Teorija kodiranja in kriptografija

Znane šifre. (vse gledamo po modulu, vse so bločne, gledamo bloke različnih dolžin)
Cezarjeva šifra: $E_k(b) = b + k$
Substitucijska šifra: $E_\pi(b) = \pi(b)$
Vigenerjeva šifra: $E_{\underline{k}}(\underline{b}) = \underline{b} + \underline{k}$
Hillova šifra: $E_A(\underline{b}) = A\underline{b}$
Afina šifra: $E_{(A,\underline{b})}(\underline{x}) = A\underline{x} + \underline{b}$
Vernamova šifra: Vigenerjeva, samo da je ključ enake dolžine kot besedilo.

SPN. ($B = C = \Sigma^{lm}$) substitucije $\sigma \in S(\Sigma^{lm})$, permutacije $\pi \in S_{lm}$. Postopek kodiranja: primešamo ključ, premešamo zloge, premešamo bite, ponovimo po želji.

Feistlova šifra. Razdelimo besedilo na dva polovici, v vsakem krogu levo nastavimo na prejšnjo desno, desno pa je $L_{i-1} \oplus f(R_{i-1})$.

Tokovne šifre. Vsak blok zašifriramo s svojim ključem. **LFSR.** V registru je na začetku IV, shiftamo v levo, novega izračunamo s pomočjo prejšnjih $z_n = \sum_{i=1}^{m} c_i z_{n-i}$. Karakteristični polinom je $c(x) = 1 + \sum c_i x^i$. LFSR ima periodo $q^m - 1$, q je ponavadi 2. Če je karakteristični polinom LFSR-ja nerazcepen, je perioda enaka njegovemu redu, tj. najmanjši tak t, da $c \mid x^t - 1$.

RSA. (Asimetričen, iz kodirnega ključa ne znamo dobiti dekodirnega ključa) Izberemo p, q, $n = pq$. $m = \varphi(n) = (p-1)(q-1)$. Izberemo $e \cdot d \equiv 1 \pmod{m}$. Javni ključ ($n$,$e$). Kodiranje $E_{(n,e)}(x) = x^e \pmod{n}$, dekodiranje $D_{(n,d)}(y) = y^d \pmod{n}$.

Izmenjava ključev. Veliko praštevilo p in $\alpha \in \mathbb{Z}_p^*$ z velikim redom n. Alenka izbere naključen $a \in \{1,2,\ldots,n-1\}$ in Bojan $b \in \{1,2,\ldots,n-1\}$. Alenka pošlje α^a, Bojan pa α^b. Skupni ključ α^{ab}. Napadalec pozna samo α, α^a in α^b. Varnost na problemu diskretnega logaritma. Man in the middle attack.

ElGamalov kriptosistem. p praštevilo in α primitiven element, $A = \alpha^a, B = \alpha^b$, $B = C = \mathbb{Z}_p^*$, $K = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$, $E_{(a,B)} = B^a \cdot x \pmod{p}$, $D_{(b,A)}(y) = A^{p-b-1} \cdot y \pmod{p}$. Javni ključ p,α, b). Alenka pošlje A in besedilo. a je vsakič drug, preprečimo napad z znanim besedilom.

Lastnost popolne tajnosti. B, K, C slučajne spremenljivke z zalogo vrednosti $\mathcal{B}, \mathcal{K}, \mathcal{C}$. Če sta B in K neodvisni, in $P(B = b) > 0$ za vsak b, potem ima kriptosistem $\mathcal{S}$ z dano verjetnostno porazdelitvijo na $\mathcal{B} \times \mathcal{K}$ lastnost popolne tajnosti, če za vsak b in c velja $P(B = b|C = c) = P(B = b)$. Če ima kriptosistem to lastnost, potem velja, $|\mathcal{B}| \leq |\mathcal{C}| \leq |\mathcal{K}|$. Če veljajo enakosti, potem ima sistem lastnost popolne tajnosti natanko tedaj, ko za vsak b, c obstaja natanko en ključ, ki ju zakodira in K je enakomerno razporejena. Velja $LPT \iff P(C = c|B = b) = P(C = c)$. $P(C = c|B = b) = \sum_{E_k(b)=c} P(K = k)$.

Verjetnost. Bayesova formula: $P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}$. Popoln sistem dogodkov je tak, da so vsi neodvisni in velja $P(B) = \sum P(B|A_i)P(A_i)$.

Zgoščevalne funkcije. $h : \{0,1\}^* \to \{0,1\}^n$. Odpornost praslik: za vsak z se ne da najti x, da $h(x) = z$ (enosmerna funkcija), odpornost drugih praslik: za dani x ne moremo najti x', da $h(x) = h(x')$. Odpornost na trke: najti x in x' da $h(x) = h(x')$. Najbolj pogost način je iterativno klicanje kompresijske funkcije. $H_i = f(H_{i-1}||x_i)$. Če besedilo ni primerno dolgo, dodamo še primerno število ničel, potem pa še za en blok, število za dolžino besedila dodamo na konec, po blokih dolgih $r - 1$, z enicami na začetku.

Bločno kodiranje. Naivno. Verižno: $c_0 = IV$, $c_j = E(b_j \oplus c_{i-1})$. S števcem: $c_j = b_j \oplus E(cnt + j \pmod{2^n})$. Izhodna povratna zanka: $c_j = b_j \oplus E^j(IV)[:r]$. Kodna povratna zanka: $l_0 = IV$. Pri vsakem j $O_j = E(l_j), c_j = b_j \oplus O_j[:r], l_j = O_j \cdot 2^r \oplus c_j \pmod{2^n}$.

Digitalni podpisi. Podpišemo izvleček z RSA. Najprej podpišemo, potem šifriramo. ElGamalov sistem podpisovanja. Naj bo p praštevilo in $\alpha^a = \beta$ v $\mathbb{Z} + p^*$. Znani so (p, α, β). Podpisnik izbere naključen k iz $\mathbb{Z}_p^*$ in izračuna podpis $(\gamma, \delta), \gamma = \alpha^k \pmod{p}, \delta = (x - a\gamma)k^{-1} \pmod{p-1}$. Preverimo, če je podpis veljaven $\beta^\gamma \gamma^\delta = \alpha^x \pmod{p}$.

Razširjeni evklidov algoritem. Zadnji neničelen r je ostanek, v tisti vrstici tudi s, t.

	r_0	1	0
q_1	r_1	0	1
q_2	$r_2 = r_0 - q_1 r_1$	$s_2 = s_0 - q_1 s_1$	$t_2 = t_0 - q_1 t_1$

Kitajski izrek o ostankih. $x = a_i \pmod{m_i}$, $m = \prod m_i$. $M_i = m/m_i$. $\exists y_i : y_i M_i = 1 \pmod{m_i}$. $x = \sum a_i y_i M_i \pmod{m}$.