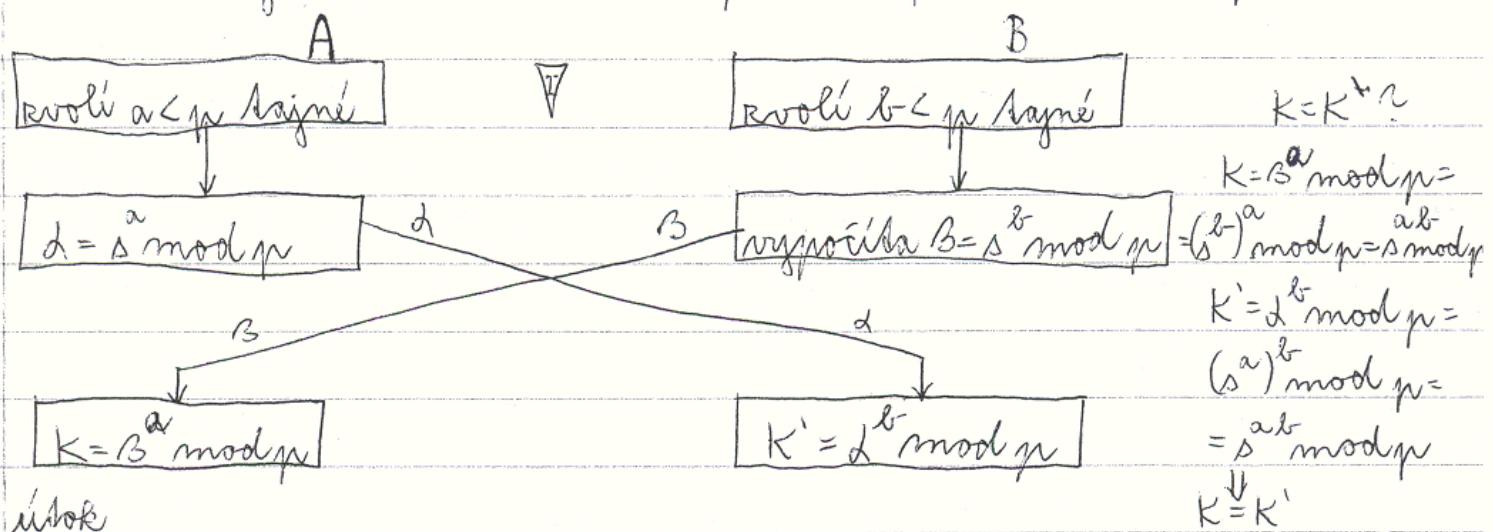
- lepsi spôsob

- menší a jednoduchý kryptogr. útok

# DIFIE HELLMANova výmena kľúčov

- protokol na výmenu kľúčov

1. A, B sú verejne dohodnuté na veľkom prvočíslu  $p$  a čísle  $0 < s < p$

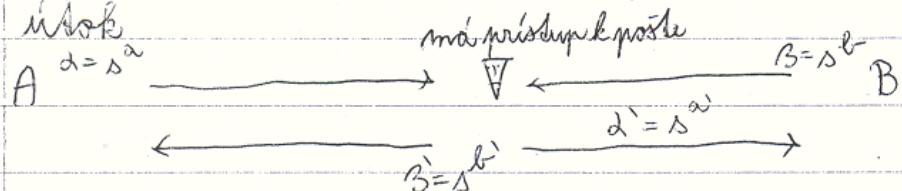


útok

$\nexists B = s^b \pmod{p}$  - neriešme riešiť

$$b = \log_s B$$

útok



$$K_A = s^{a \cdot b}$$

$$K_B = s^{a \cdot b}$$

- komunikuje s oboma promocon svojich kľúčov  $a, b$

- kontrola kľúča medzi A,B, aby zamezdili útoku

## IDEA

-  $128b$  blok - slabina

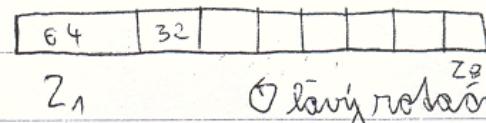
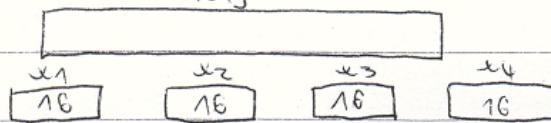
-  $64b$  kľúč

- operácie:

① - mísolenie mod  $2^{16}+1$   $\sim 2^{2^{16}+1}$   
alebo, pravdepodobnosť

⊕ - sčítanie mod  $2^{16}$

④ - binárny XOR  
 $84b$



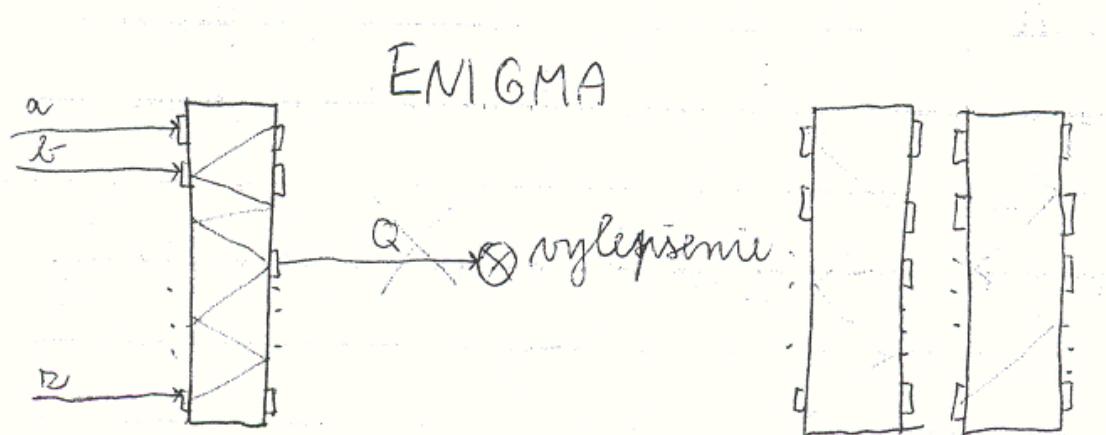
128b

Z<sub>1</sub>

Očkový rotacioný shift 825

# PGP

- šifrovací klíč
- ako šifrovací alg. obsahuje IDEA

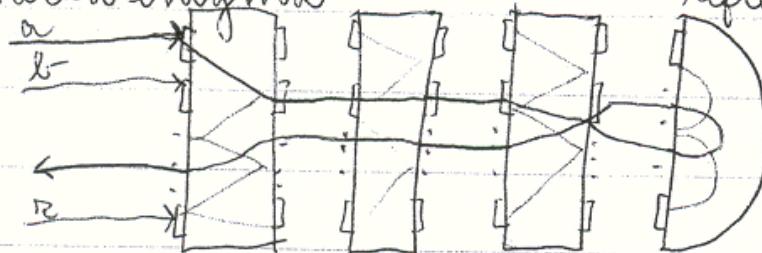


- keď sa stavia, kontakt (koliesko) sa posunie o 1 (na b-)

⇒  $26 \times 26 \times 26$  možnosti

- nemecká enigma

reflektor - odváža signál späť



- a nikdy nebolo zašifrovane na a

$26 \times 26 \times 26 \times 26 \times 26 \times 26 + 3!$

počet a... zásada počítania  
na kolieskach počet koliesok

## Asymetrická kryptografie

$$N = \{1, 2, 3, \dots\}$$

$$C = \{0, \pm 1, \pm 2, \dots\}$$

0

$$a, b \quad a \mid b \quad \exists k \quad b = a \cdot k$$

Základní věta aritmetiky

$m \in N$   $m > 1$  každé číslo  $m$  se dá napísať  $m = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$

kde  $p_i$  jsou prvocísla a  $d_i \in N$  a  $i \geq 1$

A tento rozklad je jednoznačný

- číslo  $m$  se nedá napísať 2 různými způsobami

$$54 = 2 \cdot 27 = 2^1 \cdot 3^3$$

Největší společný delitel čísla  $a, b \in N$   $\text{NSD}(a, b)$

- jaké číslo

$$1. d \mid b \quad \text{a } d \mid a$$

$$2. \text{ ak } d \mid a \quad \text{a } d \mid b \Rightarrow d \mid d$$

Euklidov alg.

$$\text{NSD}(a, b)$$

$$r_0 = a, r_1 = b$$

$$r_0 = r_1 - q_1 r_2, \text{ kde } r_2 < r_1$$

$$r_1 = r_2 - q_2 r_3, \quad r_3 < r_2$$

$$\vdots$$

$$r_{m-3} = r_{m-2} - q_{m-2} r_{m-1}$$

$$r_{m-2} = r_{m-1} - q_{m-1} r_m$$

$$r_{m-1} = r_m \cdot q_{m-1} + 0$$

Končíme a prověříme  $r_m = \text{NSD}(a, b)$

$$\begin{array}{l} \lambda \\ \gamma p_0 = 0 \end{array}$$

$$\begin{array}{l} \lambda \\ \gamma p_1 = 1 \end{array}$$

$$\lambda_n = \lambda_{n-2} - q_{n-1} \cdot \lambda_{n-1} \bmod r_n$$

$$\text{pre každé } i, j \in \lambda_i \cdot r_i \bmod r_0$$

$$r_m \equiv \lambda_m \cdot r_1 \bmod r_0$$

$a \equiv b \pmod q \Rightarrow (a - b)$  je deliteľné číslom  $q$

kongruencie

$q \nmid (a - b)$  alebo  $\exists k$

je deliteľom  $(a - b) = kq$

- ak  $\text{NSD}(a, b) = 1$ , potom  $1 \equiv a_m - b \pmod r_0$

$$1 \equiv a_m - b \pmod a$$

$$\Leftrightarrow a \equiv b \pmod a$$

- ak  $b < a$

$$a_m, b \in \mathbb{Z}_a$$

$\forall \mathbb{Z}_a$  platí  $a_m \cdot b = 1$

je riešením rovnice  $x \cdot b = 1$

$a_m$  inverzny pravok  $k \neq b \in \mathbb{Z}_a$  a  $\text{NSD} = 1$

- treba vedieť, že preto NSD a ak  $b < a$ , existuje rozšírenie, ktoré umožní vyprázdniť inverzny pravok  $k$  k  $b$

$a \equiv b \pmod q$  c ľubovoľné

$$\Downarrow c \cdot a \equiv c \cdot b \pmod q$$

$$\exists k \quad (a - b) = k \cdot q$$

$$c \cdot a - c \cdot b = \cancel{c} (a - b) = \cancel{c} (k \cdot q) = k \cdot \cancel{q}$$

$$6 \equiv 2 \pmod 2$$

$$15 = 5 \pmod 5$$

$$15/5 \stackrel{?}{=} 5/5 \pmod 5$$

$$3 \not\equiv 1 \pmod 5$$

$$c \cdot a \equiv c \cdot b \pmod q \quad c \text{ nesúdeliteľné s } q$$

$$c(a - b) = k \cdot q$$

↓

$$q \nmid (a - b) \Rightarrow a \equiv b \pmod q$$

$$b - x \equiv 1 \pmod a$$

$$a \cdot x \equiv 1 \pmod b$$

} vieme riešiť

Eulerova funkcia  $\varphi$

Def.

$\varphi(n)$  je počet prirodzených č. menších alebo rovinných č. menej než  $n$  a ktoré sú s  $n$

$$\varphi(1)=1$$

$$\varphi(2)=1$$

:

$n$	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4

$\varphi(p^n) = p^n - p^{n-1}$ , kde  $p$  je prvočíslo

$$\varphi(p^n) = p^n - p^{n-1}$$

$\underbrace{p \cdot 1 \cdot p \cdot 2 \cdot p \cdot 3 \cdots p \cdot p^{n-1}}_{p^n} - p^{n-1}$  - nesúdeliteľné

$$\text{pre } 9 \quad 3^2 - 3 = 9 - 3 = 6$$

$$8 \quad 2^3 - 2^2 = 8 - 4 = 4$$

ak  $a, b$  nesúdeliteľné, potom  $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

$$m = p_1^{d_1} \cdot p_2^{d_2} \cdots \cdot p_k^{d_k}$$

$$\varphi(m) = \varphi(p_1^{d_1}) \cdot \varphi(p_2^{d_2}) \cdots \varphi(p_k^{d_k}) = \varphi(p_1^{d_1}) \cdot \varphi(p_2^{d_2}) \cdots \varphi(p_k^{d_k}) =$$
$$= (p_1^{d_1} - p_1^{d_1-1}) \cdot (p_2^{d_2} - p_2^{d_2-1}) \cdots (p_k^{d_k} - p_k^{d_k-1})$$

$$= p_1^{d_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{d_2} \left(1 - \frac{1}{p_2}\right) \cdots p_k^{d_k} \left(1 - \frac{1}{p_k}\right) =$$

$$= (p_1^{d_1} \cdot p_2^{d_2} \cdots p_k^{d_k}) \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$m$

$$= m \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

- ak  $p_1, p_2$  prvočísla

$$\varphi(p_1 \cdot p_2) = (p_1 - 1) \cdot (p_2 - 1)$$

$p^n$  - prvočíslo

$$(a+b)^n \equiv a^n + b^n \pmod{p}$$

$$(a+b)^n = \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + 1 \cdot b^n$$

$$= \binom{n}{n} = \frac{n(n-1)(n-2)\cdots(n-i+1)}{1 \cdot 2 \cdots} = n(\dots)$$

$$n \geq p \text{ platí } (a+b)^n = a^n + b^n$$

$$2^p = (1+1)^p = 1^p + 1^p = 2 \pmod{p}$$

$$3^p = (2+1)^p = 2^p + 1^p = 2 + 1 = 3$$

:

$$a^p \equiv a \pmod{p} \quad \text{malá veda Fermatova}$$

$$c^p \equiv c \pmod{p} \quad \text{pre libovolné prvočíslo } p \text{ a lib. } c \in \mathbb{N}$$

- ak  $c$  nesúdeliteľné s  $p$  (staci aby  $c < p$ )

$$\text{c je } c \cdot c^{p-1} = c \cdot 1 \pmod{p}$$

$$c^{p-1} \equiv 1 \pmod{p}$$

- v kryptografii - na test, či je  $m$  prvočíslo

- otázka: je  $M$  složené číslo?

- odpoved: ak  $c^{M-1} \not\equiv 1 \pmod{M}$  pre nejaké  $c \in \{1, 2, \dots, M-1\} \Rightarrow M$  je složené

- tento test rešpektuje - Carmichaelove čísla - složené č., ktoré prejdú testom

$$p \cdot q \cdot r \quad 3 \cdot 11 \cdot 17 = 561$$

- ako zistujeme prvočislnosť veľkých čísel: (treba vedieť)

- testy: Lehmanov test

Rabin-Millsov test

$$m \in \mathbb{N} \quad a_1, a_2, \dots, a_k - \text{všetky } i \in \mathbb{Z} < m, \text{ nesúdeliteľné s } m$$
$$k = \varphi(m)$$

$$a_1 \cdot x, a_2 \cdot x, \dots, a_k \cdot x \quad \text{kde } x \text{ je nesúdeliteľné s } m$$

- otázka: ďaleko môže platiť  $a_i \cdot x \equiv a_j \cdot x$ ?

ak  $a_i \neq a_j \Rightarrow x(a_i - a_j)$  deliteľné  $m$  - nemôže to mať miesto

$$a_i \cdot x \equiv a_j \cdot x$$

$$a_1 \cdot a_2 \cdots a_k \equiv a_1 \cdot x, a_2 \cdot x, \dots, a_k \cdot x \pmod{m}$$

$$a_1 \cdot a_2 \cdots a_k \equiv a_1 \cdot a_2 \cdots a_k \cdot x^k$$

$$1 \equiv x^k \pmod{m}$$

$$1 \equiv x^{\varphi(m)} \pmod{m} \quad \text{pre } x \text{ nesúdeliteľné s } m$$

obdoba malého Fermatovego vety

$$x^{\varphi(m)} \equiv 1 \pmod{m}$$

$$x \cdot x^{\varphi(m)-1} \equiv 1 \pmod{m}$$

$$x \cdot \underbrace{x^{-1}}_{\sim 2^{\varphi(m)}} \sim 2^{\varphi(m)} \cdot x \cdot x^{\varphi(m)-1} \equiv 1 \pmod{m} \quad \text{pre } x \text{ nesúdeliteľné s } m$$

$$n \in \mathbb{Z}_{\geq 0} \quad x^{-1} = x^{p-2}$$

- Rhozbyne ako Euklidov alg. - rozklad na povočísla - niekedy ľahko vypočítateľný

## RSA algoritmus

- patent expiroval 20.9.2000  $\Rightarrow$  voľne použiteľný

- postup: (500-1000b)

1. zvolime 2 veľké povočísla  $p, q$  - sújné

2. vypočítame  $n = p \cdot q$ ,  $n$  je verejné

3. vypočítame  $\varphi(n) = (p-1)(q-1)$ ,  $\varphi(n)$  musí ostáť sújné  $\varphi(n) < p(n)$

4. zvolime 2 veľké čísla  $e$  a  $d$  také, že  $e \cdot d \equiv 1 \pmod{\varphi(n)}$

5.  $e, n$  - verejný kľúč;  $d, n$  - sújny (rozšírený Eukl. alg.)

6. keďže nám ťifruje správa  $x$   $0 \leq x < n$ , takto  $y = x^e \pmod{n}$

7. my dešifrujeme  $y$ , takto  $x = y^d \pmod{n}$

- počet povočísel  $\leq n$  je  $\approx \frac{1}{\ln n}$

- berieme čísla, kt. sú velkou pravdep. povočísla

$\vdash$

$$\begin{array}{ll} x & b_0 \ b_1 \ b_2 \dots b_k - \text{bity} \\ x^2 \pmod{n} & b_0 \ b_1 \dots b_k = x^{2^0 b_0 + 2^1 b_1 + \dots + 2^k b_k} \\ x^4 \pmod{n} & b_2 \\ x^8 \pmod{n} & b_3 = x^{2^0 * x^{2^4} * x^{2^8}} \\ x^{16} \pmod{n} & b_4 \quad \text{násobím len riadky, kt. majú} \\ & \vdots \quad b_i = 1 \end{array}$$

niektoré  $b_i$  sú = 0

$$y^d = (x^e)^d \pmod{n} = x^{e \cdot d} \pmod{n} = x^{k \cdot \varphi(n) + 1} \pmod{n}$$

$$e \cdot d \equiv 1 \pmod{\varphi(n)} \quad x^{\varphi(n)} \equiv 1 \pmod{n}$$

$$\begin{aligned} e \cdot d &= k \cdot \varphi(n) + 1 \\ &= x \cdot x^{k \cdot \varphi(n)} \pmod{n} = x^{k \cdot \varphi(n) + 1} \pmod{n} = x \end{aligned}$$

- ak  $x$  je nesúdeliteľné s  $n$

- keby  $p \mid x \Rightarrow p \nmid x$ ,  $x$  je nesúdeliteľné s  $q$

$$\begin{aligned} x^{\varphi(p)} &\equiv 1 \pmod{p} = x^{\varphi(p) \cdot \varphi(q)} \equiv 1 \pmod{q} = x^{\varphi(p) \cdot \varphi(q)} \equiv 1 \pmod{q} = \\ &= x^{\varphi(p) \cdot \varphi(q)} \end{aligned}$$

$$x^{k \cdot \varphi(p) \cdot \varphi(q)} \equiv 1 \pmod{q}$$

$$x^{k \cdot \varphi(p) \cdot \varphi(q)} \equiv x \pmod{pq}$$

⋮

$$= x$$

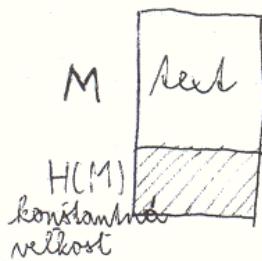
- vediet popis; rozšírený alg. nebude viedieť  
vedieť ho nesvetší

26.11.

Prednáška Č.8

## Jednocestné hash-funkcie

$n$  možnosti pre  $H(M)$



MAC  
FINGERPRINT

- dodatočná správa, aby sme vedeli, či  
medošlo k zmene

Vlastnosti  $H(M)$ : HASH

1. pre každú správu  $M$  je ľahké vypočítať  $H(M)$
2. pre každé  $H$  je ľahké nájsť  $M$  také, že  $H = H(M)$
3. pre každé  $M$  je ľahké nájsť iné  $M' \neq M$  také, že  $H(M') = H(M)$
4. je ľahké nájsť 2 rôzne správy  $M$  a  $M'$  tak, že  $H(M) = H(M')$

$\hat{=}$  COLISION RESISTANCE (v literatúre) - odolnosť voči kolíciám

- kolícia - 2 správy s rovnakou hodnotou hash

- ideom hľadať 2 správy tak, aby venikla kolízia

$$p_1 = 1 \quad p_2 = 1 - \frac{1}{2} \quad p_3 = 1 - \frac{2}{m} \quad \dots \quad p_k = 1 - \frac{(k-1)}{m}$$

- post., že nenašané kolízia      vyberiem 3 správy

$$P = 1 \cdot \left(1 - \frac{1}{m}\right) \cdot \left(1 - \frac{2}{m}\right) \cdot \left(1 - \frac{3}{m}\right) \cdots \cdot \left(1 - \frac{(k-1)}{m}\right)$$

$$= \prod_{i=1}^{k-1} \left(1 - \frac{i}{m}\right) \approx \prod_{i=1}^{k-1} e^{-\frac{i}{m}} = e^{\sum_{i=1}^{k-1} -\frac{i}{m}} = e^{-\frac{k(k-1)}{2m}}$$

$$e^{-x} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \frac{x^4}{4!} - \dots$$

veľmi malé

$$P = 1 - e^{-\frac{k(k-1)}{2m}} \quad - \text{post., že naxstane kolízia}$$

$$\approx \frac{1}{2}$$

$$k \approx \sqrt{2m \cdot \log \frac{1}{2}}$$

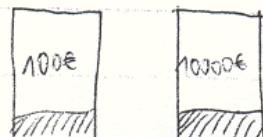
$\approx 1,17 \cdot \sqrt{m}$  - aspoň 2 majú rováký hash, ak  $k \approx 1,17 \cdot \sqrt{m}$

- narodeninový efekt

- 64b hash

- potom s dať  $2^{32}$  správ a vygenerujeme 2 správy s rovnakým hashom

- birthday attack



- ak elektronicky podpisujeme nejaký dokument, treba spraviť becvýmenu

## Hash pomocou kryptosystému



$$h_0 = IV \quad h_n = f(m_n, h_{n-1})$$

$$h_n = E_{k_{n-1}}(m_n) \oplus m_i$$

$$= E_{k_{n-1}}(m_n) \oplus m_i \oplus h_i$$

$$= E_{k_{n-1}}(m_n) \oplus h_{n-1} \oplus m_i$$

- 15 je bezpečných - nevýhoda vedeť

$$h_n = E_{m_n}(h_{n-1}) \oplus h_{n-1}$$

- najčastejšie používaná, výhoda sa pamäť

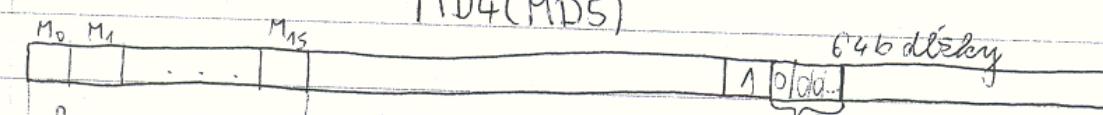
- dĺžka hashu a kľúča nemusí byť rovnaká

$$h_i = E_{m_n}(h_{n-1}) - nesmie sa používať, je prelomená$$

- nevhodné väčšie kryptografické ľahky

- mi - kriptovaný blok musí byť dosť dobre dlhý - 128b, 192b, 256b

## MD4(MD5)



chcem, aby celá správa bola dlhá k. 512b - pridám 0 medzi 1 a 64b blok

512b

vypočítam preto hash

$$1. A = 64452301 H$$

$$B = EFC DAB B89 H$$

$$C = 98 BADC F E H$$

$$D = 10325476 H$$

N - počet blokov rozšírenej správy

for i=0 to N/16-1

for j=0 to 15 maplin  $M_0, M_1, \dots, M_{15}$

$$AA := A \quad BB := B \quad CC := C \quad DD := D$$

ROUND 1

ROUND 2

ROUND 3

$$\text{ROUND 4} \quad A = AA + A \quad B = BB + B \quad C = CC + C \quad D = DD + D \quad + \text{mod } 2^{32}$$

- nedostatky v MD4, MD5  $\Rightarrow$  jmenovane - útok

riskosť niektorých kódov

- program - do 1 minúty nájde kolíziu

- neponával

- MD4 - 3 kola po 16 operácií

- MD5 - 4 kola po 16 operácií

### SHA-0

- 4 kola po 20 iterácií (80 iterácií na 512b blok)

- rábal siadne útoky v rozumnom čase

### SHA-2

- spracova sa 8 blokov v 1 kroku

- hash - 256b

### Digitálny podpis

odsklané:



príjemce:



desifrovanie

$$E_{KV}(Sig) = M$$

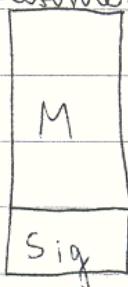
$$E_{KV}(E_{KT}(M)) = M$$

KV - kľúč verejný

KT - kľúč Časujú

- problém - správa môže byť veľmi veľká  $\Rightarrow$  podpis rovnako veľký ako správa

- riešenie:



$$D_{KT}(H(M)) = Sig$$

príjemec:



$$H(M) \stackrel{?}{=} E_{KV}(Sig)$$

ak sú rovnaké, potom

správa bola podpisaná  
správcom osobou

- nedá sa nájsť iná správa s rovnakým Sig a H(M)

- Ánočkov distribúcia kľúčov  $\Rightarrow$  certifikáty autorita ich vydáva, aj vrátaneich plasť

- chcem dokázati, že správa bola podpisana v tomto čase

## Systém časových snačiek



$$X = H(H(M), PUB)$$

hodnota, kt. nemohla byť známa dňu voľnosti

$$Y = \text{sig}_{K_T}(X)$$

- posle sa na certifikačnú autoritu