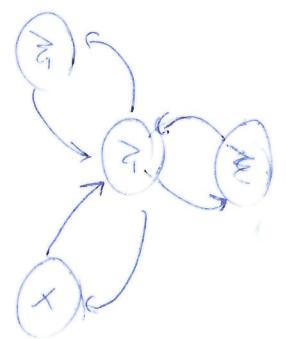


+  
+ 3  
+ R



Útok typu SQL injection a ohana potí němu.

Obráncení proti zájdelelkům systému

⇒ systém se interpretuje správcem, který nelze ovládat tímto cílenou

⇒ typicky ~ PHP ↗ MySQL

↘ MySQL:

⇒ nelze vložit typu SQL injekční ⇒ ak někdy správce redstavují v obehru systému

Tipy ochury:

- Sanitizace - neštěstí letanu miciel jule

- Least privilege princip

- Data validation

- Použití placeholcér

- DB Server má WANU? → Špatné?

- Default users

- Speciální bezpečné procedury ⇒ neštěstí privilegia

- Použít si mít své ochury



Útok typu DoS - Denial of Service a ohlaha jeho následků.

Cílem je mít systém nedostupný

- útok na stabilitu aplikací nebo OS
- útok na CPU, paměť, rozhraní sítě

Symptomy: nedostupnost služby / sítě

: místní nebo celá síť

: mít výjemu správ

Mají: PING of Death - datagram se fragmenty a offsety se nacházejí tak, aby byly v NETBIOS OOB - out of band - neobsahovaly žádat

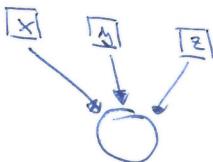
Nacházení dat a registrů ⇒ všechny objekty

Enumeration služeb nebo sítě ⇒ útok na to

Všechny objekty aloaci ⇒ zaplnění RAM

Spuštění programu v licencování

DDoS :



Důležité je sejmíka časování  
funkce ohnou je systém objevu písma

- Lepší linky
- Zastavení útoku u ISP
- Firewall
- Cache

⇒ otevírání portů a kanálům volání / přijímatelné

SYN Flood ohnou: Filtrace

Synacke

Firewall a proxy

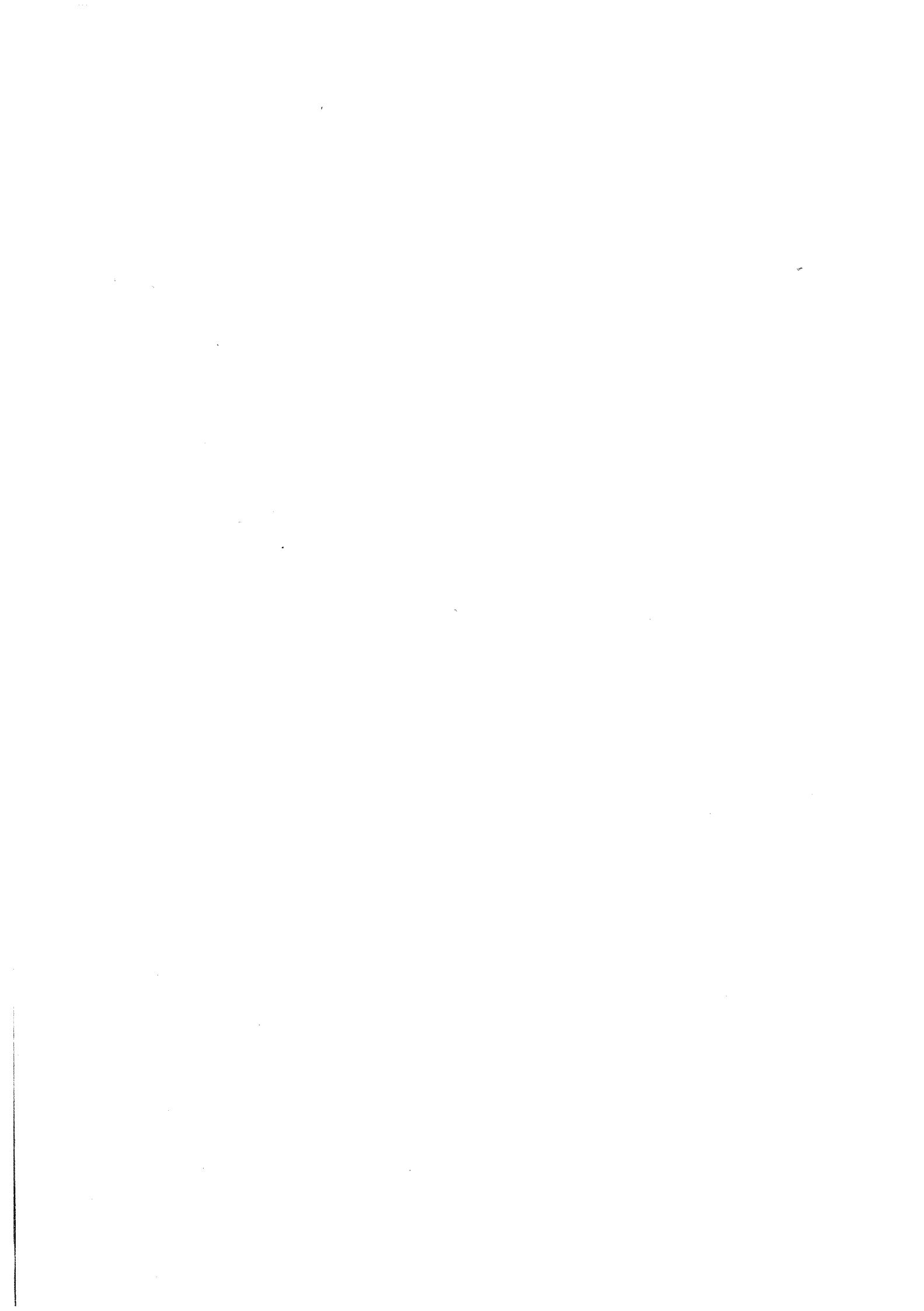
P2P útok ⇒ důležité kvalitativní DC++, aby způsobit nápor k různým

DNS amplification - false source IP

Permanent attacks ⇒ zničení HW typický flashováním FW

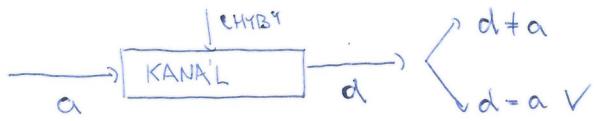
IDS a IPS ⇒ detection a prevention system

- detektace
- Signatury
- statistika



## PB 7.

Lineární kód - generuje a kontrolní matice a syndromy. (Matice a jenit.)

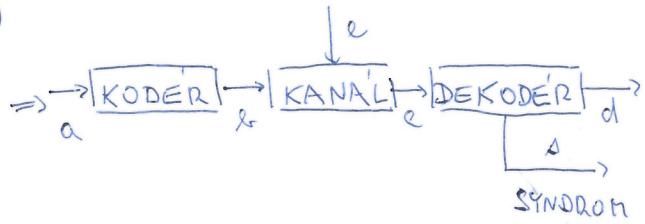


Kanál: Symetrický - kód (0→1) = kód (0-1)

Nesymetrický - II + II

Symetrický

Bez paměti - nezávislý  
s pamětí - závislý



Kód  $\Rightarrow$  převod  $a \rightarrow b$

$\Rightarrow$  několik funkci množin kód slouží

Slouží: informační část

kontrolní část

Vlastnosti:  $l_2$  - inf. obsah

$R = M/l_2$  = Redundance = součíti se 2 jednotky Shannon

$l_2/m = R/m$  - relativní měří

Kód  $\Rightarrow$  dva hody, které mají stejný řešení významu slova

- Blahý kód -  $(M, l_2)$ 
  - detekce chyb - detekční kód
  - korekce chyb - opravný kód
  - obecný - samokorekční kód

Hamming vzdálenost a) SLOV - počet odlišných bitů

b) KODOV - min vzdálenost  $(l_1, l_2)$  kde  $l_1 < l_2$  = kódov.

Vála slouží  $\Rightarrow$  počet mostech jednotek  $\Rightarrow$  vzdálenost  $(l_1, l_2) = \text{Mst}(l_1, l_2)$

Principy: dle ... poč. detekčních chyb

och ... poč. opravitelných chyb

a platí, že  $\text{och} \leq \text{dch}$

$\Rightarrow$  Detekce a dle  $\text{dch} < \text{kódov}$

$\Rightarrow$  Detekce a oprava chyb  $\text{dch} + \text{och} < \text{kódov}$

ZNAČENÍ - E C/D - correcting / detection

↓  
SINGLE, DOUBLE, TRIPLE, QUADRUPLE

KVD=4

0ch =	0	1
DEH =	3	2
1ch	D	X
2ch	D	D
3ch	D	X
4ch	N	N

← řízení  
korekce

Lineární kód : svedly mat. lin. vztahem  
- mst. V nad tělesem S

- monom
- associativa
- regr. slal.
- distributivita
- nejs. Osobnosti

$$\forall \text{ j} \in \text{nat} \text{ k} \in (\mathbb{F}_{q^k}) (\forall n \in V) \exists r \in V \\ (\forall m \in V) (\forall n \in V) \quad \text{m+n} \in V$$

$\Rightarrow$  lin. nezáv. vztahy mezi Bází  $\Leftrightarrow$  jiné obecné systémy LP

$$\text{Shálkni smysl} \Rightarrow \sum_{n \in V}$$

$\Rightarrow$  atog. dvojitého vztahu  $\Rightarrow$  nezáv. jiné bázové vztahy  $\nabla$

Lineární kód  $\Rightarrow$  sloučit triviální LP

Lýgající kód  $\Rightarrow$  dvojité lineární kód

GENERUJICÍ MATICE: G - rázový triviální vztah - triviální (gen.) mst.  $G^*$   
 $\Rightarrow \lambda = aG \dots$  tj. lineární kombinace rázové  
 $\nexists$  Kdlo generující matici je lineární  
 $\nexists$  Lin. kód je sloučením kódů gen. až jeho matici B  $\Rightarrow$  tj. má i bází  
 PŘÍDKY G jsou LN  $\nabla$

KONTROLNÍ MATICE: ~~H ... triviální mst. G\*~~ H ... tj. triviální atogujiční mst. k G\*  
 $\dots$  tj.  $GH^T = 0$   $\nabla$   
 $\forall c \in G^* \Rightarrow cH^T = 0$

SYNDROM:  $A = C^T H^T \dots$  charakter dle

Rázová matica H mohou být LZ  $\nabla$ . Ale mst. generuje  $H^* \perp G^*$

TVARY MATIC  $G = [I_k | F] \quad H = [-F^T | I_{m-k}]$   
 $\uparrow$  inf. obec.  $\uparrow$  redundance  $\begin{matrix} h & \left( \begin{matrix} | & G \\ | & \end{matrix} \right) & \left( \begin{matrix} | & H \\ | & \end{matrix} \right)_{m-k} \end{matrix}$   
 Polohu bázové GF(2)  $\Rightarrow \underline{F = -F^T}$

$\Rightarrow$  min. neopřímo sloučit sloučit ojnice po kódovém matici  $\nabla$ . PŘÍDKY

$$G = \begin{pmatrix} 11 & 110 \\ 10 & 101 \end{pmatrix} \Rightarrow G' = \begin{pmatrix} 10 & 101 \\ 01 & 011 \end{pmatrix} \Rightarrow H = \begin{pmatrix} 10 & 100 \\ 01 & 010 \\ 11 & 001 \end{pmatrix}$$

Příklad min. neopřímo sloučit sloučit ojnice po kódovém matici  $\nabla$   
 a příklad ojnice po kódovém matici  $\pi^{-1}$

EKVALENTNÍ KODY: Shálkni sloučit jiného kódu

DUALNÍ KODY: Kódová sloučit jiného kódu

$$H_1 \sim G_2^* \\ G_1 \sim H_2^*$$

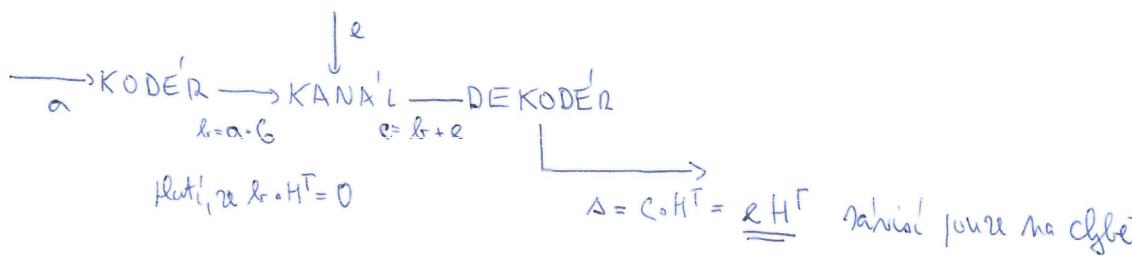
Upravmi řádku matice tak, aby byly všechny hodnoty ko jedn. matici  $I_8$ .  
 Pak ošlikyne (stup se sloupcem pěmitací).

Eliminalní řádky  $\Rightarrow$  řádky s nula v desetinové pěmitaci (složené řádky)

Dvojité řádky  $\Rightarrow$  řádky s dvěma nula v desetinové pěmitaci  $\Leftrightarrow G_1 = H_2 \quad G_2 = H_1$

Syndrom  $S = eH^T - cH^T = m - h$

- za první lin. nezáv. řádku  $H$



$\Rightarrow$  v HW implementaci je jaročky a XORy

$\Rightarrow$   $-1t$   $H$  je řádkový  $\Downarrow$   $\Rightarrow$  majíme mi SYNDRON

- ten řádek do delodku a hodnotu XORUJI

↑ ležíthen řádek dat

Lin. řádky  $\Rightarrow$  řádek = min. nula  $\neq 0$

Syndrom určuje řádky a řádkové matici je možné upravit

$\Rightarrow$  fázilní hodnota řádky je opnutá  $\Rightarrow$  SWAP jaročky?

$\Rightarrow$  Proč ten delodk?



## MI-PB 8

Typické kód - generátér polynom, kódování, detekce a ošetva chyb

Residuální polynom mod tělesem GF(2) :  $\ell(x) = c_{n-1}x^{n-1} + \dots + c_1x + c_0$   
 $\Rightarrow x \neq 0$  neznamá?

$\Rightarrow$  nerozdělitelný  $\Rightarrow$  nerozdělitelný maticí  $\Leftrightarrow$  neštoraří reprezentace  
 $\Rightarrow$  součástí scítání, odčítání  $\Rightarrow$  stupeň  $\leq n$   $\Rightarrow$  GF(2)  
 množením také, dělení je nerozdělitelný polynom

$$P(x) \% Q(x) = 0 \Leftrightarrow Q(x) | P(x)$$

$\Rightarrow$  stupeň polynomu je index resp. koeficientu  $\Rightarrow$  spec. množstvo 0

Nerozdělitelný polynom  $\Leftrightarrow$  nemají řadu dělitele nižší než  $c$  a  $P(x)$   
 $\Leftrightarrow$  nerozdělitelný množstvo

Nerozdělitelný množstvo  $\Rightarrow$  jednoznačný až na abstraktní množobly kmen 0

KONGRUENCE :  $\exists K(x) : P(x) = Q(x) + M(x) \circ K(x)$

$\downarrow$  algoritmus       $\downarrow$  dělitel       $\downarrow$  podíl

$\Leftrightarrow K(x) \equiv Q(x) \bmod M(x) \Leftrightarrow$  množstvo ekvivalence

$a \sim A(x) \dots$  kódování informací

$b \sim B(x) \dots$  množstvo kodování slov - identické se

$c \sim E(x) \dots$  množstvo cyklových slov

$c \sim C(x) \dots$  množstvo čteného data  $\Rightarrow c = b + e$

$\Rightarrow$  dělba schématu chyb  $\Leftrightarrow E(x) = E'(x) \circ \underbrace{x^j}_{\text{POSUV VEEVO}}$  až  $x^j E'(x)$

$$E(x) = \underbrace{0101100}_{x^2} \Rightarrow j=2$$

$$E'(x) \quad \deg E'(x) = 3$$

$$\Rightarrow \deg E(x) = 4$$

$E'(x) \dots$  tzv. schéma  
 $\deg E'(x) + 1 \dots$  délka schématu

### Kód generátor polynomů - 1. TYP

$$G(x) = q_1 x^k + \dots + q_0 \Rightarrow B(x) = A(x) \circ G(x)$$

$\downarrow$   
redundance

$\deg G(x) = k \dots$  redundance

$\max \deg A(x) + 1 = k \dots$  jiná data

$\max \deg B(x) + 1 = M$

$$a = 1010$$

$$b = 1011$$

$$1010 + 1011 = \begin{array}{r} 10100 \\ 1010 \\ \hline 11110 \\ 1010 \\ \hline 1001110 \end{array}$$

$$\begin{array}{r} 101000 \\ 1010 \\ \hline 1000100 \\ 1010 \\ \hline 1001110 \end{array}$$

$$b = x^6 + x^3 + x^2 + x$$

Jak na syndrom chyb?

$$C(x) = B(x) + E(x) \Rightarrow C(x) \% G(x) = \text{SYNDROM } \underline{S(x)}$$

$$\text{Příklad: } C(x) = 1000110 \quad G(x) = 1011$$

$$C(x)/G(x) = \underline{1011^2 + 11}$$

$$\begin{array}{r} 1000110 : 1011 = 1011 \\ | 001110 \\ | 0000 \\ | 1000 \\ | 0011 \end{array}$$

$\Rightarrow$  Zde zjistit schůzky dle délky maximální chyby  $L \leq n = 16 \deg G(x)$

$$\text{neži } G(x) = x^{16} + 1 \Rightarrow L \leq 16$$

$\rightarrow$  Kód generací množicemi je lineární!

$\rightarrow$  Generační matice?

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-1} \\ g_0 & g_2 & \dots & \\ \vdots & & & \\ g_0 & & \dots & g_0 \end{pmatrix} = \left( \begin{array}{cccc} g_n & g_{n-1} & \dots & \\ 0 & g_2 & g_{n-1} & \dots \\ 0 & 0 & \ddots & g_0 \end{array} \right) \quad \left. \begin{array}{l} M = n+2 \\ \text{rozdíl} = g_n \\ \max \text{ rozdíl} = M \end{array} \right\}$$

Kód generací polynomem - 2 TYP

$$B(x) = \underbrace{A(x) \cdot x^2}_{\text{SHIFT}} + \underbrace{A(x) \cdot x^2 \% G(x)}_{\text{SHIFT + MODUL}}$$

CYKLICKÝ KOD

$\Rightarrow$  Dáleží na jistém  $\Rightarrow$  cyklický jenž má dvojí slouž

$\Rightarrow$  Polynom je cyklický  $\Rightarrow$  je lineární

a	K <sub>1</sub>
00	000
01	011
10	101
11	110

Kód generací polynomem  $G(x)$  je cyklický - hledat  $(n, k)$   $\Rightarrow$  je lineární

$\forall$  Cyklický hledat, nebo jiné hledat je generací nějakého polynomu

$$\Rightarrow \text{neži: } |x^n - 1|$$

flamingo holds

$$\Rightarrow \text{Gram-Schmidt matrix } H = \begin{pmatrix} d^{m-1} & d^{m-2} & \dots & 1 \end{pmatrix} \quad \text{bij min. punts } \in GF(2^m)$$

$$\Delta = \mathbf{e}^\top \mathbf{H}^\top = \mathbf{e}^\top \mathbf{H}^T$$

What's mine's name's phone?

$$c = (c_{m-1}, \dots, c_0)$$

$\Delta = 0 \Leftrightarrow \lambda \in \text{hünen } C(x) \Leftrightarrow \underbrace{M_2(x)}_{\text{Gesamtfläche}} \mid C(x)$

$B(x) \dots$  irreducible polymer deg  $\geq 2$

... Rückt Polynom  $\Rightarrow P(z) \mid (z^k - 1)$  und  $(\prod_{j=1}^k (z - c_j)) \mid P(z) \mid (z^k - 1)$

$$\therefore n = \deg G(x) \text{ nach 8}$$

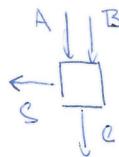
... n = card  $G(x)$  map 255

$$k_2 = m - n = 255 - 8 = 247 \Rightarrow G(x) \text{ generiert Hamming}(255, 247)$$



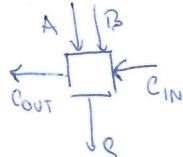
Sčítací a odčítací sčítání pomocí

Základ: jednočíselné sčítání

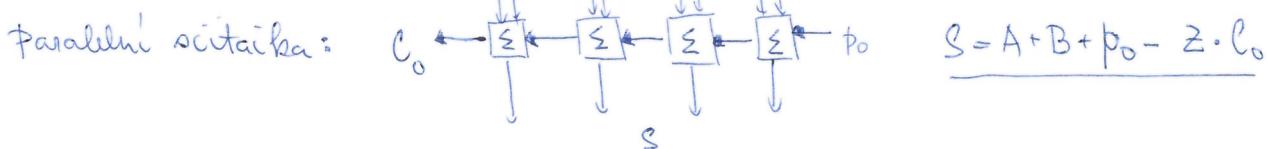
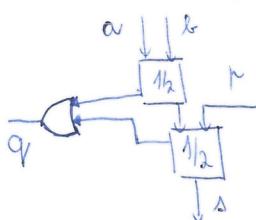


$$\begin{aligned} S &= A \oplus B \\ C &= A \oplus B \end{aligned}$$

úplně sčítání



přijde použití jednočíselného sčítání k násobnému sčítání



A	B	C <sub>IN</sub>	C <sub>OUT</sub>	S
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

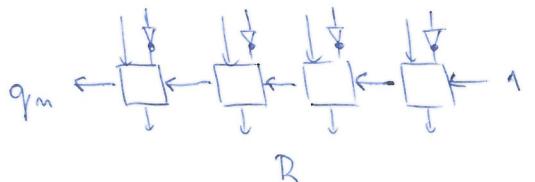
$$\begin{aligned} C_{\text{OUT}} &= AB + C(A \oplus B) \\ S &= A \oplus B \oplus C \end{aligned}$$

$\Rightarrow$  kódem lze ležky uložit na hodinách

ALE: kódovým písmenem

- Součinné odčítání - závědne výpočtu s řádkem a koňákem  
 $\Rightarrow$  nevliv

- ležky  $\Rightarrow$  množit sčítáním  $\Rightarrow$  POUŽIJEME DVOJKOVÝ DOPLNĚK



$$\begin{aligned} R &= A + (Z - B) - q_m Z = \\ &= A - B + (1 - q_m) Z \end{aligned}$$

$$q_m = 0 \Rightarrow A \leq B$$

$$q_m = 1 \Rightarrow A \geq B$$

$\Rightarrow$  výsledek v doplňkovém kódu

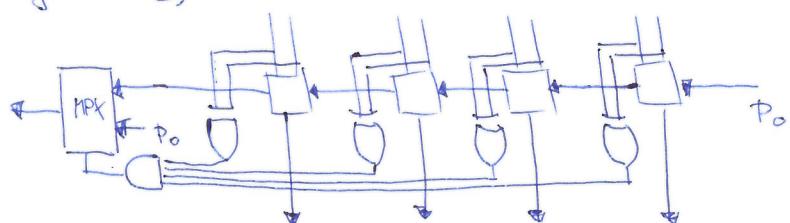
$\Rightarrow$  Sčítání s postupním sčítáním pomocí  $\Rightarrow$  musíme čelit až na ustálení!

$\Rightarrow$  řešitelné je oříšky  $\Rightarrow$  řešitelné jsou všechny i  $G_n = a_n^x b_n^x$   
 řešitelné jsou všechny i  $G_n = a_n^x \oplus b_n^x$

### SČÍTAČKA S VÝHÝBKAMI

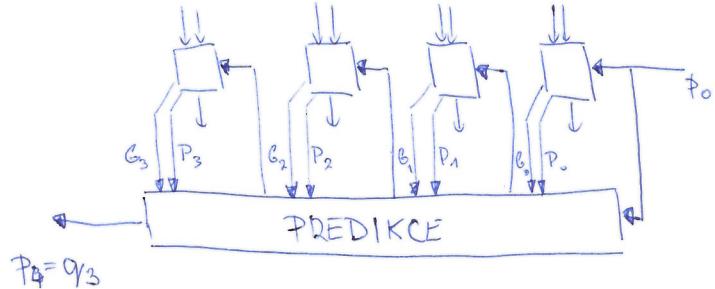
- sekvence mezi členy se nemohou dotýkat
- alespoň 3 sekvence

### SEKCE



$\Rightarrow$  jednoduché, když můžeme podle sekvencí takto souběžně

### SČÍTAČKA S PREDIKCI PRĚNOSU



$$P_0 = Q_3$$

$G_0 \rightarrow$  generuje se  $G_0 = a_0^x b_0^x$   
 $P_0 \rightarrow$  můžeme se  $P_0^x = a_0^x \oplus b_0^x$   
 $P_0 -$  gen. nebo přenáší  $P_0^x = a_0^x + b_0^x$

$$M_1 = G_0 + P_0 P_0$$

$$M_2 = G_1 + P_1 M_1 = G_1 + P_1 (G_0 + P_0 P_0)$$

$$M_3 = G_2 + P_2 M_2 = G_2 + P_2 G_1 + P_2 P_1 G_0 + P_0 P_1 P_2 P_0$$

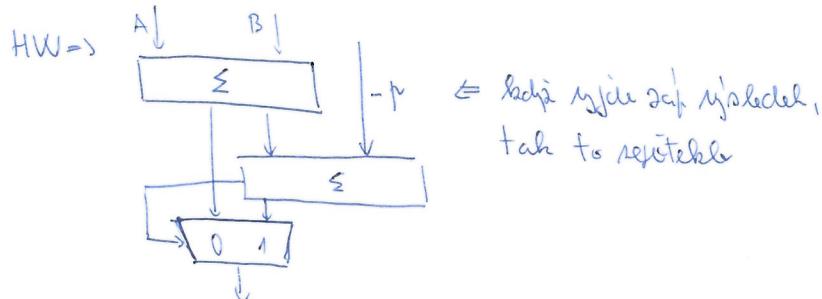
⋮

$\Rightarrow$  lze různé kombinace a hodnoty zvolit?

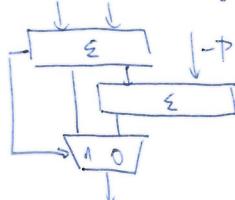
$\Rightarrow$  nelze je optimálně sekvencí obdržet?

HW a SW implementace operací nad konečnými tělesy  $GF(p)$  a  $GF(2^m)$ ,  
Scítání, násobení, inverze a dělení množine.

Scítání mod  $GF(p)$ : SW  $\Rightarrow$  systémy čísla a jednoduché sumace  
 $\Rightarrow$  jinoté součíty  $P$ , tak aby byly jen co potřeba



Odečítání nad  $GF(p)$ : SW  $\Rightarrow$  nášli stejně jen 2. operand v doslouchavém módu  
 HW  $\Rightarrow$  pouze doslouchající módu



Násobení nad  $GF(p)$ : SW  $\approx$  HW  $\Rightarrow$  most significant bit multiplication  
 $\Rightarrow$  T2N od rev. binu následující SHIFT and MULTIPLY

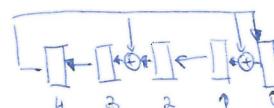
Scítání nad  $GF(2^p)$   $\Rightarrow$  Vždy XOR  $x_0 x_1 x_2 \dots$

Násobení nad  $GF(2^p)$   $\Rightarrow$  faktorial ne zvolení bude  $\Rightarrow$  Polynomální  $\times$  Numérní

$\Rightarrow$  pouze MSB multiplication

$\Rightarrow$  2 termů se lodičí ISFR  $A = A_0 \times \text{Mod } F(x)$

$$F(x) = x^5 + x^3 + x + 1$$



$\Rightarrow$  počítá modulo a shift

$\Rightarrow$  následující shift a následující A poslat je bit 1

$$C = 0$$

$$\text{for } i = m-1 \text{ to } 0$$

$$C = C \times \text{Mod } F(x) + A_i \cdot A$$

Umocněním  $\sim GF(2^p)$   $\Rightarrow$  2družství mezi  $a$  a  $A = (a_0, a_1, a_2)$

$\Rightarrow$  poly. linií?

$$A^2 = (a_0, a_1, a_2)^2 = a_0^2, a_1^2, a_2^2$$

$\Rightarrow$  polynom 0

Normální linií  $\{d^{2^0}, d^{2^1}, d^{2^2}, \dots, d^{2^{m-1}}\} \Rightarrow$  reprezentace něho nejdřívších polynomů

$\Rightarrow$  scítání  $\Rightarrow$  opět XOR

Umocněním  $\sim GF(2^p)$   $\Rightarrow$  Fermatova věta  $d^{2^p} = d$   
 $\Rightarrow$  Normální?

$$\Rightarrow A = (a_0, a_1, \dots, a_{m-1})$$

$$A^2 = (a_{m-1}, a_0, a_1, a_2, \dots, a_{m-2})$$



Násobení  $\sim$  normální linií  $C = A \times B$

$$C_0 = A \times B^T \quad M \dots \text{Multiplication matrix}$$

$$C = 0$$

for  $i = 0$  to  $m-1$

$$c_i = A \cdot M \cdot B^T$$

$$A = LSHIFT(A); \quad B = LSHIFT(B)$$

Inverze  $\sim$  normální linií  $\Rightarrow$  nelze použít EEA?

$\Rightarrow$  Fermatova malá věta  $a^{2^m} = a \Rightarrow a^{2^m - 2} = \bar{a}^{-1}$

Inverze  $\sim$  polynomické linií  $\Rightarrow$  EEA

$\Rightarrow$  Génerace mod  $GF(2^p)$

operace nad  $GF(p)$

BAZE	POLY	NORM
NEUTR. EL	0000000	0000000
IDENTITA EL	000001	111111
SCÍTANI	$\oplus$	$\oplus$
NAŠOBEŇI	MSB	MATICE
SQUARING	PROLOŽENÍ	SHIFT
INVERZE	EEA	FERM. V.

SCÍTANI	NAŠOBEŇI	INVERZE	NAŠOBEŇI A MODULO
			MSB
			EEA
			<del>SCÍTANI</del>
			NAŠOBEŇI

SQUARE AND MULTIPLY



exponent  $\sim$  2. Autore

a polynomická možnost

a  $\sim$  řídicí 1. = našobení

$\Rightarrow$  kdežo, ažden se zhlíží inverzi v GF(p) ... můžeme použít Montgomery Field

$\Rightarrow$  předne do MF  $\Rightarrow$  inverzne (BEZ INVERZE)  $\Rightarrow$  předne scít

$$\begin{aligned} \bar{a} &= |aR|_m & \bar{c} &= \bar{a} + \bar{b} = ||aR|_m + |bR|_m|_m & D &= 100 \quad m = 97 \\ \bar{c} &= |\bar{a} \bar{b} \bar{D}^{-1}|_m \Leftrightarrow c = |ab|_m & & & & \text{Např. některé možnosti} \\ a &= |\bar{a} \cdot \bar{D}^{-1}|_m & \bar{a} &= |aR|_m & & \text{sousty} \end{aligned}$$



Diskritní logaritmus - DH, El Gamal - Baby step Giant step, Pollardova Rho metoda, Pohling-Hellman a Index calculus

$\Rightarrow$  Výměna klicí => řešení se o vložení jednoznačnosti

$\Rightarrow$  možnost rychlejší řešení problemu  $\Rightarrow$  logaritmus není snadný

$G \dots$  grupa  $\Rightarrow g, h \in G \quad g^x = h \quad \times \dots$  diskritní logaritmus

$\Rightarrow$  & kružnice cyklické grupy  $G$  s generátorem  $g$  má několik řešení!

a) Kdysi hledalo řešení -  $g$  je řádu  $N \Rightarrow$  sloučitost  $O(n)$

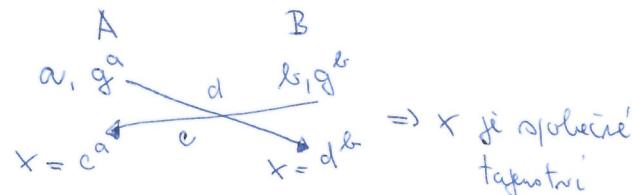
$\Rightarrow$  Isomorfismus mezi  $G$  a gen  $g$  řádu  $d$  je izomorfismus  $\mathbb{Z}_d^\times$

$\Rightarrow$  Je jichlo jich řešení, ktere  $g^x = h \dots$  jenž řešení hledané.

### Diffie Hellman

- používá se generátor  $g \in \mathbb{Z}_p^\times$

- ale obecně libovolná grupa



$\Rightarrow$  Použit řešení DLP, jehož můžeme DH

vyřešit v log. čase.

$\Rightarrow$  Řešit DHP nemůžete obdobněji než DLP

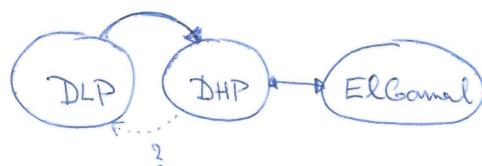
### El Gamal

- Zvolí se grupa a generátor  $g$ ,  $a$  je PRIV  $\Rightarrow A = g^a \dots$  PUBLIC

$\Rightarrow$  Druhá strana má efemerní klicí  $b \in \mathbb{Z}$   $c_1 = g^b \quad c_2 = m A^b$   
a poté řešit  $\Rightarrow$  ta řešit sítat  $(A^b)^{-1}$

$\Rightarrow$  Nežen  $c_1^a \dots \times$  a udělá inverzi  $\Rightarrow m = c_2 \cdot x = m A^b \cdot A^{-b} = m \quad QED$

opět můžeme vyřešit jenž řešení DLP v log. m ... m je řád generátora



### b) Baby-step - Giant-step

$\Rightarrow \text{DLP } \sim O(\sqrt{N})$  moch  $\rightarrow N$  je nicht geraden

$$M = 1 + \lfloor \sqrt{N} \rfloor$$

$$x, g, g^2, \dots, g^{m-1}$$

$$h, hg^m, hg^{2m}, \dots, hg^{(m-1)m} \Rightarrow \text{Maschine wählt nach } \Rightarrow g^{\hat{i}} = h \cdot g^{\hat{j}m}$$

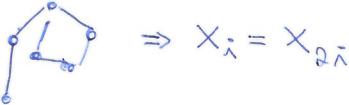
$\Rightarrow$  reine Punktjagd?

$$\Rightarrow \hat{i} + \hat{j}m = x$$

### c) Pollard's Rho Method

$\Rightarrow$  drei Menge melli' Polynomti

$$x_{i+1} = f(x_i) \Rightarrow \text{Maschine wählt } \Rightarrow \text{Maschine wählt } x_i$$



$\Rightarrow$  Schritt  $\sqrt{N}$  ... als bez Jagdi

$$x_{i+1} = f(x_i) = \begin{cases} g x_i & x_i \in S_1 \\ x_i^2 & x_i \in S_2 \\ h x_i & x_i \in S_3 \end{cases} \Rightarrow \text{P. c. t. h. n. m. l. i. n. e.}$$

$\Rightarrow$  drei Polynomti:  $\lambda, \alpha, \beta \Rightarrow x_{2i} = x_i \Leftrightarrow g^{\lambda} h^{\beta} = g^{\alpha} h^{\beta}$

$$\Leftrightarrow g^{\lambda-\beta} = h^{\beta-\alpha} \Leftrightarrow g^{\lambda-\beta} = h^{\alpha-\beta}$$

$$\Leftrightarrow \lambda-\beta = \alpha-\beta \bmod N \Rightarrow \text{Rückwärts}$$

hätzt ja je a je fo hatorr! :

### d) Chinese Remainder Theorem

$\Rightarrow$  keinheit, da je nicht ganz  $N$  je kleinere Zahl

$\Rightarrow$  periodenweise do folgen a stetig' slvne' problema

$$N = \prod m_i \Rightarrow x \equiv a_1 \bmod m_1, \dots, x \equiv a_n \bmod m_n \Rightarrow \text{CRT}$$

$$N = q_1^{e_1} \cdots q_k^{e_k}$$

$$1. \quad q_{i_1}^{-1} = g \frac{N}{q_1^{e_1}} \quad h_{i_1} = \frac{N}{q_1^{e_1}}$$

$$2. \quad \text{Resüne } q_{i_1}^{m_1} = h_{i_1}$$

$$3. \quad \text{Solvne' jumoci CRT} \quad x \equiv m_1 \bmod q_1^{e_1}$$

$$\vdots$$

$$x \equiv m_2 \bmod q_2^{e_2}$$

$\Rightarrow$  Existiert  $\hat{i}$  spätestens jdl problem und oblid a schrit se exponenti. ?

## 2) Index Calculus

$\Rightarrow$  efektívni násí DLP  $\sim$  grybil, kde bude řešit faktorom bári

1. Náhled  $\mathcal{S} = \{p_1, \dots, p_r\}$  = faktorai faire

$\Rightarrow$  kolik výsledku části  $\subseteq G$  lze sestrojiti sice jake možnosti fakturací bári?

2. Málbači sybreni  $d_{l,i}$ ,  $0 < l < N$

$\Rightarrow g^l$  a mále  $g^l = \prod_{i=1}^r p_i^{d_{l,i}}$   $\Rightarrow$  mále máložiduji  $\sim$  bári

$$l \equiv \sum \log_p p_i \pmod{N}$$

$\Rightarrow$  Právdu náhled jisté  $l$

OPAKOVJEME  $\Rightarrow$  alydu máložiduji  $\log_p p_i$  a sustavu

3. Výpočtu hruzence  $\log_p p_i$

4. Náhledi sybreni  $d_{l,i}$  a speciální  $\log^{-l} = \prod_{i=1}^r p_i^{d_{l,i}}$

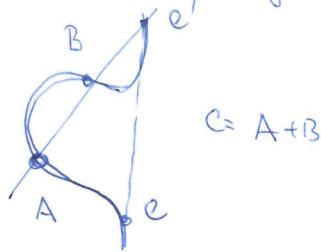
$$\Leftrightarrow \log^{-l} = \underbrace{\sum_{i=1}^r d_{l,i} \log_p p_i}_{\text{mále záležitosti}} + l \pmod{N}$$



Elliptické křivky - mají reálnémi čísla, mají GF, projektivní geometria, náleží MOV algoritmu

$$\text{EL nad } \mathbb{R} : y^2 = x^3 + ax + b \quad (x, y) \in \mathbb{R}^2 \text{ a } 4a^3 + 27b^2 \neq 0$$

= Spec. riad Weierstrassovy křivky



$\Rightarrow$  Křivka je singulární jenom na vnitří  
štítu, mimo řešení norma se zmenší

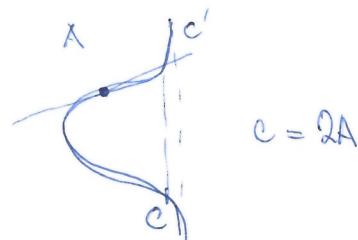
$\Rightarrow$  Štít Závěrečného bodu nebo křivky 0

a)  $P \oplus 0 = P$

b)  $P(Q_{11}, Q_{12}) \quad Q(Q_{11}, Q_{12})$

$$Q_1 = P_1 \text{ a } Q_2 = -Q_1 = P + Q = 0$$

c) Sečene formou množiny



Množina EL body traci s  $\oplus$  abelianou grupou.

Projektivní křivka : řadit 0 k řadě smíšené

$$\Rightarrow \text{P-křivka} = \mathbb{P}^3 - (0,0,0) \text{ a máži eliptické možnosti } x \sim y \Leftrightarrow (\exists z \in \mathbb{R}) (x = zy)$$

Projevy jsou  $(x_1, x_2, x_3)$  a jde o křivku  $\mathbb{P}^3$

$\nexists$  trojice (křivka) máži reprezentanci  $(x_1, x_2, x_3)$

$\Rightarrow$  „objevuje“ afimní křivku je součástí projektivní

$$\mathbb{R}^2 \subseteq \mathbb{P}^3 \Rightarrow (x_1, x_2) \rightarrow (x_1, x_2, 1)$$

$\rightarrow$  body a reprezentační jsou  $(x_1, x_2, 1)$  !

$\rightarrow$  výkladí to z lineární křivky a 3 parametry a z měsí zjednodušit 0

EC nad GF()

$$\text{náleží } \text{GF}(p^k) = \{(x, y) \mid x, y \in \text{GF}(p^k), y^2 = x^3 + ax + b\} + 0 \quad \checkmark \quad \text{②}$$

opět traci abelianou grupou a opět počítajte počet



Počet body na křivce :  $N_{E,p} = \# E(\text{GF}(p^k))$  kde  $a = p^k + 1 - N_A$

1.  $a^2 \leq 4p^k$

2.  $t^2 - at + p^k$  máži 2 kořeny  $\Delta = a^2 - 4p^k$

3.  $N_{E,p} = |\Delta - 1|^2 = p^k - t^2 - \Delta^2$

$$\Rightarrow p^k + 1 - 2\sqrt{p^k} \leq \# E(\text{GF}(p)) \leq p^k + 1 + 2\sqrt{p^k}$$

$$\Rightarrow \text{oleg' trvan } A^2 + a_1x_1 + a_3x_3 \neq x^3 + a_2x^2 + a_4x + a_6 \neq 0$$

$\Rightarrow$  je tu diskriminant  $\Delta$ , když  $\neq 0$  aby ne docházelo  
k singularitym

$$ECDLP : \text{problem } Q = mP$$

$\Rightarrow$  umíme Double and Add, ale ohřeje se?

$\Rightarrow$  Nelze použít index calculus? není fakturační bába?

Weilova párování  $\Rightarrow$  n následné problem do GF( $n$ ), zjistit a  
následné ocešetit.  $G[m]$  mácijsi množ. moli řády, když je delitelem m  
 $\Leftrightarrow \{g \in G \mid g^m = 1\}$

MOV algoritmus : Stupeň možnosti  $= E$  nad GF( $p$ ) a  $m \geq 1$  nedelitele p  
Stupeň možnosti  $E$  může být m již mohou byt i, i.e.  
 $E(GF(p^k))[m] \subseteq \mathbb{Z}_m^+ \times \mathbb{Z}_m^+$

Pokud je m násobek jeho vlastního řádu  $\Rightarrow$  Stupeň možnosti je 1  
j)  $n \equiv 1 \pmod l \Rightarrow$  možnost je l  
k)  $n \not\equiv 1 \pmod l \Rightarrow$  možnost je  $\frac{n}{l}$  nebo  $\frac{n}{l} + 1 \pmod l$   
Vše GF( $p$ ) a existuje kód řádu l

Princip MOV:  $E$  je EC nad GF( $p$ ) a  $P$  je jeho řádový kód řádu l.  $\exists$  je stupeň možnosti E může být l.  $Q$  je násobek P

1. Vypočti  $N = *E(GF(p^k))$  a násobek l | N  $\Leftrightarrow$  kód řádu je delitelem l
2. Zvol násobek  $T \in E(GF(p^k))$   $T \notin E(GF(p))$
3. Vypočti  $T' = \left(\frac{N}{l}\right)T$  a opakuji 2-3 while  $T' = 0$   
 $T'$  je kód řádu l
4. Vypočti Weilova párování  $L = e_L(P, T')$  a  $B = e_L(Q, T')$
5. Vypočti DLP kód L a B
6. Pak  $Q = mP$

Algoritmus je něčím pouze ne mohou využít stupeň možnosti.