

riptografie și Securitate

- Prelegerea 8 - Securitate semantică

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

1. Securitate - interceptare simplă
2. Securitate - interceptare multiplă

Securitate semantică - interceptare simplă

- Reamintim: (Enc, Dec) peste spațiul $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ este perfect sigură dacă

$\forall m_0, m_1 \in \mathcal{M}$ cu $|m_0| = |m_1|$ are loc egalitatea

$$\{Enc_k(m_0)\} = \{Enc_k(m_1)\}$$

(distribuțiile sunt identice)

pentru $k \leftarrow^R \mathcal{K}$;

- Incercăm o relaxare:

$\forall m_0, m_1 \in \mathcal{M}$ cu $|m_0| = |m_1|$ are loc

$$\{Enc_k(m_0)\} \approx \{Enc_k(m_1)\}$$

(distribuțiile sunt indistinctibile computațional)

pentru $k \leftarrow^R \mathcal{K}$;

Însă adversarul trebuie să aleagă m_0 și m_1 explicit.

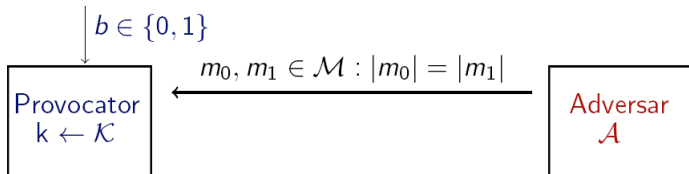
Securitate semantică - interceptare simplă

- ▶ Vom defini securitatea semantică pe baza unui experiment de indistinguibilitate $Priv_{\mathcal{A}, \pi}^{eav}(n)$ unde $\pi = (Enc, Dec)$ este schema de criptare iar n este parametrul de securitate al schemei π
- ▶ Personaje participante: **adversarul** \mathcal{A} care încearcă să spargă schema și un **provocator (challenger)**.
- ▶ Trebuie să definim capabilitățile adversarului: în contextul sistemelor de criptare fluide, el poate vedea **un singur text criptat cu o anume cheie**, fiind un adversar *pasiv* care poate rula atacuri în timp polinomial.

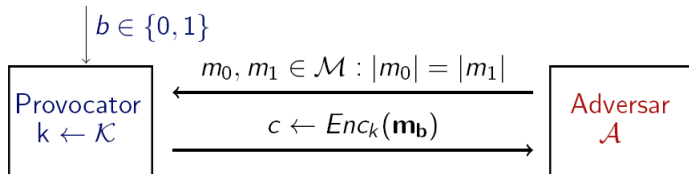
Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{eav}}(n)$



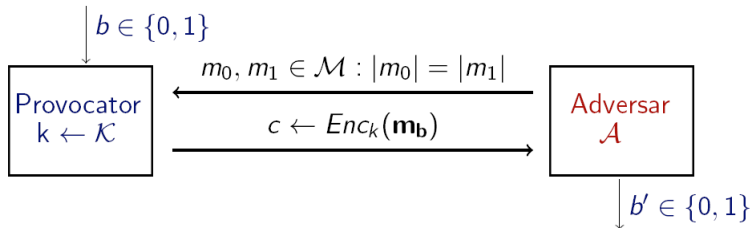
Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{eav}}(n)$



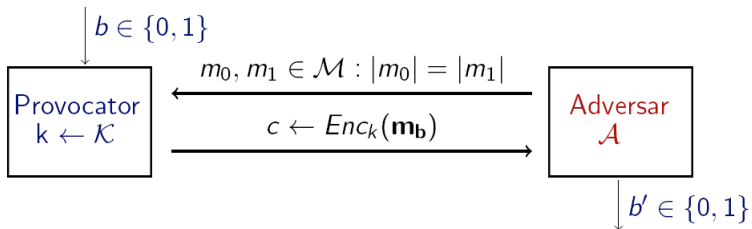
Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{eav}}(n)$



Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{eav}}(n)$



Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{eav}}(n)$



- Output-ul experimentului este 1 dacă $b' = b$ și 0 altfel. Dacă $\text{Priv}_{\mathcal{A}, \pi}^{\text{eav}}(n) = 1$, spunem că \mathcal{A} a efectuat experimentul cu succes.

Securitate semantică - interceptare simplă

Definiție

O schemă de criptare $\pi = (Enc, Dec)$ este indistinctibilă în prezența unui atacator pasiv dacă pentru orice adversar \mathcal{A} există o funcție neglijabilă $negl$ așa încât

$$Pr[Priv_{\mathcal{A}, \pi}^{eav}(n) = 1] \leq \frac{1}{2} + negl(n).$$

- Un adversar pasiv nu poate determina care text clar a fost criptat cu o probabilitate semnificativ mai mare decât dacă ar fi ghicit (în sens aleator, dat cu banul).

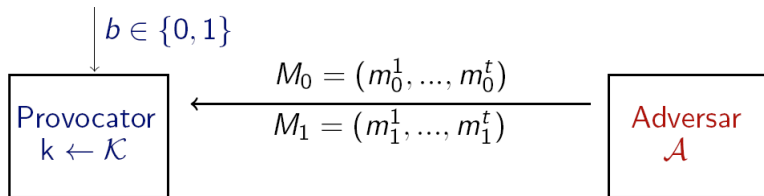
Securitate pentru interceptare multiplă

- ▶ În definiția precedentă am considerat cazul unui adversar care primește **un singur** text criptat;
- ▶ În realitate, în cadrul unei comunicații se trimit **mai multe mesaje** pe care adversarul le poate intercepta;
- ▶ Definim ce înseamnă o schemă sigură chiar și în aceste condiții.

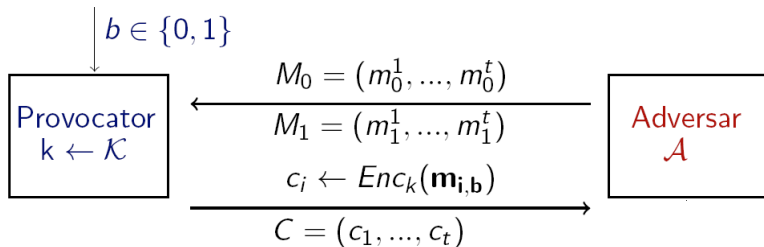
Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{mult}}(n)$



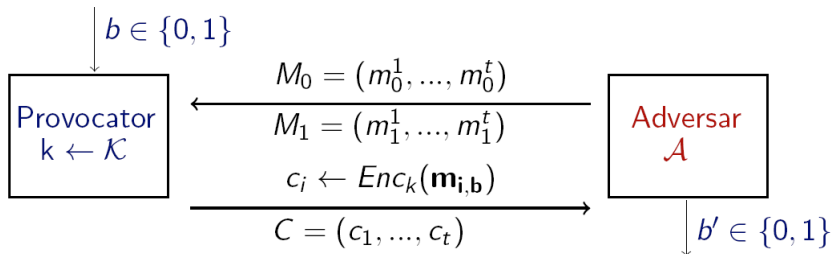
Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{mult}}(n)$



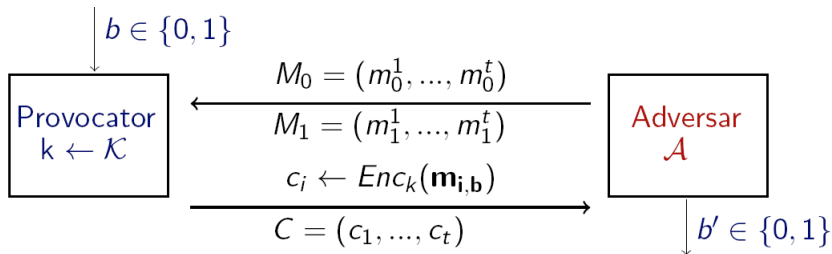
Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{mult}}(n)$



Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{mult}}(n)$



Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{mult}}(n)$



- ▶ Output-ul experimentului este 1 dacă $b' = b$ și 0 altfel;
- ▶ Definiția de securitate este aceeași, doar că se referă la experimentul de mai sus.
- ▶ Securitatea pentru interceptare **simplă** nu implică securitate pentru interceptare **multiplă**!

Securitate pentru interceptare multiplă

Definiție

O schemă de criptare $\pi = (Enc, Dec)$ este indistinctibilă în prezența unui atacator pasiv dacă pentru orice adversar \mathcal{A} există o funcție neglijabilă $negl$ așa încât

$$Pr[Priv_{\mathcal{A}, \pi}^{mult}(n) = 1] \leq \frac{1}{2} + negl(n).$$

Teoremă

O schemă de criptare (Enc, Dec) unde funcția Enc este deterministă nu are proprietatea de securitate la interceptare multiplă conform cu definiția de mai sus.

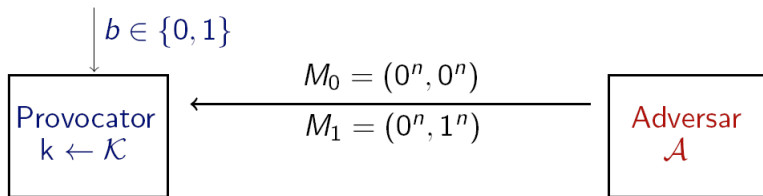
Demonstrație

- ▶ Intuitiv, am vazut că schema OTP este sigură doar când o cheie este folosită o singură dată;
- ▶ La sistemele fluide se întâmplă același lucru;
- ▶ Vom considera un adversar \mathcal{A} care atacă schema (în sensul experimentului $\text{Priv}_{\mathcal{A},\pi}^{mult}(n)$)

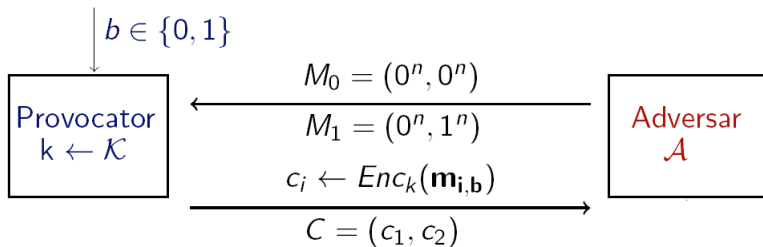
Demonstrație



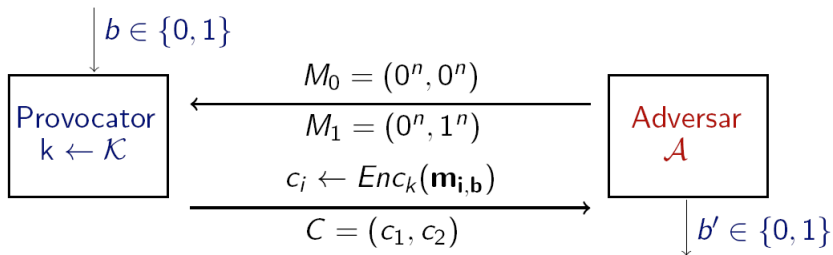
Demonstrație



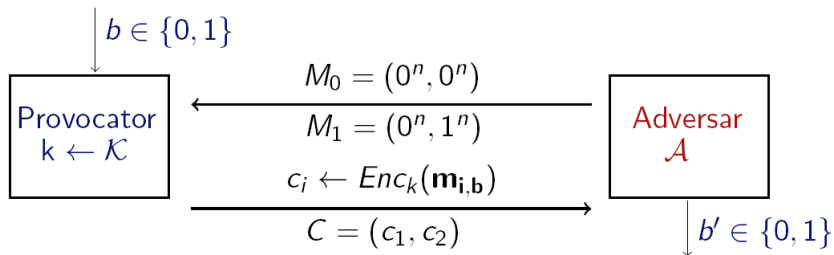
Demonstrație



Demonstrație



Demonstrație



- ▶ Dacă $c_1 = c_2$, atunci \mathcal{A} întoarce 0, altfel \mathcal{A} întoarce 1.
- ▶ Analizăm probabilitatea ca \mathcal{A} să ghicească b : dacă $b = 0$, același mesaj este criptat mereu ($m_0^1 = m_0^2$) iar $c_1 = c_2$ și deci \mathcal{A} întoarce mereu 0;
- ▶ Dacă $b = 1$, atunci ($m_1^1 \neq m_1^2$) iar $c_1 \neq c_2$ și deci \mathcal{A} întoarce mereu 1.

Important de reținut!

- ▶ Securitate - interceptare simplă \nRightarrow securitate - interceptare multiplă
- ▶ Schemele deterministe nu sunt sigure la interceptare multiplă