Kriptosistem

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

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 $\mathcal{S}_1 = (\mathcal{B}_1, \mathcal{C}_1, \mathcal{K}_1, \mathcal{E}', \mathcal{D}')$ in $\mathcal{S}_2 = (\mathcal{B}_2, \mathcal{C}_2, \mathcal{K}_2, \mathcal{E}'', \mathcal{D}'')$ 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 $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ je prevedljiv na $\mathcal{S}' = (\mathcal{B}, \mathcal{C}, \mathcal{K}', \mathcal{E}', \mathcal{D}')$, če obstaja $f : \mathcal{K} \to \mathcal{K}'$, da za vsak $k \in \mathcal{K}$ velja:

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

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

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

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 $\underline{k} \in \mathcal{K}$

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

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 $A \in \mathcal{K}$

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

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

Sestavlja jih

- **razpored ključev**: Naj bo K ključ. K uporabimo za konstrukcijo krožnih ključev $(K^1, \dots, K^{N_r})$ temu seznamu pravimo razpored ključev.
- **krožna funkcija**: ima dva argumenta: tekoče stanje in krožni ključ:
  $$w^r = g(w^{r-1}, K^r)$$
  Da je dešifriranje možno mora biti g injektivna za vsak fiksen ključ K; tj. $\exists g^{-1}$:
  $$g^{-1}(g(w, K), K) = w \qquad \forall w, K$$
- **šifriranje skozi N_r podobnih krogov**: Besedilo x vzamemo 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

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:

$w^0 = b$
za $r = 1, \dots, N_r - 1$:
  $u^r = w^{r-1} \oplus K^r$ // primasamo K
  za $i = 1, \dots, m$:
    $\underline{v}_i^r = \pi_s(\underline{u}_i^r)$ // substitucija zlogov
  $w^r = v^r_{\pi_p(1)}, \dots, v^r_{\pi_p(\ell m)}$ // permutacija bitov
// zadnji krog
$u^{N_r} = w^{N_r - 1} \oplus K^{N_r}$
za $i = 1, \dots, m$:
  $\underline{v}_i^{N_r} = \pi_s(\underline{u}_i^{N_r})$
vrni $c = v^{N_r} \oplus K^{N_r + 1}$ // beljenje

Dekodiranje:

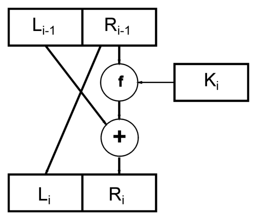
$v_r^N = c \oplus K^{N_r + 1}$
za $i = 1, \dots, m$:
  $\underline{u}_i^{N_r} = \pi_s^{-1}(\underline{v}_i^{N_r})$
za $r = N_r - 1, \dots, 1$:
  $w^r = u^r \oplus K^{r+1}$
  $v^r = (w^r_{\pi_p^{-1}(1)}, \dots, w^r_{\pi_p^{-1}(\ell m)})$
  za $i = 1, \dots, m$:
    $\underline{u}_i^r = \pi_s^{-1}(\underline{v}_i^r)$
$b = u^1 \oplus K^1$

Feistelova šifra

je bločna iterativna šifra dolžine $2t$ za abecedo $\Sigma = \{0, 1\}$.

N_r je št. krogov, $K^1, \dots, K^{N_r}$ razpored ključev, ki ga dobimo iz ključa K in $f_K : \Sigma^t \to \Sigma^t$ je *Feistelova kodirna funkcija.*

En krog kodiranja:



Kodiranje

$L_0 =$ leva polovica b
$R_0 =$ desna polovica b
za $i = 1, \dots, N_r$:
  $L_i = R_{i-1}$
  $R_i = L_{i-1} \oplus f_{K_i}(R_{i-1})$
$c = R_{N_r} \| L_{N_r}$

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

Dekodiranje

za $j = 1, \dots, t$:
  $b_j = D_{z_j}(c_j)$
$b = b_1 b_2 \dots c_t \in \mathcal{B}^t$

Aditivne tokovne šifre

Naj bo $(G, +)$ grupa, $\mathcal{B} = \mathcal{C} = \mathcal{K}$ in $z_1, z_2, \dots$ 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 $z_1 \in \mathbb{Z}_{26}$

$$z_i = b_{i-1} \quad \text{za} \quad i > 1$$

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 rekurzivna 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 $\mathbb{Z}_s$:

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

Zaporedju lahko priredimo polinom:

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

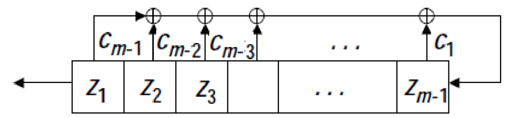
Kodiranje/Dekodiranje:

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

Pomični register z linearno povratno zanko

V pomičnem registru je na začetku inicializacijski vektor $(z_1 z_2 \dots z_m)$ (ključ).

Na vsakem koraku izpišemo z_1 register pomaknemo v levo zadnji bit z_m pa izračunamo kot z $c_1, \dots, c_m$ uteženo vsoto.



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 bo G multiplikativna 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

$$\alpha^x = \beta$$

Številu x rečemo diskretni logaritem elementa β z osnovo α.

Diffie-Hellmanova izmenjava ključev

- Alenka in Bojan se dogovorita za veliko praštevilo p in $\alpha \in \mathbb{Z}_p^*$, 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 $K = \alpha^{ab} = A^b = B^a$

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
- 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:

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

Naj bo $B = \alpha^b \bmod p$ in $A = \alpha^a \bmod p$. Potem kodirnemu ključu (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.
- **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 izvleček.
- **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 $i = 1, \dots, t$:
  $H_i = f(H_{i-1} \| x_i)$
$h(x) = H_t$

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 velike bloke.

Če je kompresijska funkcija odporna na trke, je tudi zgoščevalna funkcija odporna na trke.

Teorija števil

Eulerjeva funkcija

Eulerjeva funkcija nam pove koliko je obrnlivih elementov v $\mathbb{Z}_m$.

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

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

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

Euljerjev izrek:

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

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

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

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

Razširjen evklidov algoritem

vhod: (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
vrni: $(r_{i-1}, x_{i-1}, y_{i-1})$

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

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

Grupe

- **grupoid** $(M, \cdot)$ urejen par z neprazno množico M in zaprto opreacijo $\cdot$.
- **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 $\mathbb{Z}_m^*$

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*:

$$xy + km = 1$$

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

je število elementov G, oznaka $|G|$.

Ciklična grupa

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

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

Končni obsegi

$(K, +, \cdot)$ je obseg, če je

- $(K, +)$ abelova grupa
- $(K^*, \cdot)$ grupa $(K^* = K \setminus \{0\})$
- velja distributivnost:

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

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

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

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

- $u \in \mathbb{Z}_p[x]$ je nerazcepen polinom stopnje n
- 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 obsega.