RSA

Init:
1. zvolíme prvočísla $p \neq q$
2. zvolíme e aby $\mathrm{nsd}(e, \phi(n)) = 1$
3. dorátame d aby $ed \equiv 1 \pmod{\phi(n)}$

public: (n, e), private: d

Šifrovanie:
$E(m) = m^e \bmod n$

Dešifrovanie:
$D(c) = c^d \bmod n$

Bezpečnosť:
- vieme faktorizovať $\to$ rozbijeme RSA
- vieme $\phi(n) \to$ vieme faktorizovať
- vieme $d \to$ položíme $m = ed - 1$, potom m je násobok $\phi(i)$, kým platí $\forall a \in Z^*; a^m \equiv 1$ ho delíme 2, potom s pp 1/2 je $\mathrm{nsd}(n, a^{m/2} - 1)$ faktor.
- zdieľané $n \to$ vieme rozbiť svoje n, a teda aj n niekoho iného
- $|p - q|$ je malé $\to$ vyskúšame a je
- $p - 1$ má len malé prvoč. faktory $\to$ zvolíme K ako vhodný násobok malých prvoč., bude $(p-1)|K$, preto pre náh. a je $a^K \equiv 1 \pmod p$, pravdep. $a^K \not\equiv 1 \pmod q$, preto $\mathrm{nsd}(n, a^K - 1)$ je faktor.
- malý priestor správ $\to$ vyskúšame $\forall$
- malé $e \to$ stačí odchytiť správu poslanú e ľuďom
- malé $d \to$ dá sa nejako
- takmer CCA: ak niekto podpíše $\forall$ čo mu pošleme, vieme si dekryptovať $E(m)$: dáme podpísať $r \cdot E(m)$, on nevie čo podpisuje
- bezpečnosť posledného bitu: keby sme ho vedeli, vieme rozbiť RSA

ElGamalov systém

Init:
1. zvolíme verejné prvočíslo p a generátor g grupy $(Z_p \setminus \{0\}, \cdot)$
2. každý užívateľ zvolí $x \in_R \{1, \ldots, p-2\}$, spočíta $y = g^x \bmod p$

public: (p, g, y), private: x

Šifrovanie:
1. zvolí sa $k \in_R \{1, \ldots, p-2\}$
2. $E(m) = (g^k, my^k)$

Dešifrovanie:
$D(c_1, c_2)$: spočítame $a = c_1{}^x (= g^{kx})$, potom $m = c_2 a^{-1}$

Bezpečnosť:
- ekviv. s Diffie-Hellmannovým problémom: z g^a, g^b určiť g^{ab}
- najviac tak ťažké ako DLOG
- nesmie sa prezradiť k, y^k
- nerecyklovať k
- môžu sa sharovať p, g

Pohlig-Hellmannov alg.

máme $p - 1 = q_1^{e_1} \ldots q_k^{e_k}$, chceme rátať $x = DLOG_g y \pmod p$

porátame $x \bmod q_k^{e_k}$, z toho a čínskej zv. vety vieme x

hľadajme $x \bmod q^e$ v tvare $\sum_{i=0}^{e-1} a_i q^i$

platí: $y^{(p-1)/q} \equiv x^{a_0(p-1)/q} \pmod p$, z toho brute-force dorátame a_0, upravíme $y' = yx^{-a_0}$ a pokračujeme odznova určiť a_1, atď.

Vyplýva z toho, že pre $p = 2^s t$ vieme posledných s bitov $DLOG$u

Rabinov systém

Init:
1. zvolíme prvočísla $p, q \equiv 3 \pmod 4$

public: $n = pq$, private: (p, q)

Šifrovanie:
$E(m) = m^2 \bmod n$

Dešifrovanie:
nájdeme odmocniny mod p a mod q, z čínskej zv. vety máme 4 odmocniny, nejako určíme, ktorá je dobrá (odmocnina z c je $c^{(p+1)/4} \pmod p$)

Bezpečnosť:
- ekviv. s faktorizáciou
- CCA útok: zvolíme si m, dáme si dešifrovať m^2, s pp=1/2 dostaneme dve odmocniny, z kt. sa dá spočítať faktor
- dá sa pridať vhodný padding

Goldwasser-Micali

Init:
1. zvolíme prvočísla $p, q \equiv 3 \pmod 4$
2. zvolíme $y \in QNR_n$

public: $(n = pq, y)$, private: (p, q)

Šifrovanie:
rozbijeme správu na bity, pre $m_i \in \{0, 1\}$ zvolíme $x \in_R Z_n^*$, potom $E(m_i) = x^2 y^{m_i}$

Dešifrovanie:
- test či $c \in QR_n$: pozri, či $c^{(p-1)/2} \equiv 1$

Bezpečnosť:
- najviac tak ťažký ako faktorizácia

BBS generátor

Init:
1. zvolíme prvočísla $p, q \equiv 3 \pmod 4$, nech $n = pq$
2. zvolíme $x \in_R Z_n^*$, nech $x_0 = x^2 \bmod n$
3. zostrojíme $\{x_i\}_{i \geq 0}$: $x_{i+1} = x_i^2 \bmod n$
4. zostrojíme $\{b_i\}_{i \geq 0}$: $b_i = x_i \bmod 2$

Šifrovanie:
rozbijeme správu na bity, pre $m_i \in \{0, 1\}$ je $E(m_i) = m_i \oplus b_i$, navyše pošleme $x_{|m|}$

Dešifrovanie:
vieme $p, q \to$ vieme odmocňovať x_i, práve 1 zo 4 odmocnín bude QR_n

Chaum-van Heijst-Pfitzmann hash

nech $p = 2q + 1$ sú prvoč., g, c generátory v $(Z_p \setminus \{0\}, \cdot)$

$h : (Z_q \times Z_q) \to (Z_p \setminus \{0\})$

$h(x_1, x_2) = g^{x_1} c^{x_2} \bmod p$

- ak vieme nájsť kolíziu, vieme $DLOG_g c$

Predĺženie hash fcie

nech $h : \{0, 1\}^m \to \{0, 1\}^t$, $m \geq t + 2$

nasekáme správu x na úseky x_i dĺžky $m - t - 1$, posledný doplníme paddingom (tvaru 10..0), rátame:

$h_1 = h(0^{t+1} \| x_1)$

$h_2 = h(h_1 \| 1 \| x_2)$

…

$h^*(x) = h_n = h(h_{n-1} \| 1 \| x_n)$

ak h je odolná voči kolíziám, aj h^* je

MAC

message authentication code

cieľ: zabezpečiť integritu správy

pošleme $(m, h_K(m))$ (h je hash, K kľúč)

vhodná h_K: $h_K(m) = h(K \| pad \| m \| K)$, kde pad je dohodnutý padding, aby to bolo dosť dlhé

RSA podpis. schéma

podpisujeme D, overujeme E

podpisuje sa hash správy, aby sme zabránili random message forgery (z dvoch podpísaných podpísaný súčin)

ElGamal podpis. schéma

Init ako pri šifrovaní

Podpisovanie:
1. zvolí sa $k \in_R \{1, \ldots, p-2\}$
2. vypočítame $r = g^k \bmod p$, dorátame s tak, aby $H(m) = (xr + ks) \bmod p - 1$

podpis: (r, s)

Overovanie:
1. pozrieme, či $1 \leq r < p$
2. overíme, či $y^r r^s \equiv g^{H(m)} \pmod p$

Bezpečnosť:
- ak by sme neoverili 1., vieme z 1 podpisu vyrobiť podpis ľub. správy – dorátame vhodné r
- viacnásobné k vedie k prezradeniu k a následne súkr. kľúča
- podpisuje sa hash kvôli forgery

DSA podpis. schéma

Init:
1. p, q prvoč., $q | p - 1$
2. zvolí sa $h \in_R \{2, \ldots, p-2\}$, doráta $g = h^{(p-1)/q}$, musí $g > 1$, potom rád g je q
3. používateľ zvolí $x \in_R Z_q^*$, doráta $y = g^x \bmod p$

private: x, public: (y, p, q, g)

Podpisovanie:
1. zvolí sa $k \in_R \{1, \ldots, q-1\}$
2. vypoč. $r = (g^k \bmod p) \bmod q$
3. $s = k^{-1}(H(m) + xr) \bmod q$
4. ak $rs = 0$, odznova

podpis: (r, s)

Overovanie:
Spočítame: $w = s^{-1} \bmod q$

$u_1 = H(m) w \bmod q$, $u_2 = rw \bmod q$

overíme, či $(g^{u_1} y^{u_2} \bmod p) \bmod q = r$

Slepé podpisy

podpisujúci nevie čo podpisuje, dá sa tak napr. modifikovať RSA

Diffie-Hellmann protokol

úloha: dohodnúť session key

vopred známe: p, generátor g

A si zvolí α, B zvolí β

$A \to B$: g^α

$B \to A$: g^β

kľúč je $g^{\alpha\beta}$

Útoky:
Eva: musí vedieť riešiť DH problém

Oscar: uspeje (podvedie oboch)

Station-to-station protokol

modifikácia DH, máme od TA vydané certifikáty na podpisy A, B

$A \to B$: g^α

$B \to A$: $g^\beta, E_k(sign_B(g^\alpha, g^\beta)), C(B)$

$A \to B$: $E_k(sign_A(g^\alpha, g^\beta)), C(A)$

$(k = g^{\alpha\beta})$

Útoky:
Eva: musí vedieť riešiť DH problém

Oscar: nemá ako zasiahnuť

Interlock protokol

úloha: sťažiť v DH situáciu Oscarovi

$A \to B$: g^α

$B \to A$: g^β

A zvolí m_A, B zvolí m_B

A spočíta $E_k(m_A)$, B spočíta $E_k(m_B)$

$A \to B$: polovica bitov $E_k(m_A)$

$B \to A$: polovica bitov $E_k(m_B)$

$A \to B$: zvyšok

$B \to A$: zvyšok

A, B si overia prenos m_A, m_B secure cestou

Útoky:
Eva: musí vedieť riešiť DH problém

Oscar: teoreticky môže oklamať jedného, ak zvládne narušiť aj posledný krok

Shamirov 3-prech. protokol

treba E, D aby $E_a(D_b(x)) = D_b(E_a(x))$

$A \to B$: $E_{k_1}(x)$

$B \to A$: $E_{k_2}(E_{k_1}(x))$

$A \to B$: $D_{k_1}(E_{k_2}(E_{k_1}(x))) = E_{k_2}(x)$

Útoky:
- xor nie je dobrá funkcia

Oscar: vie sa tváriť ako B

Wide Mouth Frog

používame timestampy T_x, trusted autoritu T, kľúče KX medzi X a T

$A \to T$: $A, \{T_A, B, K\}_{KA}$

$T \to B$: $\{T_B, A, K\}_{KB}$

Útoky:
- nonces nezafungujú
- dá sa rozbíjať kľúč a počas toho si refreshovať timestampy, riešenie je rôzny formát posielaných správ v 1. a 2. kroku

ZO SYLABOV CHÝBA

- Yahalom + ďalšie haluzné protokoly
- útoky proti nim a BAN logika
- konštrukcia HMAC
- neinteraktívne dôkazy
- overiteľné zdieľanie tajomstva
- elektronické voľby
- symetrické šifry

©MišoF. 2003

Needham-Schroeder protokol

T je TA, N_x sú nonces

$A \to T$: A, B, N_A

$T \to A$: $\{N_A, B, K, \{K, A\}_{KB}\}_{KA}$

$A \to B$: $\{K, A\}_{KB}$

$B \to A$: $\{N_B\}_K$

$A \to B$: $\{N_B - 1\}_K$

Útok:
útočník rozbije K, začne od 3. kroku a presvedčí B o autenticite K

Opravený NS protokol

$A \to B$: A

$B \to A$: $\{A, N_B\}_{KB}$

$A \to T$: $A, B, N_A, \{A, N_B\}_{KB}$

$T \to A$: $\{N_A, B, K, \{K, N_B, A\}_{KB}\}_{KA}$

$A \to B$: $\{K, N_B, A\}_{KB}$

NS Public-Key

$A \to B$: $\{N_A, A\}_{KB}$

$B \to A$: $\{N_A, N_B\}_{KA}$

$A \to B$: $\{N_B\}_{KB}$

session key: $f(N_A, N_B)$

Útok:
1. $A \to E$: $\{N_A, A\}_{KE}$

1'. $E(A) \to B$: $\{N_A, A\}_{KB}$

2'. $B \to E(A)$: $\{N_A, N_B\}_{KA}$

2. $E \to A$: $\{N_A, N_B\}_{KA}$

3. $A \to E$: $\{N_B\}_{KE}$

3'. $E(A) \to B$: $\{N_B\}_{KB}$

Interakt. dokaz. systémy

prover P neobmedzený, verifier V polynomiálny pravdepodobnostný, ak $x \in L$, V skoro určite akceptuje, inak skoro určite neakceptuje

IDS je zero-knowledge, ak z prepisu komunikácie P a V nevieme zistiť nič, čo by sme bez nej nevedeli, formálne ak $\exists S$, ktorý bude generovať rovnaké komunikácie (resp. computational zero knowledge, ak je výstup S v BPP nerozlíšiteľný od komunikácie od komunikácie)

ZK dôkaz pre NIG

máme dva grafy G_1, G_2, P chce presvedčiť G, že nie sú izomorfné

protokol: veľa kôl:
1. V dá challenge $\varphi(G_i)$
2. P nájde j aby $G_j \sim \varphi(G_i)$
3. ak $i \neq j$, sú izom. $\Rightarrow V$ rejectne

ZK dôkaz pre IG

detto že sú izomorfné

protokol: veľa kôl:
1. P zverejní $G = \varphi(G_i)$
2. V dá challenge j, chce izomorfizmus G a G_j
3. P mu ho nájde

(Feige-)Fiat-Shamir

Sú známe $x_1, \ldots, x_k$, tvrdíme, že vieme ich odmocniny $u_i \pmod n$

P zvolí $v \in_R Z_n$, zverejní $y = v^2 \bmod n$

V zvolí $c_1, \ldots, c_k \in \{0, 1\}^k$, zverejní

P zverejní $z = v \cdot \prod u_i^{c_i}$

V overí $z^2 \equiv y \cdot \prod x_i^{c_i} \pmod n$

Shamirova secret-sharing schéma

n ľudí, treba t z nich, aby mali secret s

Zostr. polynóm f stupňa $< t$ tak, aby $f(0) = s$

i-ty človek dostane $(i, f(i))$

Útoky:
- ak 1 klame, zrekonštruujú zle, on si to vie opraviť
- riešenie: obmedzenie voľby s na menší interval, aj keď $t - 1$ podvádza, posledného neoblbnú

Blakleyho secret-sharing schéma

share: nadrovina v E_t

Ideálna schéma

$S(P_i)$ – možné shary pre P_i

K – priestor secretov

$\rho_i = \frac{\lg |K|}{\lg S(P_i)}$, $\rho = \min \rho_i$

Pre perfektnú schému $\rho \leq 1$, ideálna je ak $\rho = 1$

Chaffing & Winnowing

posielame správy, k nim MAC kódy, pomedzi to posielame balast s random bitmi namiesto MAC kódu, cenzor nevie, ktoré správy sú závažné

Bit commitment

máme $f : \{0, 1\} \times X \to Y$ takú, že:
- z $f(v, r)$ nevieme určiť v
- nevieme r_0, r_1 aby $f(0, r_0) = f(1, r_1)$

napr. $f(v, r) = H(v \| r)$

Použitie:
máme bit v, hodíme si x, zverejníme $f(v, x)$, tým sa zaviažeme k v, hocikedy môžeme zverejniť x a dokázať to

Oblivious transfer I

A má secret s, B ho môže dostať, A nemá vedieť, či ho B má
1. A zvolí p, q, pošle $n = pq$
2. B zvolí $u \in Z_n^*$, pošle $z = u^2 \bmod n$
3. A pošle B niektorú odmocninu z
4. s pp=1/2 vie B faktorizovať

Oblivious transfer II

A má secrety $s_1, \ldots s_n$, B môže dostať 1, A nemá vedieť, ktorý

A má verejnú fciu E, tajnú D
1. A zverejní náhodné $x_1, \ldots x_n$
2. B zvolí náh. a, poráta $v = x_i \oplus E(A)$, pošle v
3. A spočíta hodnoty $y_j = D(v \oplus x_j) \oplus s_j$, zverejní y_j
4. B si zoberie y_i a spočíta s_i

Dámy porovnávajú vek

A má i rokov, B má j

A má funkcie E (public), D (private)
1. B si zvolí veľké x, spočíta $k = E(x)$, pošle $k - j$
2. A vyp. $y_l = D((k - j) + l)$ pre $l \leq 100$
3. A zvolí $p \ll x$, vyp. $z_l = y_l \bmod p$ (musí byť $\forall u, v; 0 < z_u < p - 1$ a $|z_u - z_v| \geq 2$, inak gen. nové p)
4. A zverejní $z_1, \ldots, z_i, z_{i+1} + 1, \ldots, z_{100} + 1, p$
5. B overí $z_j \equiv x \pmod p$