ČERNÝ 87

Malá Fermatova věta
$a \in \mathbb{Z}$
$p \in \mathbb{P}$
$\gcd(a,p) = 1$
$a^{(p-1)} \equiv 1 \pmod p$
$|381^{152}|_{13}$ $p-1 = 12$
$= |(381^{12})^{12} \cdot 381^{8}|_{13}$
$= |(1)^{12^{12}} \cdot 381^{8}|_{13}$

Eulerova věta
- $a \in \mathbb{N}$
- $m \in \mathbb{N}$
- $\gcd(a,m) = 1$
- $a^{\varphi(m)} \equiv 1 \pmod m$

$|11^{32}|_{35}$ $\varphi(35) = 24$
$= |11^{24} \cdot 11^{8}|_{35}$
$= |1 \cdot 11^{8}|_{35}$

Eliptické křivky (ECC)
$E: y^2 = x^3 + ax + b$
- spojíme $P[x_P, y_P]$ a $Q \Rightarrow -R \Rightarrow R$
- $P + O = P$
  $P + (-P) = O$
  $O + O = O$
  $O = -O$
  $P + P = R$
- Výpočet R:
  - $x_R = |s^2 - x_P - x_Q|_p$
  - $y_R = |s(x_P - x_R) - y_P|_p$
- Tečna: $s = \left| \frac{3x_P^2 + a}{2y_P} \right|_p$
- Přímka: $s = \left| \frac{y_Q - y_P}{x_Q - x_P} \right|_p$
- #P = nejmenší r pro které $rP = O$
- #E = počet bodů na křivce
- $\frac{\#E}{\#P}$ = kofaktor, ideálně malý

Square & Multiply
$|6^{23}|_{13}$ $23 = 10111_2$

6^1	$\|_{13} = 6$	$\|_{13} = 6$
6^{10}	$\|_{13} = \|6^2\|_{13} = 10$	$\|_{13} = 10$
6^{101}	$\|_{13} = \|10^2 \cdot 6\|_{13} = 2$	$\|_{13} = 2$
6^{1011}	$\|_{13} = \|2^2 \cdot 6\|_{13} = 11$	$\|_{13} = 11$
6^{10111}	$\|_{13} = \|11^2 \cdot 6\|_{13} = 11$	$\|_{13} = 11$

Eulerova funkce (φ)
$\varphi(1) = 1$
$\varphi(p) = p - 1$
$\varphi(p^n) = p^n - p^{n-1} = (p-1) \cdot p^{n-1}$
$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \Leftrightarrow \gcd(x,y) = 1$

Exponenciální
$m \in \mathbb{P}$
$e \in \mathbb{N}$
$\gcd(e, m-1) = 1$
PDL

$c = |p^e|_m$
$p = |c^d|_m$
$d = |e^{-1}|_{m-1}$

Rozdělení šifer
- Klasické
  - Transpoziční
  - Substituční
    - Monoalfa – Hill, Caesar, Afinní
    - Polyalfa – Hill, Vernam, Vigenère, Exponenc.
- Proudové: A5/1, RC4, Salsa, Chacha
- Blokové: AES, Feistel (DES, 3DES)

Caesar
- substituční
- $c = |p + k|_{26}$
  $p = |c - k|_{26}$
- k = posun

Afinní
- substituční, s transformací
- $a, b \in \mathbb{Z}$; $\gcd(a, 26) = 1$
- $c = |ap + b|_{26}$
  $p = |a^{-1}(c - b)|_{26}$
  $p = |a^{-1}c + (-b \cdot a^{-1})|_{26}$
- Celkový počet klíčů $\varphi(26) \cdot 26 = 312$

Hillova
- $c_1 = |5p_1 + 17p_2|_{26}$
  $c_2 = |4p_1 + 15p_2|_{26}$
- $|c|_{26} = |A p|_{26}$
  $|p|_{26} = |A^{-1} c|_{26}$ proudová
- $A^{-1} = \frac{\text{adj } A}{\det A}$ $\gcd(\det A, 26) = 1$

Vernamova
- proudová
- abs. bezpečná
- keystream max 1x protože XOR

Transpoziční
- cílem difúze
- trans – permutace
- padding

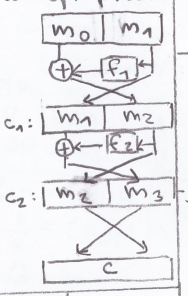
Vigenèrova
- polyalfa, subst, proud.
- víckrát Caesar
- $c_j = |p_j + k_{|j|_n}|_N$
- n – délka klíče
- N – velikost abecedy Z_N

IN: THELI
KEY: BRIDG
OUT: UYMOO

Vigenèrův autokláv
- asynchronní, samosynchronizace
- heslo 1 písmeno klíče, sčítání mod 26
- $h_1 = k$
  $h_i = c_{i-1}$
  $c_i = p_i + h_i$

AES
- bloková, NE feistel, klíč 128/192/256 b
- blok 128 b, rund 10/12/14
- pracuje s prvky Galoisova tělesa $GF(2^8)$
- výhodné na HW, přenosy do vyšších řádů nejsou, stačí XOR a mod
- SubBytes – nelineární operace
- Shift Rows – posun řádků o 0–3B
- Mix Columns – přenásobení sloupců, není v posl. runtě
- Add Round Key – na sloupce matice se XORuje rund. klíč

Feistel
$k = \{f_1, f_2, \ldots\}$, f nemusí být prosté
- 8b zpráva $m \in M$
  $m = (m_0 m_1)$
- Vytváříme novou
  $c_1 = (m_1 m_2)$
  $m_2 = m_0 \oplus f_1(m_1)$
  $c_2 = (m_2 m_3)$
  $m_3 = m_1 \oplus f_2(m_2)$



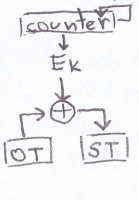
DES
- bloková
- feistel
- klíč 56+8 = 64b
- rund 16 – klíče po 48b
- blok 64b, 2x 32b
- S-box – jediný nelineární prvek

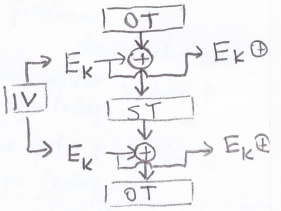
Triple DES
- klíč 56/112/168 b
- EDE: $E_{K3}(D_{K2}(E_{K1}(OT)))$

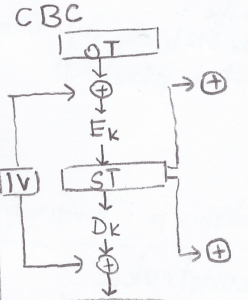
Diffie-Hellman
- PDL
- VK: m, a
- SK: k_A, k_B ; $\gcd(k, m-1) = 1$
- A pošle B svoje $Y_A = |a^{k_A}|_m$
  B pošle A svoje $Y_B = |a^{k_B}|_m$
- $K = |Y_A^{k_B}|_m = |Y_B^{k_A}|_m = |a^{k_A \cdot k_B}|_m$

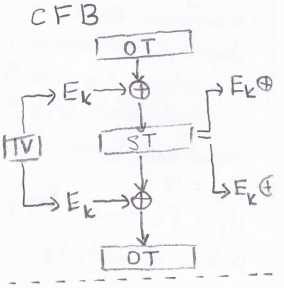
DH na ECC
- VK: křivka E (a,b,p) a bod P
- SK: k_A, k_B
  A pošle B svoje $Q_A = k_A P$
  B pošle A svoje $Q_B = k_B P$
- $Z = k_A Q_B = k_A(k_B P) = (k_A k_B) P$

Módy
ECB


CTR


OFB


CBC


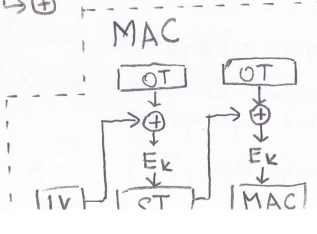
CFB


HMAC
- využívá SHA-x
- hashuje M ale i K
- ipad = b/8 bajtů = 0x36
  opad = b/8 bajtů = 0x5c
- b – velikost bloku v bitech
- K, K^+ = doplněný 0 zleva od MSB v případě, že $\log_2(K) < b$
- $HMAC_K(M) = H((K^+ \oplus opad) \,||\, H((K^+ \oplus opad) || M))$

Testování náhodných RNG
- Frekvenční – cca stejně 0 a 1
- Runs – zda délka po sobě jdoucích bitů je náhodná
- Hodnosti matice – odhalení lin. závislosti
- Spektrální – odhalení periodicity pomocí Fourierova
- Maurerův univerzální – výrazná komprimace

Blum-Blum-Shub PRNG
- $X_0 > 1$ = seed
- $X_{n+1} = X_n^2 \bmod m$
- p, q ≡ 3 (mod 4)
- $\gcd(\varphi(p-1), \varphi(q-1))$ by měl být malý
- i-tý prvek posl.:
  $X_i = \left(X_0^{2^i \bmod (p-1)(q-1)}\right) \bmod m$

BB84
- detekce odposlechu, polar. kód. fotonů
- Heisenbergův princip neurčitosti
- A generuje bin. posl., provádí polar. kód. dle báze
- B dekóduje bin. posl. dle svojí báze
- oznámí si navzájem báze → bity shody pro sym. klíč
- dobotování u bitů → prav. detekce odposlechu
  $1 - \left(\frac{3}{4}\right)^b$

MAC


RSA
- náročnost faktorizace $n = pq$
- $\gcd(e, \varphi(n)) = 1$
- $c = |m^e|_n$, $0 < c < n$
  $m = |c^d|_n$
  $d = |e^{-1}|_{\varphi(n)}$
- VK = (n, e)
  SK = (n, d)

RSA - CRT
- zrychlení šifrování - malá Hamming
- dešifrování - čvoz
- VK = (n, e)
  SK = (p, q, d_p, d_q, q_{inv})

čvoz
- p = 7, q = 11, n = 77, e = 13
- $\varphi(n) = 6 \cdot 10 = 60$
- $d = |e^{-1}|_{\varphi(n)} = |13^{-1}|_{60} = 37$
- $d_p = |d|_{p-1} = |37|_6 = 1$
- $d_q = |d|_{q-1} = |37|_{10} = 7$
- $q_{inv} = |q^{-1}|_p = |11^{-1}|_7 = 2$
- VK = (77, 13)
- SK = (7, 11, 1, 7, 2)
- $m_1 = |c^{d_p}|_p = |64^1|_7 = 1$
- $m_2 = |c^{d_q}|_q = |64^7|_{11} = 4$
- $h = |(m_1 - m_2) \cdot q_{inv}|_p = |(1-4)2|_7 = 1$
- $m = m_2 + hq = 4 + 1 \cdot 11 = \underline{15}$

Narozeninový paradox
$$P(N,k)_s = 1 - \frac{N!}{N^k (N-k)!}$$
N - počet dní
k - počet lidí
Pro $p = \frac{1}{2}$: $k \approx \sqrt{2N \ln(2)}$

Posuzování spolehlivosti
- nějaký ŠT
- nějaký ŠT + nějaký OT
- nějaký ŠT + vybraný OT
- vybraný ŠT + odpovídající OT
- vybraný ŠT + vybraný OT

Rabin-Miller (prvočíselnost)
- p = 21, a = 5
- (p-1) = 20
$P(p \text{ je prvočíslo}) = 1 - (\frac{3}{4})^k$
$(5^{20} - 1) \equiv 0 \pmod{21}$
$(5^{10} - 1)(5^{10} + 1) \equiv 0 \pmod{21}$
$(5^5 - 1)(5^5 + 1)(5^{10} + 1) \equiv 0 \pmod{21}$

Vlastnost	SHA-1	256	384	512
Délka hashe	160	256	384	512
Délka zprávy	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Vel. bloku	512	512	1024	1024
Vel. slova	32	32	64	64
Počet rund	80	64/80	80	80
Bezpečnost	80b	128b	192b	256b

Generátor grupy
- pokud má g, je cyklická
- $|g^a|_p = b$, $g < p$
- $b \in \langle 1, p-1 \rangle$

LGG - Lineární kongruenční generátor
- PRNG, není kryptograficky bezpečný
- X_0 = seed
- $X_{n+1} = (aX_n + c) \bmod m$, $m > 0$ (často mocnina 2)
- a = násobitel, c = inkrement

RC4
- Algoritmická proudová
- Pokaždé nový klíč
- Klíč 40/128 b

IN	OUT	MUX
00, 11	-	Deskriptor
01	0	
10	1	

A5/1
- synchronní, proudová
- klíč 64b, rámec 228b
- 3x LFSR
- Taktovací bity CCU: $R_1[8]$, $R_2[10]$, $R_3[10]$
- Posun majoritních dle CCU
- $k_i = R_1[18] \oplus R_2[21] \oplus R_3[22]$

El - Gamal
- vychází z DH a PDL
- šifrování i digitální podpis
- nesoudělná prvočísla g, m $1 < g < m$
- k_A: $0 < k_A < m$
- $y_A = |g^{k_A}|_m$ SK: k_A VK: (m, g, y_A)
- $K = |y_A^{k_B}|_m = |(g^{k_A})^{k_B}|_m$
- $c = |p \cdot K|_m$
- ŠT = (y_B, c)
- $p = |c \cdot K^{-1}|_m$
- Pro každou zprávu nový y!

chaCha
- proudová
- vyšší rozptyl než Salsa20
- lichá/sudá QR na sloupa/diagonály

PS	PS	PS	PS
K	K	K	K
K	K	K	K
C	C	N	N

Salsa 20
- bitové sčítání $\oplus$ XOR
- 32b sčítání $\boxplus 2^{32}$ políček 4x4
- rotace $\lll_d$, $d = \{7, 9, 13, 18\}$
- výstupem 64b keystreamu
- ARX (Add - Rotate - XOR)
- lichá/sudá QR na sloupa/řádky

PS	K	K	K
K	PS	N	N
C	C	PS	C
K	K	K	PS

Distribuce VK
- zveřejnění na net
- veřejný adresář - 3. str
- autorita - podepisuje VK svým VK
- certifikace CA

Křížová certifikace
- A chce komunikovat s B, pošle mu:
- $C_{A1}(A)$
  $C_{A1}(C_{A1})$ - kořenový CA
  $C_{A2}(CA_1)$ - křížový CA

Hashování
$h: X \to \{0,1\}^n$
- jednosměrnost
  1. typu: náročnost inv. op. ($y \to pq$)
  2. typu: znalost padacích vrátek (klíče)
- orákulum - na totožný vstup odpovídá stejným výstupem
- náhodné o. - na nový vstup odp. náhodným výběrem z množiny výstupů
- bezkoliznost
  1. řádu: můžu zvolit oba vstupy, počet op. pro 50%: $2^{\frac{n}{2}}$
  2. řádu: 1 vstup mám, hledám 2., počet op. pro 50%: 2^n

Entropie
- množství informace ve zprávě,
- míra náhodnosti

$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i$
$H(X) = \frac{1}{4} \cdot \log_2(\frac{4}{1}) + \frac{3}{4} \cdot \log_2(\frac{4}{3})$
- maximální = $\log_2 n$, pokud $p = \frac{1}{n}$
- minimální = 0 při $p_1 = 1$
- N = délka zprávy
- $R_N = \frac{H(X)}{N}$ = obsáznost jazyka (prům. ent.)
- $R = \log_2 L$ = abs. obsáznost, L = 26
- $D = R - r$ = nadbytečnost, D = 4,7 - 1,5 = 3,2
- $\frac{100D}{R}$ = bitů nadbytečnosti v %
- $S_U = \frac{H(K)}{D}$ = vzdálenost nadbytečnosti

AES-192 s kódováním UTF-32:
H(K) = 192
R = 32
D = 32 - 1,5 = 30,5
$S_U = \frac{192}{30,5} \approx 6,3$

Hodnocení odolnosti
- Určena vnitřní strukturou šifry (nelineární prvky, délka klíče)
- Kerckhoffsův princip - bezpečnost založena na klíči, ne utajení šifry
- Teoretická - při splnění podmínek v praxi těžké splnit
- Nepodmíněná - nelze prolomit bez ohledu na prostředky
- Absolutní - pokud opakováním šifry nezíská nové info (Vernamova, NE asymetrická)
- Podmíněná - prolomení vyžaduje prostř., které nemáme
- LProkazatelná - mat. dok., NP těžký
- LVýpočetní - prolomení trvá dlé, než životnost informace

Damgard - Merklova konstrukce
- kompresní fa f, kontext H_i, blok zpr. M_i
- doplnění (zarovnání) hashe
  - bitem 1 a poté 0 do 512b, aby zbylo 64b
  - posledních 64b = počet b původní M
- iterativní konstrukce
  $H_0 = IV$
  $H_i = f(H_{i-1}, M_i)$
- pokud je hash fa bezkoliziní, je i kompresní

Davies - Meyerova konstrukce
- zesiluje kompresní fci XORem vzoru před výstupem
$H_i = f(H_{i-1}, M_i) = E_{M_i}(H_{i-1}) \oplus H_{i-1}$

Autentizace - zajišťuje totožnost uživatele (MAC)
Nepopiratelnost - nelze popřít původ (digit. podpis)
Důvěrnost - utajení dat (proud. + blok. šifry)
Integrita - data nedotčena, neznměněna (MAC)
Konfúze - ztížení určení způsobu transformace
Difúze - rozptýl informace po celém textu
Polyalf. subst. - stejný symbol, jiná záměna
Monoalf. sub. - stejný symbol, stejná záměna
Polygraf. šifry - záměna víceznakových bloků
Monograf. šifry - záměna jednoho znaku
Synchronní proud. š. - heslo nezávislé na OT a ŠT
Asynchronní proud. š. - heslo závislé na OT nebo ŠT, samosynchronizace
Qubit - kvantový bit - měřením získáme 1 stav (1b informace), zničíme superpozici