Kriptosistem

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

$$\forall e \in \mathcal{K} \exists d \in \mathcal{K} : D_d(E_e(x)) = x \quad \forall x \in \mathcal{B}$$

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

Klasični kriptosistem

Klasične šifre (povzetek)

Sistem	Model
Cezarjeva	$\mathcal{B} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{25}$, $E_k(x) \equiv x + k \pmod{25}$, $D_k(y) \equiv y - k \pmod{25}$
Substitucijska	$\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}$, $\mathcal{K} = S(\mathbb{Z}_{25})$, $E_\pi(x) = \pi(x)$, $D_\pi(y) = \pi^{-1}(y)$
Afina	$\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}$, $\mathcal{K} = \mathbb{Z}_{25}^* \times \mathbb{Z}_{25}$, $E_{(a,b)}(x) \equiv ax+b \pmod{25}$, $D_{(a,b)}(y) \equiv a^{-1}(y-b) \pmod{25}$
Vigenerjeva	$\mathcal{B} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{25}^n$, $E_{\underline{k}}(\underline{x}) \equiv \underline{x} + \underline{k} \pmod{25}$, $D_{\underline{k}}(\underline{y}) \equiv \underline{y} - \underline{k} \pmod{25}$
Permutacijska	$\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}^n$, $\mathcal{K} = S_n$, $E_\pi(\underline{x}) = (x_{\pi(1)}, \ldots, x_{\pi(n)})$, $D_\pi(\underline{y}) = (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(n)})$
Hillova	$\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}^n$, $\mathcal{K} = \{A \in \mathbb{Z}_{25}^{n \times n} \mid \det(A) \in \mathbb{Z}_{25}^*\}$, $E_A(\underline{x}) \equiv A\underline{x}$, $D_A(\underline{y}) \equiv A^{-1}\underline{y} \pmod{25}$

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:

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

DES in AES

DES: 56-bitni ključ + 8 paritetnih
AES: 128, 192, 256 bitni ključ (odvisno od specifikacije)

Sistemi s popolno tajnostjo (LPT)

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

$$B : \Omega \to \mathcal{B}, \qquad K : \Omega \to \mathcal{K}, \qquad C : \Omega \to \mathcal{C}$$

C je 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:

$$P(B = b) > 0 \quad \text{oziroma} \quad P(C = c) > 0$$

Potem ima kriptosistem S **lastnost popolne tajnosti** natanko tedaj, ko

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

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

$$c = E_k(b)$$

Verjetnost dogodka $(C = c)$ dobimo iz formule za popolno verjetnost:

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

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

Popolna tajnost je ekvivalentna temu, da napadalec ne ugane bolje od naključja:

$$\Pr[b' = b] \leq \frac{1}{2}.$$

Verjetnostne 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 $|\mathcal{B}| \leq |\mathcal{C}| \leq |\mathcal{K}|$
Izrek (Shannon): Naj velja $|\mathcal{B}| = |\mathcal{C}| = |\mathcal{K}|$. Potem ima kriptosistem 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 $E_k(b) = c$
- slučajna spremnljivka K je enakomerno porazdeljena.

Tokovne šifre

Za tok ključev $z_1, z_2, \ldots$ in bloke b_i velja po simbolih:

$$c_i = E_{z_i}(b_i), \qquad b_i = D_{z_i}(c_i), \qquad i = 1, \ldots, t.$$

Aditivne tokovne šifre

$(G, +)$ grupa, $\mathcal{B} = \mathcal{C} = \mathcal{K} = G$:

$$c_i = b_i + z_i, \qquad b_i = c_i - z_i.$$

Samokodirna šifra

$\mathcal{B} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$, z_1 naključen, za $i > 1$: $z_i = b_{i-1}$.

Vermanova šifra

$\mathcal{B} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$:

$$E_k(b) = b \oplus k, \qquad D_k(c) = c \oplus k.$$

Klasični OTP: ključ je enako dolg kot besedilo; v praksi tok dobimo iz semena.

Linearna rekurzivna šifra

je sinhrona tokovna šifra, pri kateri je $\mathcal{B} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_s$ zaporedje ključev z linearno rekurzivno enačbo reda m s konstantnimi koeficienti nad $\mathbb{Z}_s$:

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

$E_{z_i}(x_i) = x_i + z_i \mod s \quad D_{z_i}(y_i) = y_i - z_i \mod s$
Zaporedju lahko priredimo polinom:

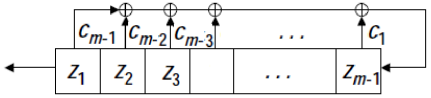
$$C(x) = 1 + \sum_{i=1}^{m} c_i x^i \mod s$$

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.
Geffejev generator kombinira tri LFSR-je:

$$z = x_1 x_2 + x_2 x_3 + x_3 \pmod 2$$

Pomični register z linearno povratno zanko

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



Na vsakem koraku izpišemo z_1 register pomaknemo v levo 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:

$$\begin{bmatrix} z_0 & z_1 & \ldots & z_{m-1} \\ z_1 & z_2 & \ldots & z_{m-2} \\ \vdots & \vdots & & \vdots \\ z_{m-1} & z_m & \ldots & z_{2m-2} \end{bmatrix} \begin{bmatrix} c_m \\ c_{m-1} \\ \vdots \\ c_1 \end{bmatrix} = \begin{bmatrix} z_m \\ z_{m+1} \\ \vdots \\ z_{2m-1} \end{bmatrix}$$

Če smo pravilno uganili red m ima sistem enolično rešitev.

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 $n = p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m}$ velja:

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

Eulerjev 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:

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

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 izmed:

- $a^d \equiv_n 1$
- $\exists r \in 0, 1, \ldots, s-1$, 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 rešitev:

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

$$x_k = x_0 - k\frac{b}{\gcd(\text{a, b})} \qquad y_k = y_0 + k\frac{a}{\gcd(\text{a, b})}$$

REA (Razširjen Evklidov algoritem)

REA poišče ne le gcd(a,b) ampak tudi $s, t \in \mathbb{Z}$, da velja $a \cdot s + b \cdot t = \gcd(\text{a,b})$.

Postopek

Začetne vrednosti: $r_{-1} = a \quad s_{-1} = 1 \quad t_{-1} = 0$
$r_1 = b \quad s_1 = 0 \quad t_1 = 1$
Iteracija za i = 1,2,. . . n+1, kjer je n+1 najmanjši indeks, za katerega $r_{n+1} = 0$:

$$k_i = \lfloor \tfrac{r_{i-2}}{r_{i-1}} \rfloor$$
$$r_i = r_{i-2} - k \cdot r_{i-1}$$
$$s_i = s_{i-2} - k \cdot s_{i-1}$$
$$t_i = t_{i-2} - k \cdot t_{i-1}$$

	a	1	0
k_1	b	0	1
k_2	r_1	s_1	t_1
k_3	r_2	s_2	t_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
k_{n+1}	$r_n \neq 0$	s_n	t_n
	$r_{n+1} = 0$	s_{n+1}	t_{n+1}

$$a \cdot s_i + b \cdot t_i = r_i \quad \text{za } i = -1, 0, 1, \ldots, n+1$$
$$r_n \mid r_i \quad \text{za } i = n, n-1, \ldots, 0, -1$$
$$\gcd(a, b) = r_n$$

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

$$a^n = e$$

Red grupe

je število elementov G, oznaka $|G|$.

Ciklična grupa

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

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

Grupa $\mathbb{Z}_p^*$

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

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

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, jer je $p - 1 = p_1^{k_1} \ldots p_l^{k_l}$.

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.

Kitajski izrek o ostankih

Naj bodo $n_1, \ldots, n_k$ paroma tuja.

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ &\vdots \\ x &\equiv a_k \mod n_k \end{aligned}$$

Vse rešitve zgornjega sistema so kongurentne po modulu $N = n_1 \cdot n_2 \cdot \cdots \cdot n_k$.

$$N_i = \frac{N}{n_i} \qquad M_i = \text{ inverz } N_i \text{ po modulu } n_i$$

$$x = \sum_{i=1}^{k} a_i M_i N_i \mod N$$

V abstraktni algebri se CRT običajno navede tako: če so si vsi n_i med sabo tuji, potem preslikava

$$x \bmod N \mapsto (x \bmod n_1, x \bmod n_2, \ldots, x \bmod n_k)$$

definira izomorfizem kolobarja

$$(\mathbb{Z}/N\mathbb{Z}, +, \cdot) \cong (\mathbb{Z}/n_1\mathbb{Z}, +, \cdot) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}, +, \cdot),$$

kjer je $N = n_1 \cdot n_2 \cdot \cdots \cdot n_k$.

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 $d = e^{-1} \in \mathbb{Z}_m^*$

Modularno potenciranje - algoritem kvadriranja in množenja

$a^m \bmod n$ za velike vrednosti. Potem za dvojiško predstavitev $m = (b_{k-1} \ldots b_0)_2$:

```
p = 1
za i = 0,..., k-1:
    ce je b_i = 1: p = p * a mod n
    a = a^2 mod n
vrni p
```

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 $x \in \{0, \ldots, n-1\}$, da je

$$\alpha^x = \beta$$

Številu x rečemo diskretni logaritem elementa β z osnovo α.

Shanksov algoritem (veliki korak - mali korak)

```
vhod: G grupa, α, β ∈ G, n = red(α)
izhod: x = log_α β
m = ⌈√n⌉
za j = 0, ..., m − 1:
    (j, α^{m−j}) → L_1
uredi L_1 po drugi komponenti
za i = 0, ..., m − 1:
    (i, βα^{−i}) → L_2
uredi L_2 po drugi komponenti
poisci (j, y) ∈ L_1 in (i, y) ∈ L_2
x = (mj + i)
vrni x
```

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 $a \in \{1, \ldots, n-1\}$, izračuna $A = \alpha^a \mod p$ in pošlje A Bojanu.
- Bojan si izbere naključno število $b \in \{1, \ldots, n-1\}$, 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 $B = \alpha^b \mod p$ in $A = \alpha^a \mod p$. Potem kodirnemu ključu (a, B) ustreza dekodirni ključ (b, A). Bojan izbere skrivni ključ b in izračuna $B \equiv \alpha^b \pmod p$. Objavi svoj javni ključ (p, α, B).

Učenje z napakami (LWE)

Naj bo $A \in \mathbb{Z}_p^{m \times n}$, $x \in \mathbb{Z}_p^n$, $e \in \mathbb{Z}_p^m$ (majhen šum):

$$y \equiv Ax + e \pmod p.$$

Če bi bil $e = 0$, bi dobili navaden linearni sistem; pri LWE je zaradi šuma iskanje x težko.

Sporočilo $\mu \in \mathbb{Z}_q$ kodiramo z razdelitvijo $\mathbb{Z}_p$ na q odsekov:

$$m(\mu) = \left\lfloor \frac{p}{q} \right\rfloor \mu \in \mathbb{Z}_p,$$

privzeto $q = 2$ (bita 0/1).

Tajni ključ: x. Javni ključ: (A, y), kjer je $y = Ax + e$.

Šifriranje ($s \in \{0,1\}^m$):

$$c_1 = A^T s, \qquad c_2 = y^T s + m(\mu), \qquad c = (c_1, c_2).$$

Dešifriranje:

$$w = c_2 - x^T c_1 = e^T s + m(\mu).$$

Odločimo μ po najbližjem odseku v $\mathbb{Z}_p$. Korektnost velja, če

$$|e^T s| < \frac{1}{2} \left\lfloor \frac{p}{q} \right\rfloor.$$

Nekateri napadi z vaj

KPA na Hillovo šifro: iz znanih parov (b_i, c_i) če je matrika B obrnljiva dobimo ključ

$$A \equiv CB^{-1} \pmod p,$$

RSA, skupni modul (REA): če za isti n dobimo $c_1 = b^{e_1}$ in $c_2 = b^{e_2}$ ter $\gcd(e_1, e_2) = 1$, iz $e_1 x + e_2 y = 1$ sledi

$$b \equiv c_1^x c_2^y \pmod n.$$

RSA broadcast/Hastad: pri istem sporočilu pod več paroma tujimi moduli in malem e lahko s CRT rekonstruiramo b^e in nato izračunamo celoštevilski e-ti koren.