Kriptosistem

 \mathcal{B} ...besedila $\mathcal{C} \dots kriptogrami$ $\mathcal{K}\dots$ ključi $\mathcal{E} = \{E_k : \mathcal{B} \to \mathcal{C}; k \in \mathcal{K}\} \dots \text{ kodirne f.}$ $\mathcal{D} = \{D_k : \mathcal{C} \to \mathcal{B}; k \in \mathcal{K}\} \dots \text{dekodirne f.}$

Za vsak $e \in \mathcal{K}$ obstaja $d \in \mathcal{K}$

$$D_d(E_e(x)) = x \quad \forall x \in \mathcal{B}$$

Vsaka kodrirna funkcija $E_k \in \mathcal{E}$ je injektivna.

Produkt kriptosistemov

Naj bosta $S_1 = (\mathcal{B}_1, \mathcal{C}_1, \mathcal{K}_1, \mathcal{E}', \mathcal{D}')$ in S_2 $(\mathcal{B}_2, \mathcal{C}_2, \mathcal{K}_2, \mathcal{E}'', \mathcal{D}'')$ kriptosistema za katera je $\mathcal{C}_1 = \mathcal{B}_2$.

$$S_1 \times S_2 = (\mathcal{B}_1, \mathcal{C}_2, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D})$$

$$E_{(k_1,k_2)}(x) = E''_{k_2}(K'_{k_1}(x))$$

$$D_{(k_1,k_2)}(y) = D'_{k_1}(D''_{k_2}(y))$$

Prevedljivost kriptosistemov

Kripto sistem S = (B, C, K, E, D) je prevedljiv na S' = $(\mathcal{B},\mathcal{C},\mathcal{K}',\mathcal{E}',\mathcal{D}'),$ če obstaja $f:\mathcal{K}\to\mathcal{K}',$ da za vsak $k\in\mathcal{K}$

$$E_k = E'_{f(k)} \qquad D_k = D'_{f(k)}$$

Tedaj pišemo $S \to S'$.

Kriptosistema sta **ekvivalentna**, če velja $S \to S'$ in $S' \to S'$

Tedaj pišemo $S \equiv S'$.

Idempotentnost kriptosistemov

Kriptosistem S je idempotenten, če

$$S \times S \equiv S$$

Klasični kriposistem so vsi idempotentni.

Klasični kriptosistem

Cezarjeva šifra

$$\begin{split} \mathcal{B} &= \mathcal{C} = \mathcal{K} = \mathbb{Z}_{25} \\ E_k(x) &\equiv x + k \mod 25 \\ D_k(y) &\equiv y - k \mod 25 \end{split}$$

Substitucijska šifra

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}, \quad \mathcal{K} = S(\mathbb{Z}_{25})$$

Ključ je permutacija $\pi \in \mathcal{K}$

$$E_k(x) = \pi(x)$$

$$D_k(y) = \pi^{-1}(y)$$

Afina šifra

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}, \quad \mathcal{K} = \mathbb{Z}_{25}^* \times \mathbb{Z}_{25}$$

Ključ $(a,b) \in \mathcal{K}$

$$K_{(a,b)}(x) = ax + b \mod 25$$

$$D_{(a,b)}(y) = a^{-1}(y-b) \mod 25$$

Vigenerjeva šifra

$$\mathcal{B} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{25}^n$$

Ključ $k \in \mathcal{K}$

$$K_{\underline{k}}(\underline{x}) = \underline{x} + \underline{k} \mod 25$$

$$D_k(y) = y - \underline{k} \mod 25$$

Permutacijska šifra

Simbolov ne nadomeščamo, ampak jih premešamo

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}^n, \quad \mathcal{K} = S_n$$

$$K_{\pi}(\underline{x}) = \underline{x}_{\pi(1)} + \dots + \underline{x}_{\pi(n)}$$

$$D_{\pi}(\underline{x}) = \underline{x}_{\pi^{-1}(1)} + \dots + \underline{x}_{\pi^{-1}(n)}$$

Hillova šifra

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}^n, \quad \mathcal{K} = \{ A \in \mathbb{Z}_{25}^{n \times n} | \det(A) \in \mathbb{Z}_{25}^* \}$$

Ključ je matrika $A \in \mathcal{K}$

$$K_A(\underline{x}) = A\underline{x} \mod 25$$

 $D_A(y) = A^{-1}y \mod 25$

Bločne šifre

Kripotsistem $(\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ je bločna šifra dolžine n, če je $\mathcal{B}=\mathcal{C}=\Sigma^n,$ kjer je Σ končna abeceda.

Vsaka kodirna funkcija je ekvivalentna neki permutaciji Σ^n , njena dekodirna funkcija pa inverzu te permutacije.

Afina bločna šifra

$$\Sigma = \mathbb{Z}_m$$

$$\mathcal{K} = \left\{ (A, \underline{b}); \ A \in \mathbb{Z}_m^{n \times n}, \det(A) \in \mathbb{Z}_m^*, \underline{b} \in \mathbb{Z}_m^n \right\}$$

$$E_{(A,\underline{b})}(\underline{x}) \equiv A\underline{x} + \underline{b} \mod m$$

$$D_{(A,\underline{b})}(\underline{x}) \equiv A^{-1}\underline{x} - \underline{b} \mod m$$

Iterativne šifre

Sestavlia iih

- \bullet razpored ključev: Naj bo K ključ. K uporabimo za konstrukcijo krožnih ključev (K^1, \ldots, K^{N_r}) temu seznamu pravimo razpored ključev.
- krožna funkcija: ima dva argumenta: tekoče stanje in krožni ključ:

$$w^r = q(w^{r-1}, K^r)$$

Da je dešifriranje možno mora biti q injektivna za vsak fiksen ključ K; tj. $\exists q^{-1}$:

$$g^{-1}(g(w,K),K) = w \quad \forall w, K$$

 \bullet šifriranje skozi N_r podobnih krogov: Besedilo xvzamemo za začetno stanje w^0 :

$$y = g(g(\dots g(g(x, K^1), K^2) \dots, K^{N_r - 1}), K^{N_r})$$

• dešifriranje:

$$x = g^{-1}(\dots g^{-1}(g^{-1}(y, K^{N_r}), K^{N_r-1})\dots, K^1)$$

Substitucijsko-permutacijsko omrežje (SPN)

je iterativna bločna šifra kjer je $\Sigma \, = \, \{0,1\}, \; \ell,m \, \in \, \mathbb{N}$ in $\mathcal{B} = \mathcal{C} = \Sigma^{\ell m}$

- substitucije: $\pi_s \in S(\Sigma^{\ell})$ S-škatla - zamenja ℓ bitov z drugimi biti
- permutacije: $\pi_p \in S_{\ell m}$ P-škatla - zamenja ℓm bitov z drugimi biti

Oznaka za delitev na zloge dolžine ℓ :

$$x = x_1 x_2 \dots x_m, \quad |x_i| = \ell$$

Kodiranje:

$$\begin{array}{l} w^0 = b \\ \mathbf{z}\mathbf{a} \ r = 1, \dots, N_r - 1: \\ u^r = w^{r-1} \oplus K^r \ / / \operatorname{primasamo} \ \mathbf{K} \\ \mathbf{z}\mathbf{a} \ i = 1, \dots, m: \\ \underline{v}_i^r = \pi_s(\underline{u}_i^r) \ / / \operatorname{substitucija} \operatorname{zlogov} \\ w^r = v_{\pi_p}^r(1), \dots, v_{\pi_p}^r(\ell m) \ / / \operatorname{permutacija} \operatorname{bitov} \\ / / \operatorname{zadnji} \operatorname{krog} \\ u^N r = w^N r^{-1} \oplus K^N r \\ \mathbf{z}\mathbf{a} \ i = 1, \dots, m: \\ \underline{v}_i^N r = \pi_s(\underline{u}_i^N r) \\ w \mathbf{m}i \ c = v^N r \oplus K^N r^{+1} \ / / \operatorname{beljenje} \end{array}$$

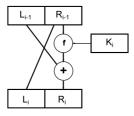
Dekodiranje:

$$\begin{split} &v_r^N = c \oplus K^{N_T+1} \\ &za \ i = 1, \dots, m; \\ &\underline{u_i^{N_T}} = \pi_s^{-1}(\underline{v_i^{N_T}}) \\ &za \ r = N_T - 1, \dots, 1; \\ &w^T = u^T \oplus K^{T+1} \\ &v^T = (w_T^T - 1)^T, \dots, w_{T-1}^T (\ell m) \\ &za \ i = 1, \dots, m; \\ &\underline{u_i^T} = \pi_s^{-1}(\underline{v_i^T}) \\ &b = u^1 \oplus K^1 \end{split}$$

Feistelova šifra

je bločna iterativna šifra dolžine 2t za abecedo $\Sigma = \{0, 1\}$. N_r je št. krogov, K^1, \ldots, K^{N_r} razpored ključev, ki ga dobimo iz ključa K in $f_K: \Sigma^t \to \Sigma^t$ je Feistelova kodirna

En krog kodiranja:



Kodiranje

$$\begin{split} L_0 &= \text{leva polovica } b \\ R_0 &= \text{desna polovica } b \\ za & i = 1, \dots, Nr \text{:} \\ L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f_{K_i}(R_{i-1}) \\ c &= R_{N_T} \|L_{N_T} \end{split}$$

DES in AES

TO-DO!

Tokovne šifre

Besedilo b razdelimo na bloke $b = b_1 \dots b_t \in \mathcal{B}^t$ Imamo zaporedje (tok) ključev: $z_1, z_2, \dots \in \mathcal{K}$. Kodiranje

$$za \ j = 1, \dots, t:$$
 $c_j = E_{z_j}(b_j)$
 $c = c_1 c_2 \dots c_t \in C^t$

Dekodiranje

$$\begin{aligned} \mathbf{z} \mathbf{a} & j = 1, \dots, t : \\ b_j &= D_{\mathbf{Z}_j}(c_j) \\ b &= b_1 b_2 \dots c_t \in \mathcal{B}^t \end{aligned}$$

Aditivne tokovne šifre

Naj bo (G, +) grupa, $\mathcal{B} = \mathcal{C} = \mathcal{K}$ in z_1, z_2, \ldots tok ključev Kodiranje

$$E_{z_i}(b_i) = b_i + z_i$$
$$D_{z_i}(c_i) = c_i - z_i$$

Samokodirna šifra

$$\mathcal{B} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$$

Začetni ključ izberemo $z_1 \in \mathbb{Z}_{26}$

$$z_i = b_{i-1}$$
 za $i > 1$

Kodiranje

$$E_{Z_i}(b_i) = b_i + z_i$$

Dekodiranje

$$D_{Z_i}(c_i) = c_i - z_i$$

Vermanova šifra

 $\mathcal{B} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$, ključ izberemo naključno. Kodiranje

$$E_k(b) = b \oplus k$$

Dekodiranje

$$D_k(c) = c \oplus k$$

To je pravzaprav Vigenerjeva šifra, le da ima ključ enako dolžino kot besedilo

Uporabimo kratko seme za generiranje dolgega toka psevdonaključnih bitov, ki jih uporabimo za ključ.

Linearna rekurziyna šifra

je sinhrona tokovna šifra, pri kateri je

$$\mathcal{B} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_s$$

zaporedje ključev z linearno rekurzinvo enačbo reda m s konstantnimi koeficienti nad Z_s:

$$z_i = c_1 z_{i-1} + c_2 z_{i-2} + \dots + c_m z_{i_m} \mod s$$

Zaporedju lahko priredimo polinom:

$$C(x) = 1 + \sum_{i=1}^{m} c_i x^i \mod s$$

Kodiranje/Dekodiranje:

$$E_{z_i}(x_i) = x_i + z_i \mod s$$
$$D_{z_i}(y_i) = y_i - z_i \mod s$$

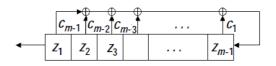
Perioda LFSR reda m je največ $2^m - 1$

Red nerazcepnega polinoma f(x) je najmanjši t, da $f(x)|x^t-1.$

Če ima LFSR nerazcepen karakteristični polinom reda t, potem ima LFSR periodo t.

Pomični register z linearno povratno zanko

V pomičnem registru je na začetku inicializacijski vektor $(z_1z_2\ldots z_m)$ (ključ).



Na vsakem koraku izpišemo z_1 register pomaknemo v levo Naj bo $B = \alpha^b \mod p$ in $A = \alpha^a \mod p$. Potem zadnji bit z_m pa izračunamo kot z c_1, \ldots, c_m uteženo vsoto. Če poznamo z_0, \ldots, z_{2m-1} , lahko rešimo sistem:

$$\begin{bmatrix} z_0 & z_1 & \dots & z_{m-1} \\ z_1 & z_2 & \dots & z_{m-2} \\ \vdots & \vdots & & \vdots \\ z_{m-1} & z_m & z_m & z_m \end{bmatrix} \begin{bmatrix} c_m \\ c_{m-1} \\ \vdots \\ \vdots \end{bmatrix} = \begin{bmatrix} z_m \\ z_{m+1} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \end{bmatrix}$$

Če smo pravilno uganili red m ima sistem enolično rešitev.

Asimetrična kriptografija RSA

n = pq kjer sta p in q različni veliki praštevili. $m = \varphi(n) = (p-1)(q-1)$

Potem je kriptosistem podan z:

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_n$$

$$\mathcal{K} = \{n\} \times \mathbb{Z}_m^*$$

$$E_{(n,e)}(x) \equiv x^e \mod n$$

$$E_{(n,d)}(y) \equiv y^d \mod n$$

e mora biti tuj m

Kodirnemu ključu (n, e) pripada dekodirni ključ (n, d), kjer je $d = e^{-1} \in \mathbb{Z}_m^*$

Problem diskretnega logaritma

Naj boGmultiplikativna grupa. Za dana $\alpha,\beta\in G,$ kjer je red elementa α enak n, je treba poiskati takšen $x \in$ $\{0, \dots, n-1\}$, da je

$$\alpha^{\omega} = \beta$$

Številu x rečemo diskretni logaritem elementa β z osnovo α . zgoščevalna funkcija odporna na trke.

Shanksov algoritem (veliki korak - mali korak)

whod:
$$G \text{ grupa, } \alpha, \beta \in G, \ n = \operatorname{red}(\alpha)$$

 $i s hod: \ x = \log_{\alpha} \beta$
 $m = \lceil \sqrt{n} \rceil$
 $z a \ j = 0, \dots, m-1:$
 $(j, \alpha^{m-j}) \to L_1$
 $u \operatorname{red} i \ L_1 \text{ po drugi komponenti}$
 $z a \ i = 0, \dots, m-1:$
 $(i, \beta \alpha^{-i}) \to L_2$
 $u \operatorname{red} i \ L_2 \text{ po drugi komponenti}$
 $poisci \ (j, y) \in L_1 \text{ in } (i, y) \in L_2$
 $x = (mj + i)$

Diffie-Hellmanova izmenjava ključev

- Alenka in Bojan se dogovorita za veliko praštevilo p in $\alpha \in \mathbb{Z}_n^*$, ki ima velik red n.
- Alenka si izbere naključno število $a \in \{1, \dots, n-1\}$, izračuna $A = \alpha^a \mod p$ in pošlje A Bojanu.
- Bojan si izbere naključno število $b \in \{1, \dots, n-1\},$ izračuna $B = \alpha^b \mod p$ in pošlje B Alenki.
- Alenka in bojan vsak zase izračunata skupni tajni ključ $K = \alpha^{a\bar{b}} = A^b = B^a$

Varnost temelji na težavnosti diskretnega logaritma.

Zaradi možnosti napada srednjega moža je pri izmenjavi ključev nujna avtentikacija!

ElGamalov kriptosistem

- Alenka in Bojan izmenjata tajni ključ k z Diffie-Hellmanovo shemo
- \bullet Alenka želi poslati sporočilo x. Izračuna kriptogram $y = k \cdot x \mod p$ in ga pošlje Bojanu.
- Bojan izračuna $x = k^{-1} \cdot y \mod p$

Formalna definicija:

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_p^*$$
 $\mathcal{K} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$
 $E_{(a,B)}(x) \equiv B^a \cdot x \mod p$
 $D_{(b,A)}(y) \equiv A^{p-b-1} \cdot y \mod p$

kodirnemu kjluču (a, B) ustreza dekodirni ključ (b, A).

Zgoščevalne funkcije

Zgoščevalna funkcija besedilu poljubne dolžine kratek izvleček.

Želene lastnosti:

- Naključnost: Če se dve sporočili razlikujeta na enem samem mestu morata povzetka izgledati kot neodvisno izbrani naključni števili.
- ullet Odpornost praslik: za poljuben izvleček z je računsko nemogoče poiskati sporočilo x, ja je h(x) = z. Oz. zgoščevalna funkcija je enosmerna. • Odpornost drugih praslik: za dano sporočilo x
- je nemogoče najti drugo sporočilo x', ki ima enak • Odpornost na trke: računsko je nemogoče poiskati

dve različni sporočili x in x' z enakim povzetkom. Trk je par različnih sporočil z enakim povzetkom

Tipična zgoščevalna funkcija

• Komprsijska funkcija: $f: \{0,1\}^{r+n} \to \{0,1\}^n$

• Zgoščevalna funkcija: $h: \{0,1\}^* \to \{0,1\}^n$

Zgoščevalna funkcija iterativno kliče kompresijsko funkcijo
$$H_0=IV$$
 za $i=1,\ldots,t:$ $H_i=f(H_{i-1}\|x_i)$ $h(x)=H_t$

Tukaj je IV začetno stanje, x_i pa so bloki besedila.

Na konec besedila dodano nekaj bitov, ki popisujejo dolžino besedila in toliko ničel, da se besedilo lahko razdeli na enako

Če je kompresijska funkcija odporna na trke, je tudi

Digitalni podpisi

Formalno je sistem na digitalno podpisovanje peterka $(\mathcal{B}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$, kjer je

- B končna množica sporočil
- A končna množica podpisov
- K končna množica ključev
- \bullet za vsak ključ $K \in \mathcal{K}$ obstaja algoritem za podpisovanje in preverjanje podpisa

$$\begin{split} & \mathrm{sig}_K \in S, \qquad \mathrm{sig}_K : \mathcal{B} \to \mathcal{A} \\ & \mathrm{ver}_K \in S, \qquad \mathrm{ver}_K : \mathcal{B} \times \mathcal{A} \to \{\mathrm{true}, \mathrm{false}\} \end{split}$$

Algoritem za podpisovanje je znan le podpisniku.

Podpisovanje z algoritmom RSA

Naj bosta p,q praštevili in n=pq. Naj bo(n,d) zasebni in (n, e) javni ključ. Potem za K = (n, e, d) definiramo:

$$\label{eq:sig} \begin{split} \operatorname{sig}_K(x) &= x^d \mod n \\ \operatorname{ver}_K(x,y) &= (\operatorname{true} \iff x = y^e \mod n) \end{split}$$

ElGamalov sistem za digitalno podpisovanje Generiranje ključa

Naj bo p takšno praštevilo, ja je v $\mathbb Z$ težko izračunati diskretni logaritem in $\alpha \in \mathbb{Z}_n^*$ primitivni element.

Potem je $\mathcal{B} = \mathbb{Z}_p^*$, $\mathcal{A} = \mathbb{Z}_p^* \times \mathbb{Z}_{p-1}$ in $\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv$ $\alpha^a \mod p$.

Število a je zasebno. Števila p, α in β pa so javna.

Podpisovanie

Podpisnik s ključem $K=(p,\alpha,a,\beta)$ izbere naključno skriteo število $k \in \mathbb{Z}_{n-1}^*$ in določi

$$\operatorname{sig}_K(x,k) = (\gamma, \delta)$$

kjer je

$$\gamma \equiv \alpha^k \mod p$$

$$\delta \equiv (x - a\gamma)k^{-1} \mod p$$

Preverianie podpisa

Za to potrebujemo p, α in β , ki so javni:

$$\operatorname{ver}_K(x, \gamma, \delta) = \left(\operatorname{true} \iff \beta^{\gamma} \gamma^{\delta} \equiv_p \alpha^x \right)$$

Digital Signature Standard (DSA) Generiranje ključa

- $\bullet\,$ Izberi 160-bitno praštevilo q
- Izberi 1024-bitno praštevilo p, da q|(p-1)
- \bullet Izberi element $h \in \mathbb{Z}_p^*$ in izračunaj $\alpha = h^{(p-1)/q}$ $\operatorname{mod} p$; ponavljaj dokler $\alpha \neq 1$. (α je generator natanko določen ciklične grupe red $q \vee \mathbb{Z}_{p}^{*}$
- Izberi naključno naravno število a < q
- Izračunaj $\beta = \alpha^a \mod p$
- Janvi ključ osebe A je (p, q, α, β) , zasebni pa a.

Opomba: red α, β, γ je enak q.

Podpisovanje

- \bullet Izberi naključno naravno število k, ki je manjše od q.
- Izračunaj $\gamma = (\alpha^k \mod p) \mod q$
- Izračunaj $k^{-1} \mod q$.
- Izračunaj $\delta = k^{-1}(h(x) + a\gamma) \mod q$, kjer je h(x)povzetek sporočila x, dobljen z zgoščevalno funkcijo
- Če je $\gamma = 0$ ali $\delta = 0$, začni ponovno.
- Podpis sporočila je (γ, δ) .

Preverjanje podpisa

- \bullet Priskirbi si overjeno kopijo javnega kjluča (p,q,α,β)
- Izračunaj $w = \delta^{-1} \mod q$ in h(x)
- Izračunaj $e_1 = h(x)w \mod q$ in $e_2 = \gamma w \mod q$
- Izračunaj $v = (\alpha^{e_1} \beta^{e_2} \mod p) \mod q$
- Sprejmi podpis, če je $v = \gamma$

Uporaba bločnih šifer

Elektronska kodna knjiga (ECB)

Naivni način uporabe bločnih šifer. Z istim klučem kodiramo zaporedoma bolk po blok

$$c_i = E_k(b_i)$$
$$b_i = D_k(c_i)$$

Veriženje kodnih blokov (CBC)

Izberemo inicializacijski vektor IV dolžine n. Kodiranie

$$c_0 = IV$$

$$za j = 1, \dots, m:$$

$$c_j = E_e(b_j \oplus c_{j-1})$$

$$c = c_1 \dots c_m$$

Dekodiraje

$$c_0 = IV$$

 $za \ j = 1, \dots, m$:
 $b_j = De(c_j) \oplus c_{j-1}$
 $b = b_1 \dots b_m$

Napaka na bloku c_i vpliva le na b_i in b_{i+1}

Način s števcem (CM)

Izberemo števec ctr dolžine n. Besedilo razdelimo na bloke dolžine n: $b = b_1 \dots b_m$.

Kodiranie

$$\begin{aligned} & \textit{za} \ j = 1, \dots, m \colon \\ & l_j = ctr + j - 1 \mod 2^n \\ & c_j = b_j \oplus E_e(l_j) \\ & c = c_1 \dots c_m \end{aligned}$$

Dekodiranje

$$za \ j=1,\ldots,m \colon \\ l_j=ctr+j-1 \ \text{mod} \ 2^n \\ b_j=c_j \oplus E_e(l_j) \\ b=b_1\ldots b_m$$

Napadi na kriptosisteme

Pasivni napadi

- Napad za golim kriptogramom: nasprotnik pozna enega ali več kriptogramov.
- Napad z znanim besedilom: nasprotnik pozna enega ali več parov (besedilo, kriptogram).
- Napad z izbranim besedilom: nasprotnik ima začasen dostop do kodirnega postopka. Generira pare (b,c) za izbrana besedila $b.\ V$ primeru kriptosistemov z javnimi ključi tak napad štejemo za paseiven.

Aktivni napadi

- Napd z izbranim kriptogramom: nasprotnik za izbrane kriptograme lahko zahteva ustrezna besedila. Kasneje dobi kriptogram c, ki ga želi dekodirat.
- Prilagodljivi napad z izbranim kriptogramom: nasprotnik skuša dešifirati $c\ \mathrm{med}\ \mathrm{tem}$ lahko za izbrane kriptograme lahko zahteva ustrezna besedila.

Stopnje varnosti

- Brezpogojna varnost: tudi če ima napadalec neomejene računske vire, samo iz kriptograma na izve nobene informacije o besedilu (razen dolžine)
- Semantična varnost: napadalec s polinomsko omejenimi viri samo iz kriptograma z nezanemarljivo verjetnostjo ne izve nobene informacije o besedilu (razen

• Polinomska varnost: napadalec s polinomsko omejenimi viri z nezanemarljivo verjetnostjo ne more ločiti med kriptogramoma danih besedil iste dolžine.

Za pasivnega napadalca sta semantična in polinomska varnost ekvivalentni.

Sistemi s popolno tajnostjo (LPT)

Simetrični kriptosistem S = (B, C, K, E, D) opremimo z verietnostno porazdelitvijo na množici $\mathcal{B}\times\mathcal{K}$

> B ... slučajna sprem. z zalogo vrednosti $\mathcal B$ K ... slučajna sprem. z zalogo vrednosti K... slučajna sprem. z zalogo vrednosti $\mathcal C$

C ie določena z B in K

Predpostavimo, da st B in K neodvisni:

$$P(B = b \cap K = k) = P(B = b)P(K = k)$$

za vsak $b \in \mathbb{B}$ in vsak $c \in \mathcal{C}$ velja še:

$$P(B=b) > 0$$
 oziroma $P(C=c) > 0$

Potem ima kriptosistem S lastnost popolne tajnosti natanko tedaj, ko

$$\forall b \in \mathcal{B}, c \in \mathcal{C} : P(B = b | C = c) = P(B = b)$$

exvivalentno $P(C = c | B = b) = P(C = c)$

Vrednost C za dana $b \in \mathcal{B}$ in $k \in \mathcal{K}$ je:

$$c = E_h(b)$$

Verjetnost dogodka $\left(C=c\right)$ dobimo iz formule za popolno

$$P(C=c) = \sum_{b \in \mathcal{B}} P(C=c|B=b)P(B=b)$$

$$P(C = c|B = b) = \sum_{k \in K: E_{+}(b) = c} P(K = k)$$

Verietnostne formule

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \qquad P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

Trditev: Če ima kriptosistem lastnost popolne tajnosti, za vsak $b \in \mathcal{B}$ in $c \in \mathcal{C}$ obstajaj $k \in \mathcal{K}$, da velja $E_k(b) = c$. In $|\mathcal{B}| \le |\mathcal{C}| \le |\mathcal{K}|$ *Izrek (Shannon):* Naj velja $|\mathcal{B}| = |\mathcal{C}| = |\mathcal{K}|$. Potem ima krip-

tosistem S lastnost popolne tajnosti natanko tedaj, ko

- za vsak $b \in \mathcal{B}$ in vsak $c \in \mathcal{C}$ obstaja en $k \in \mathcal{K}$, da je $E_k(b) = c$
- \bullet slučajna spremnljivka K je enakomerno porazdeljena.

Teoriia števil

Eulerjeva funkcija

Eulerjeva funkcija nam pove koliko je obrnlivih elementov v

$$|\mathbb{Z}_m^*| = \varphi(m)$$

Za $n \in \mathbb{N}$ s paraštevilskim razcepom $n=p_1^{\alpha_1}\cdot\ldots\cdot p_m^{\alpha_m}$ velja:

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_m^{\alpha_m}) = n \prod_{p_k \in \mathbb{P}} \left(1 - \frac{1}{p_k}\right)$$

Euljerjev izrek:

Naj boGkončna grupa. Potem red elementa $a \in G$ deli red grupe G.

$$\gcd(a,m) = 1 \Leftrightarrow a^{\varphi(m)} \equiv_m 1; a \in \mathbb{Z}_m^*$$
$$a, m \in \mathbb{N} \land \gcd(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv_m 1$$
$$a^{\varphi(m)} = 1 \lor \mathbb{Z}_m^*$$

Mali Fermatov izrek: če je $m \in \mathbb{P} \ (\varphi(m) = m-1)$ in gcd(a, m) = 1, potem:

$$a^{m-1} \equiv_m 1$$

Fermantov test praštevilskosti

$$p$$
 praštevilo $\implies a^{p-1} \equiv_p 1$

Če želimo preveriti ali je p praštevilo, zgornjo trditev preizkusimo za nekaj naključnih a-jev.

Miller-Rabinov test

Če je n praštevilo mora veljati:

Naključno število a je tuje n.

Če zapišemo $n-1=2^{s}d$, kjer je d liho število, velja eno je število elementov G, oznaka |G|.

- $a^d \equiv_n 1$
- $\exists r \in 0, 1, \dots, s-1$, da je $a^{2^r d} \equiv_n -1$

Verjetnost (napake), da zgornje velja za sestavljeno število je največ $\frac{1}{4}$

Linearne diofantske enačbe

Diofantska enačba ax + by = c ima rešitev $\Leftrightarrow gcd(a, b)|c$. Če ima eno rešitev $(x_0, y_0) \in \mathbb{Z}^2$ ima neskončno množico

$$\{(x_k,y_k):k\in\mathbb{Z}\}$$

$$x_k = x_0 - k \frac{b}{\gcd(\mathbf{a}, \mathbf{b})}$$

$$y_k = y_0 + k \frac{a}{\gcd(\mathbf{a}, \mathbf{b})}$$

Razširjen evklidov algoritem

whod:
$$(a,b)$$
 $(r_0,x_0,y_0)=(a,1,0)$ $(r_1,x_1,y_1)=(b,0,1)$ $i=1$
$$dokler \ r_i\neq 0:$$

$$i=i+1$$

$$k_i=r_{i-2}//r_{i-1}$$

$$(r_i,x_i,y_i)=(r_{i-2},x_{i-2},y_{i-2})-k_i(r_{i-1},x_{i-1},y_{i-1})$$
 konec zanke wrii: $(r_{i-1},x_{i-1},y_{i-1})$

Naj bosta $a, b \in \mathbb{Z}$. Tedaj trojica (d, x, y), ki jo vrne razširjen evklidov algoritem z vhodnim podatkomk (a, b), zadošča:

$$ax + by = d$$
 in $d = \gcd(a, b)$

- grupoid (M, \cdot) urejen par z neprazno množico M in zaprto opreacijo ·
- polgrupa grupoid z asociativno operacijo $\forall x,y,z \in$ $M: (x \cdot y) \cdot z = x \cdot (y \cdot z).$
- monoid polgrupa z enoto $\exists e \in M \ \forall x \in M : e \cdot x =$ $x \cdot e = x$.
- grupa polgrupa v kateri ima vsak element inverz $\forall x \in M \ \exists x^{-1} \in M : x \cdot x^{-1} = x^{-1} \cdot x = e.$
- abelova grupa grupa s komutativno operacijo $\forall x, y \in M : x \cdot y = y \cdot x.$

Množica \mathbb{Z}_m

$$\mathbb{Z}_m = \{0, 1, ..., m-1\}$$

Vpeljemo seštevanje $+_m$ po modulu m in množenje \cdot_m po modulu m. Dobimo grupo $(\mathbb{Z}_m, +_m)$ in monoid (\mathbb{Z}_m, \cdot_m) Red elementa $x \in \mathbb{Z}_m$ je $\frac{m}{\gcd(m,x)}$

Množica Z*

To je množica vseh obrnljivih elementov v \mathbb{Z}_m (operacija: množenje).

$$|\mathbb{Z}_m^*| = \varphi(m)$$

Element $x \in \mathbb{Z}_m$ je obrnljiv če se da rešiti diofantsko enačbo:

$$xu + km = 1$$

za neznanki y (inverz od x) in k.

Cayleyjeva tabela

Za vsak element množice imamo en stolpec in eno vrstico. V vsakem polju je produkt elementa vrstice in elementa stolpca. (Presek vrstice a in stolpca b je ab)

Red elementa

Naj bo (G,\cdot) grupa. Red elemneta a je najmanjše naravno število $n \in \mathbb{N}$, da velja

$$a^n = e$$

oznaka: #a

Red grupe

Ciklična grupa

Grupa je ciklična, če vsebuje a reda |G|:

$$G = \left\{ a, a^2, a^3, \dots, a^{|G|} = e \right\}$$

$$(\mathbb{Z}_p^*, \cdot) \cong (\mathbb{Z}_{p-1}, +)$$

$$\operatorname{red}_{\mathbb{Z}_p^*}(\alpha^i) = \operatorname{red}_{\mathbb{Z}_{p-1}}(i) = \frac{p-1}{\operatorname{gcd}(i, p-1)}$$

x je generator grupe $\mathbb{Z}_p^* \iff \#x = p-1$

x je generator grupe $\mathbb{Z}_p^* \iff x^{\frac{p-1}{p_i}} \neq 1 \mod p$, za vsak i,

Končni obsegi

 $(K, +, \cdot)$ je obseg, če je

- (K, +) abelova grupa
- velja distributivnost:

• (K^*, \cdot) grupa $(K^* = K \setminus \{0\})$

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$
$$(a+b) \cdot c = (a \cdot c) + (b \cdot c)$$

Obseg je **komutativen**, če je (K^*, \cdot) komutativna.

Praštevilski obsegi

Če je p praštevilo, je $(\mathbb{Z}_p, +_p, \cdot_p)$ končen obseg.

Galoisovi obsegi

$$GF(p) \cong \mathbb{Z}_p \qquad p \in \mathbb{P}$$
 $GF(p^n) \cong \mathbb{Z}_p[x]/(u)$

- $u \in \mathbb{Z}_p[x]$ je nerazcepen polinom stopnje n
- \bullet elementi $\mathrm{GF}(p^n)$ so ostanki polinomov iz \mathbb{Z}_p pri deljenju z polinomom u
- seštevanje je enako kot seštevanje v $\mathbb{Z}_p[x]$
- produkt izračunamo v $\mathbb{Z}_p[x]$ nato pa vzamemo ostanek pri deljenju z u

Množica neničelnih/obrnljivih elementov $(GF(p^n)^*, \cdot) \cong$ $(\mathbb{Z}_{p^n-1},\cdot)$ je vedno izomorfna neki ciklični grupi. Generatorjem te grupe rečemo primitivni elementi Galoisovega

Kitajski izrek o ostankih

Naj bodo n_1, \ldots, n_k paroma tuja.

$$x \equiv a_1 \mod n_1$$

$$\vdots$$

$$x \equiv a_k \mod n_k$$

$$N = n_1 \cdot n_2 \cdot \dots \cdot n_k$$

Vse rešitve zgornjega sistema so kongurentne po modulu ${\cal N}$

$$N_i = rac{N}{n_i}$$
 $M_i = ext{inverz } N_i ext{ po modulu } n_i$ $x = \sum_{i=1}^k a_i M_i N_i \mod N$

Kodi

Naj bo Σ končna abeceda. Definirajmo $\Sigma^* = \bigcup_{n=0}^{\infty} \Sigma^n$. **Kod** \mathcal{C} nad abecedo Σ je končna podmnožica Σ^* ($\mathcal{C} \subset \Sigma^*$)

- Kodiranje je preslikava $f: \mathcal{S} \to \mathcal{C}$
- Po prenosu po komunikacijskem kanalu prejmemo besedo y.
- \bullet Če $y \notin \mathcal{C},$ ji po neke
em pravilu priredimo besedo $x' \in \mathcal{C}$. Pravimo, da besedo **dekodiramo**.

Bločni kodi

 Kod ${\mathcal C}$ nad abecedo Σ je **bločni kod dolžine** n, če imajo vse kodne besede dolžino n ($\mathcal{C} \subseteq \Sigma^n$).

Hammingova razdalja med besedama x in y je definirana

$$d(x,y) = |\{i; x_i \neq y_i\}|$$

Teža besede x (t(x)) je definirana kot število neničelnih mest v besedi.

Razmaknjenost koda:

$$d = d(\mathcal{C}) = \min\{d(x, y); x, y \in \mathcal{C}, x \neq y\}$$

Pravila za dekodiranje

• Pravilo najmanjše napake

Prejeto besedo y dekodiramo v tisti $x \in \mathcal{C}$, ki maksimizira

P[x oddana|y sprejeta]

$$P[x|y] = \frac{P[y|x] \cdot P[x]}{P[y]} = \frac{P[y|x] \cdot P[x]}{\sum_{c \in \mathcal{C}} P[y|c] \cdot P[c]}$$

• Pravilo največje verjetnosti

Prejeto besedo y dekodiramo v tisti $x \in \mathcal{C}$, ki maksimizira

$$P[y \text{ sprejeta}|x \text{ oddana}]$$

Če so vse kodne besede enako verjetne, sta PNN in PNV enaki.

• Pravilo najbližjega soseda

Prejeto besedo $y \in \Sigma^n$ dekodiramo v tisto besedo $x \in \mathcal{C}$, pri kateri je d(x, y) najmanjša.

Če je p < 1/2, dajeta PNN in PNS enak rezultat.

Kod \mathcal{C} označimo z (n, M, d)-kod, kjer je

n ... bločna doložina M ... št. kodnih besed d ... razmaknjenost

y = x + e, kjer je $e \in \Sigma^n$ napaka.

- Kod **odkrije** s napak, če $x + e \notin \mathcal{C}$ za vse $x \in \mathcal{C}$ in vse e, za katere je $1 \le t(e) \le s$
- Kod **popravi** s napak, če

$$d(x+e,x) < d(x+e,x')$$

za vse $x, x' \in \mathcal{C}$ in vse $e \in \Sigma^n$, za katere je $t(e) \leq s$.

Bločni kod z bločno dolžino n in razmaknjenostjo d odkrije d-1 napak in **popravi** $\lfloor \frac{d-1}{2} \rfloor$ napak.

Linearni kodi

Kod $\mathcal{C} \subseteq \Sigma^n$ je **linearen**, če je vektorski podprostor:

$$\forall c_1, c_2 \in \mathcal{C}, \ \alpha, \beta \in \Sigma \implies \alpha c_1 + \beta c_2 \in \mathcal{C}$$

Dimenzija koda (k) je dimenzija vektorskega podporstora.

[n, k, d]-kod nad $\Sigma = GF(q)$ je linearen (n, q^k, d) -kod.

$$d = \min_{x \in \mathcal{C}, x \neq 0} t(x)$$

$$M = q^k$$

Generatorska matrika G koda C je matrika velikosti $k \times n$. Njene vrstice so kodne besede, ki sestavljajo bazo kode (vektorskega podporstora).

Nadzorna matrika

 $\mathcal{C}^{\perp} = \{x \in \Sigma^n; cx^T = 0 \ \forall c \in \mathcal{C}\}\ \text{je dualni kod koda } \mathcal{C}.$ Generatorsko matriko koda \mathcal{C}^{\perp} imenujemo nadzorna ma
- Meje za kode

$$G \in \Sigma^{k \times n}, H \in \Sigma^{(n-k) \times n}$$

$$rang(G) = k, rang(H) = n - k$$

potem velja: G je generatorska in H nadzorna matrika nekega linearnega koda $\iff G \times H^T = 0$.

Sindrom

$$y = x + e$$

 Hy^T imenujemo **sindrom** besede y.

$$Hy^T = He^T$$

Kodiranje

$$c = sG$$

Dekodiranje

- Izračunaj $\sigma = Hy^T$
- V tabeli T poišči e: $He^T = \sigma$ (če ga ni, zahtevaj ponoven prenos besede)
- Vrni x = y e

Razmaknjenost

Naj bo \mathcal{C} linearen kod nad abecedo GF(q) z ndzorno matriko H. Potem velia:

 $d(\mathcal{C}) \geq d \iff$ vsaka množica d-1 stolpcev matrike H je linearno neodvisna nad GF(q)

 $d(\mathcal{C}) = \max\{d; \text{vsakih } d-1 \text{ stolpcev } H \text{ je lin. neodvisnih}\}$

Ekvivalentnost

Koda sta **ekvivalentna**, če lahko iz enega dobimo drugega z zaporedjem transormacij kodne matrike

- premutacije stolpcev
- premutacije simbolov v izbranem stolpcu
- permutacije vrstic

$$C_1 \sim C_2$$

Za vsak [n, k, d]-kod obstaja ekvivalenten kod z generatorsko matriko v standardni obliki

$$G = [I_k|A] \qquad H = [-A^T|I_{n-k}]$$

$$A_q(n,d) = \max\{M; \exists (n,M,d) \text{ kod nad } GF(q)\}$$

$$A_q(n,1) = q^n$$
$$A_2(n,2) = 2^{n-1}$$

$$|K(x,r)| = \sum_{k=0}^{r} {n \choose k} (q-1)^k$$

Hamingova zgornja meja

$$A_q(n,d) \le \frac{q^n}{\sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{k} (q-1)^k}$$

Če kod dosega Hammingovo mejo, je popoln.

Gilbert-Varshamova spodnja meja

$$A_q(n,d) \ge \frac{q^n}{\sum_{k=0}^{d-1} \binom{n}{k} (q-1)^k}$$

Hammingov kod reda r

nad $\Sigma = GF(q)$ je [n, k, d]-kod dolžine $n = \frac{q'-1}{q-1}$ in dimenzije k = n - r, podan z nadzorno matriko $H \in \Sigma^{r \times n}$, v kateri sta vsaka dva stolpca linearno neodvisna.

Hammingovi kodi so popolni.

Singletonova meja

Naj bo \mathcal{C} (n, M, d)-kod nad GF(q). Potem je $M \leq q^{n-d+1}$. Za linearni [n, k, d]-kod je $d \le n - k + 1$.

Linearni [n, k, d]-kod lahko popravi največ $\lfloor \frac{n-k}{2} \rfloor$ napak.

Ciklični kodi

Besedo $\hat{x} = x_n x_1 \cdots x_{n-1}$ imenujemo **ciklični pomik** besede x.

Linearen kod je cikličen, če velja

$$x \in \mathcal{C} \Rightarrow \hat{x} \in \mathcal{C}$$

Besedo $x = x_1 \cdots x_n$ identificiramo s polinomom

$$x(t) = x_1 + x_2t + \dots + x_nt^{n-1} \in GF(q)[t]/(t^n - 1)$$

Besedi \hat{x} ustreza polinom $t \cdot x(t) \pmod{t^n - 1}$.

Naj bo $\mathcal C$ cikličen kod in g(t)neničel
n polinom najmanjše stopnje v $\mathcal{C}.$ Potem velja:

- $C = \langle g(t) \rangle = \{ g(t) \cdot a(t) \mod t^n 1; a(t) \in GF(q)[t] \}$ (ideal, ki ga generira g(t))
- $g(t) | (t^n 1)$
- $\dim(\mathcal{C}) = k = n \deg(g)$ in $B = \{g(t), tg(t), \dots, t^{k-1}g(t)\}$ je baza \mathcal{C} .

Ciklični kodi dolžine n nad GF(q) ustrezajo deliteljem polinoma $t^n - 1 \in GF(q)[t]$.

Če $\mathcal{C} = \langle g(t) \rangle$, imenujemo g generatorski polinom koda

$$G = \begin{bmatrix} g(t) \\ tg(t) \\ \vdots \\ t^{k-1}g(t) \end{bmatrix}$$

je generatorska matrika za \mathcal{C} .

$$t^{n-k+i} = q_i(t)g(t) + r_i(t)$$

Potem velja:

$$t^{n-k+i} - r_i(t) = q_i(t)g(t) \in \mathcal{C}$$

$$G' = \begin{bmatrix} -r_0(t) & 1 & 0 & \cdots & 0 \\ -r_1(t) & 0 & 1 & \cdots & 0 \\ \vdots & & & & & \\ -r_{b-1}(t) & 0 & 0 & \cdots & 1 \end{bmatrix}$$

je potem generatorska matrika za $\mathcal{C}.$

Kodiranje

$$t^{n-k}s(t) = q(t)g(t) + r(t) \implies x(t) = t^{n-k} \cdot s(t) - r(t) \in \mathcal{C}$$

Sporočilo s(x) pomnožimo z generatorskim polinomom g(x)

$$x(t) = s(t)g(t)$$

Reed-Solomonovi kodi

Naj bodo $\alpha_1, \alpha_2, \dots, \alpha_p \in GF(q)$ in $\alpha_i \neq 0, \alpha_i \neq \alpha_j$

$$g(t) = (t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_p) \mid (t^{q-1} - 1)$$

Posledica: g(t) generira linearen cikličen kod dolžine n =q-1 nad $\widetilde{GF}(q)$ dimenzije n-p.

Naj bo $n=2^r-1, \delta \in \{2,\ldots,n\}, \beta$ primitiven element $GF(2^r)$.

Reed-Solomonov kod RS(n,k) je cikličen linearen kod dolžine n in dimenzije $k = n - \delta + 1$ nad $GF(2^r)$, generiran s polinomom $g(t) = (t - \beta)(t - \beta^2) \cdots (t - \beta^{\delta - 1})$

Naj bo \mathcal{C} Reed-Solomonov kod dolžine $n=2^r-1$ in dimenzije k. Potem je $d(\mathcal{C}) = n - k + 1$.

To pomeni, da Reed-Solomonov kod doseže Singletonovo mejo – popravi največje število napak glede na št. simbolov, ki jih dodamo sporočilu.