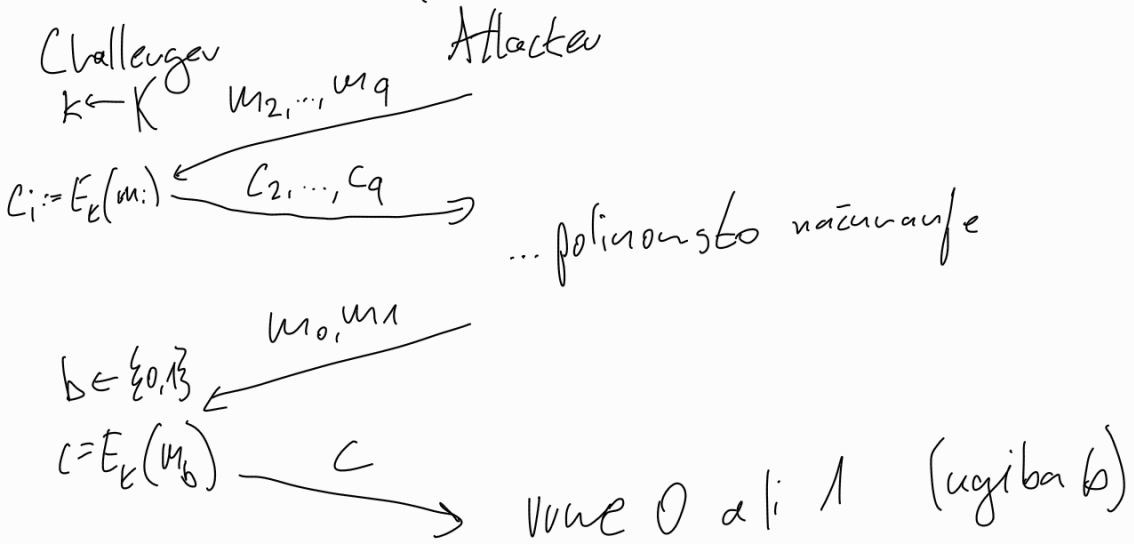
TKKP FMF 2026-03-10

semantična varnost za nečutno šifriranje.

dovolimo, da napadalec vidi šifriranje besedil po svoji izbiri (CPA-varnost / chosen plaintext attack).

Def.: Let $(\mathcal{B}, \mathcal{C}, \mathcal{K}, E, D)$ šifrosistem, E fer $|\mathcal{K}| = 2^\lambda$. Igro



$$Adv(A, E) = |P(A \text{ vrne } 1 \mid b=0) - P(A \text{ vrne } 1 \mid b=1)|$$

Šifrosistem je CPA-varen, če $\forall$ polinomski $A \exists$ zanemarljiva ε_A : $Adv(A, E) \leq \varepsilon_A$

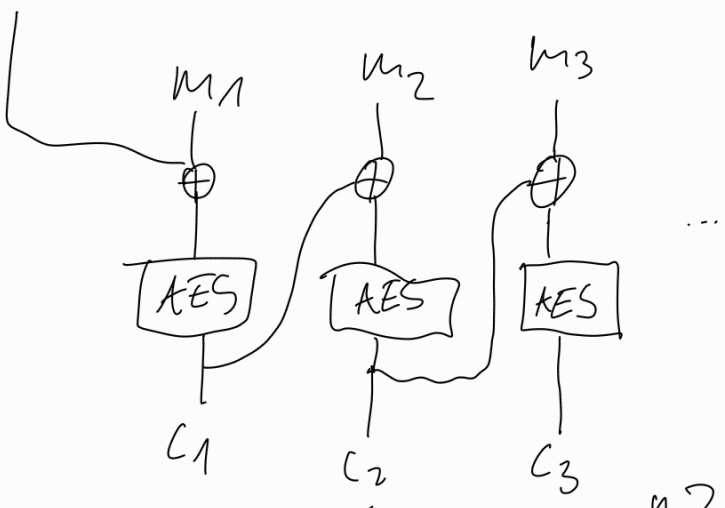
opazba: noben deterministični šifrosistem ni cpa varen

to velja nonce.

ECB slab elektronska kodna knjiga, electronic code book

CBC verižanje kodnih blokov cypher block chaining

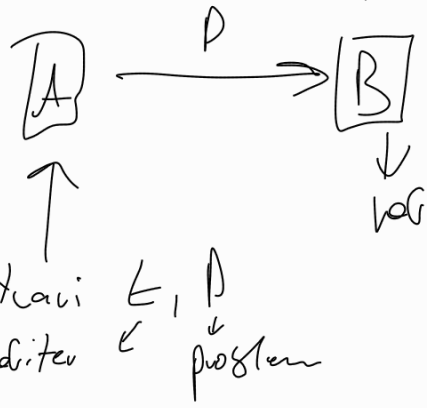
$iv \leftarrow$ naključnih 128 bitov



Izrek: Let $F = \{E_k : \{0,1\}^n \to \{0,1\}^n\}$ varna pseudonaključna permutacija. Potem je šifriranje $E_{CBC,k} : \{0,1\}^{i \cdot n} \to \{0,1\}^{i \cdot n}$ CPA varno. Za vsakega napadalca A, ki napada E_{CBC} $\exists$ napadalec B, ki napada pseudonaključno permutacijo F, da velja $Adv(A, E_{CBC}) \leq 2 Adv(B, F) + 2q^2 i^2 / 2^n$, kjer je q št poizvedb A-ja.

ASIMETRIČNE ŠIFRE

Težava: kaj če bi B znal edini reševati težke matematične probleme?



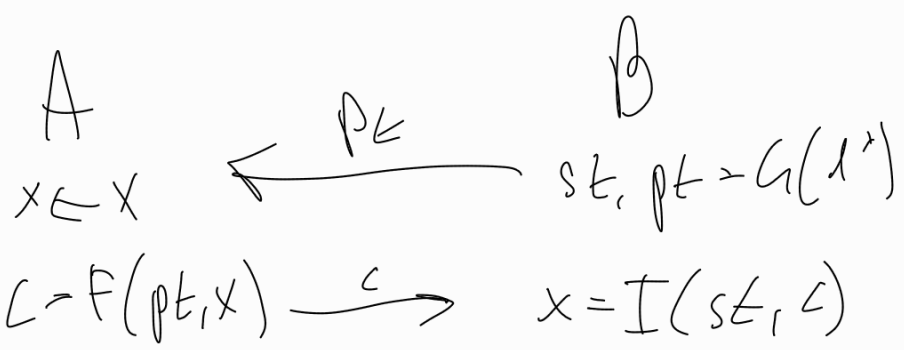
- enosmerne funkcije s povratnimi vrati

Def.: Naj $f: X \to Y$ je enosmerna, če:
- lahko $\forall x \in X$ učinkovito izračunamo $f(x)$
- za slučajen $x \in X$ je verjetnost, da polinomski napadalec A iz $f(x)$ vrne $x' \in X$, da $f(x) = f(x')$, zanemarljiva.

Def.: Shema enosmerne fje s povratnimi vrati je trojica algoritmov:
- $G(1^\lambda)$ je ključavničarski alg., ki vrne $(s_\varepsilon, p_\varepsilon)$, t.j. strimi in javni ključ.
- $F(p_\varepsilon, \cdot)$: deterministični alg. za enosmerno fjo $X \to Y$
- $I(s_\varepsilon, \cdot)$: deterministični alg. za inverz $F(p_\varepsilon, \cdot)$

in $\forall (s_\varepsilon, p_\varepsilon) \leftarrow G(1^\lambda)$ $\forall x \in X$ velja $I(s_\varepsilon, F(p_\varepsilon, x)) = x$

Izmenjava ključa s shemo en. funk. s pov. vrati:



oba imata x.

RSA

osnova

def: problem vsa faktorizacije:

za $\lambda > 0$ naj bosta p, q slučajni λ-bitni praštevili in $n = pq$. problem: iz n izračunaj p, q. polinomski v λ (ne v n).

privedimo problem s pomočjo modularne aritmetike:

$\mathbb{Z}_n^*$ – obrnljivi el. v $\mathbb{Z}_n$ za množenje

$x \in \mathbb{Z}_n$ obrnljiv $\Leftrightarrow \gcd(x, n) = 1$

$|\mathbb{Z}_n^*| = \varphi(n) = (p-1)(q-1)$

eulerjev izrek: $x^{\varphi(n)} \equiv 1 \pmod{n}$ $\forall x \in \mathbb{Z}_n^*$

Def. (problem vsa-inverz):

za $\lambda > 0$ naj bosta p in q slučajni λ-bitni praštevili in $n = pq$. naj bo $e \in \mathbb{Z}_{\varphi(n)}^*$ $e \neq 1$.

problem: izračunaj e^{-1} v $\mathbb{Z}_{\varphi(n)}^*$, če poznaš n (ne pa p, q).

če znamo faktorizirati $n \to pq$, znamo najti vsa-inver.

iztuzi se, da velja tudi obratno.