

# Criptografie și Securitate

## - Prelegerea 19 - Noțiuni de securitate în criptografia asimetrică

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică  
Universitatea din București

# Cuprins

1. Securitate perfectă

2. Securitate semantică = Securitate CPA

# Securitate perfectă

- ▶ Începem studiul securității în același mod în care am început la criptografia simetrică: cu securitatea perfectă;

# Securitate perfectă

- ▶ Începem studiul securității în același mod în care am început la criptografia simetrică: cu securitatea perfectă;
- ▶ Definiția e analoagă cu diferența că adversarul cunoaște, în afara textului criptat, și cheia publică;

# Securitate perfectă

- ▶ Începem studiul securității în același mod în care am început la criptografia simetrică: cu securitatea perfectă;
- ▶ Definiția e analoagă cu diferența că adversarul cunoaște, în afara textului criptat, și cheia publică;

## Definiție

*O schemă de criptare peste un spațiu al mesajelor  $\mathcal{M}$  este perfect sigură dacă pentru orice probabilitate de distribuție peste  $\mathcal{M}$ , pentru orice mesaj  $m \in \mathcal{M}$  și orice text criptat  $c$  cu cheia publică  $pk$  pentru care  $\Pr[C = c] > 0$ , următoarea egalitate este îndeplinită:*

$$\Pr[M = m|C = c] = \Pr[M = m]$$

# Securitate perfectă

- ▶ **Întrebare:** Securitatea perfectă este posibilă în cadrul criptografiei cu cheie publică?

# Securitate perfectă

- ▶ **Întrebare:** Securitatea perfectă este posibilă în cadrul criptografiei cu cheie publică?
- ▶ **Răspuns:** NU! Indiferent lungimea cheilor și a mesajelor;

# Securitate perfectă

- ▶ **Întrebare:** Securitatea perfectă este posibilă în cadrul criptografiei cu cheie publică?
- ▶ **Răspuns:** NU! Indiferent lungimea cheilor și a mesajelor;
- ▶ Având  $pk$  și un text criptat  $c = Enc_{pk}(m)$ , un adversar nelimitat computațional poate determina mesajul  $m$  cu probabilitate 1.



# Securitate semantică

- Securitatea semantică în criptografia cu cheie publică este corespondenta noțiunii similare din criptografia cu cheie secretă;

# Securitate semantică

- ▶ Securitatea semantică în criptografia cu cheie publică este corespondenta noțiunii similare din criptografia cu cheie secretă;
- ▶ Vom defini securitatea semantică pe baza unui experiment de indistinctibilitate  $PubK_{\mathcal{A},\pi}^{eav}(n)$  unde  $\pi = (Enc, Dec)$  este schema de criptare iar  $n$  este parametrul de securitate al schemei  $\pi$ ;

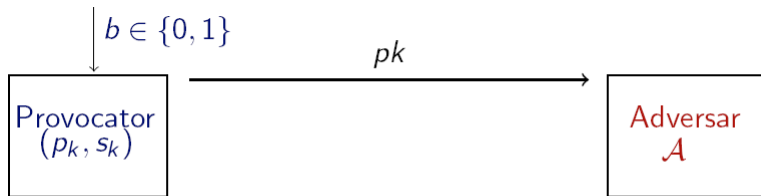
# Securitate semantică

- ▶ Securitatea semantică în criptografia cu cheie publică este corespondenta noțiunii similare din criptografia cu cheie secretă;
- ▶ Vom defini securitatea semantică pe baza unui experiment de indistinguibilitate  $PubK_{\mathcal{A},\pi}^{eav}(n)$  unde  $\pi = (Enc, Dec)$  este schema de criptare iar  $n$  este parametrul de securitate al schemei  $\pi$ ;
- ▶ Personaje participante: **adversarul**  $\mathcal{A}$  care încearcă să spargă schema și un **provocator (challenger)**.

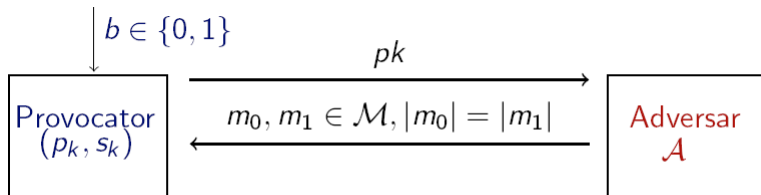
# Experimentul $\text{PubK}_{\mathcal{A}, \pi}^{\text{eav}}(n)$



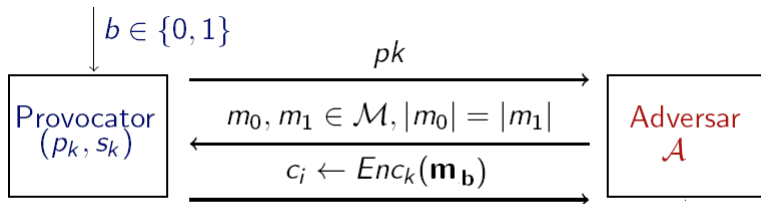
# Experimentul $\text{PubK}_{\mathcal{A}, \pi}^{\text{eav}}(n)$



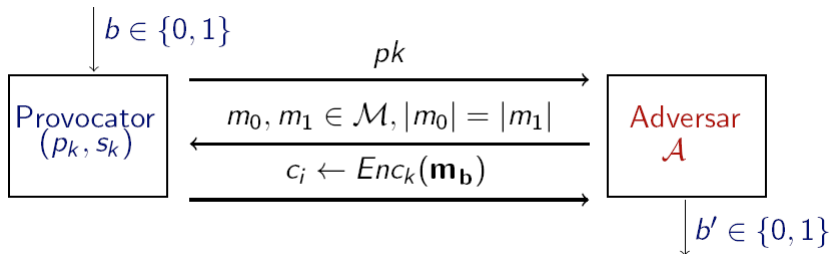
## Experimentul $\text{PubK}_{\mathcal{A}, \pi}^{\text{eav}}(n)$



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

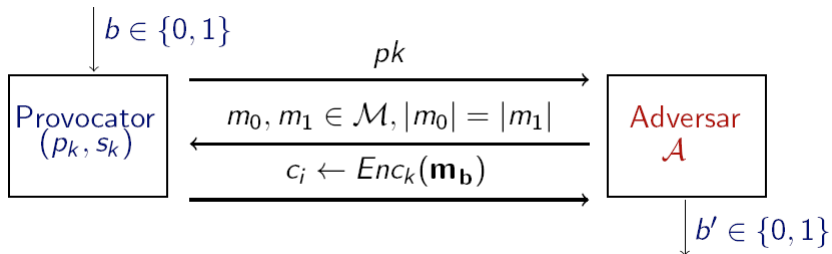


## Experimentul $\text{PubK}_{\mathcal{A}, \pi}^{\text{eav}}(n)$

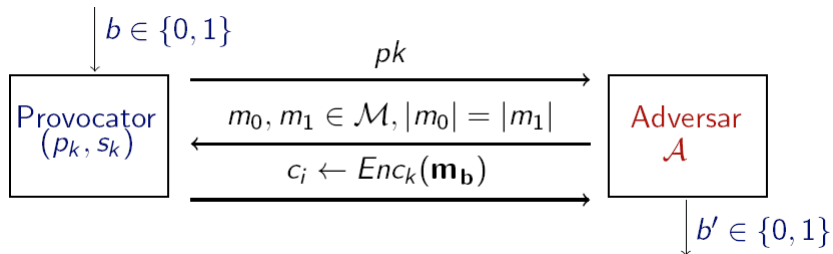




# Experimentul $\text{PubK}_{\mathcal{A},\pi}^{\text{eav}}(n)$



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



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

# Securitate pentru 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*

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

# Securitate pentru interceptare simplă

- ▶ Principala diferență față de definiția similară studiată la criptografia cu cheie secretă este că  $\mathcal{A}$  primește cheia publică  $pk$ ;

## Securitate pentru interceptare simplă

- ▶ Principala diferență față de definiția similară studiată la criptografia cu cheie secretă este că  $\mathcal{A}$  primește cheia publică  $pk$ ;
- ▶ Adică  $\mathcal{A}$  primește acces *gratuit* la un oracol de criptare, ceea ce înseamnă că el poate calcula  $Enc_{pk}(m)$  pentru orice  $m$ ;

# Securitate pentru interceptare simplă

- ▶ Principala diferență față de definiția similară studiată la criptografia cu cheie secretă este că  $\mathcal{A}$  primește cheia publică  $pk$ ;
- ▶ Adică  $\mathcal{A}$  primește acces *gratuit* la un oracol de criptare, ceea ce înseamnă că el poate calcula  $Enc_{pk}(m)$  pentru orice  $m$ ;
- ▶ Prin urmare, definiția este echivalentă cu cea pentru securitate CPA (nu mai este necesar oracolul de criptare pentru că  $\mathcal{A}$  își poate cripta singur mesajele);

# Securitate pentru interceptare simplă

- ▶ Principala diferență față de definiția similară studiată la criptografia cu cheie secretă este că  $\mathcal{A}$  primește cheia publică  $pk$ ;
- ▶ Adică  $\mathcal{A}$  primește acces *gratuit* la un oracol de criptare, ceea ce înseamnă că el poate calcula  $Enc_{pk}(m)$  pentru orice  $m$ ;
- ▶ Prin urmare, definiția este echivalentă cu cea pentru securitate CPA (nu mai este necesar oracolul de criptare pentru că  $\mathcal{A}$  își poate cripta singur mesajele);
- ▶ Reamintim că în criptografia simetrică există scheme sigure la securitate semantică dar care nu sunt CPA-sigure .

# Insecuritatea schemelor deterministe

- ▶ După cum am văzut la criptografia simetrică, nici o schemă deterministă nu poate fi CPA sigură;



# Insecuritatea schemelor deterministe

- ▶ După cum am văzut la criptografia simetrică, nici o schemă deterministă nu poate fi CPA sigură;
- ▶ Datorită echivalenței între noțiunile de securitate CPA și securitate semantică pentru interceptare simplă (în criptografia asimetrică) concluzionăm că:

## Teoremă

*Nici o schemă de criptare cu cheie publică deterministă nu poate fi semantic sigură pentru interceptarea simplă.*

# Insecuritatea schemelor deterministe

- ▶ În realitate, schemele de criptare cu cheie publică deterministe sunt vulnerabile la atacuri practice;

# Insecuritatea schemelor deterministe

- ▶ În realitate, schemele de criptare cu cheie publică deterministe sunt vulnerabile la atacuri practice;
- ▶ Acestea permit unui adversar să determine când un mesaj este trimis de două ori;

# Insecuritatea schemelor deterministe

- ▶ În realitate, schemele de criptare cu cheie publică deterministe sunt vulnerabile la atacuri practice;
- ▶ Acestea permit unui adversar să determine când un mesaj este trimis de două ori;
- ▶ Mai mult, îi permit să găsească mesajul  $m$  cu probabilitate 1, dacă spațiul mesajelor este mic.

# Criptare multiplă

- ▶ Definim noțiunea de securitate la interceptare multiplă analog cu definiția similară din criptografia simetrică, pe baza unui experiment;

# Criptare multiplă

- ▶ Definim noțiunea de securitate la interceptare multiplă analog cu definiția similară din criptografia simetrică, pe baza unui experiment;
- ▶ Este clar că ea e echivalentă cu o definiție în care sunt considerate atacuri CPA;

# Criptare multiplă

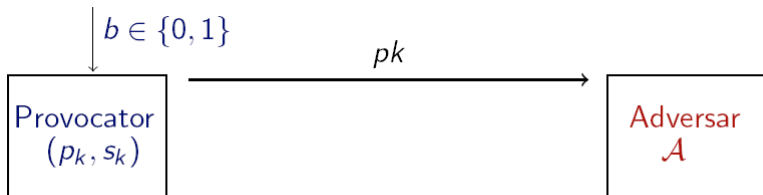
- ▶ Definim noțiunea de securitate la interceptare multiplă analog cu definiția similară din criptografia simetrică, pe baza unui experiment;
- ▶ Este clar că ea e echivalentă cu o definiție în care sunt considerate atacuri CPA;
- ▶ De remarcat că securitatea la interceptare simplă implică securitate la interceptare multiplă;

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

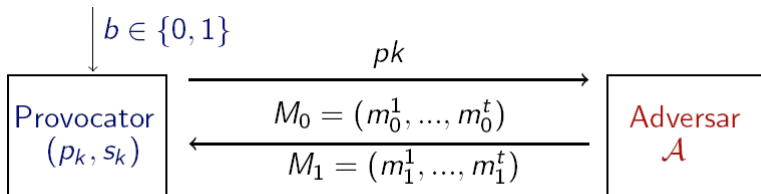




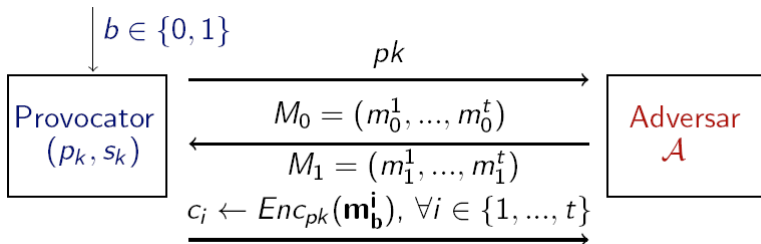
# Experimentul $\text{PubK}_{\mathcal{A}, \pi}^{\text{mult}}(n)$



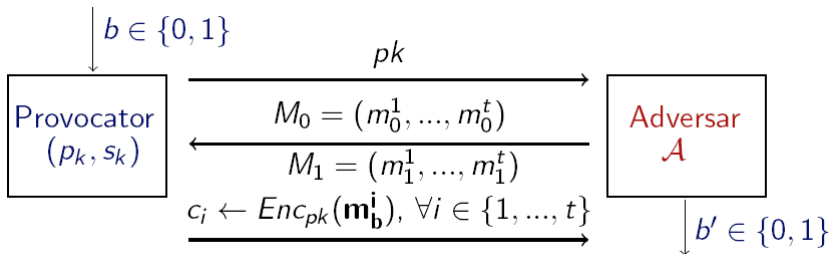
# Experimentul $\text{PubK}_{\mathcal{A}, \pi}^{\text{mult}}(n)$



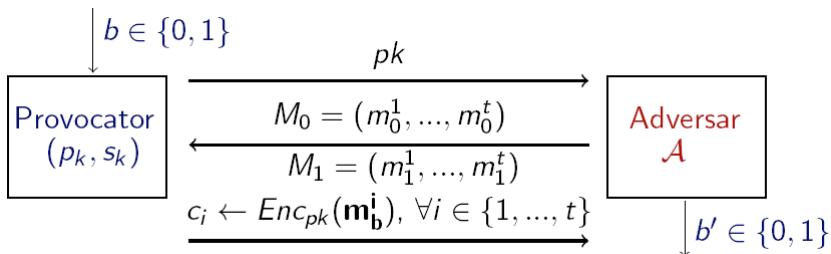
# Experimentul $\text{PubK}_{\mathcal{A}, \pi}^{\text{mult}}(n)$



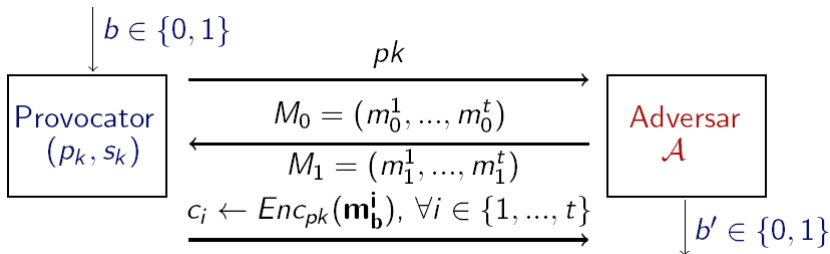
# Experimentul $\text{PubK}_{\mathcal{A}, \pi}^{\text{mult}}(n)$



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

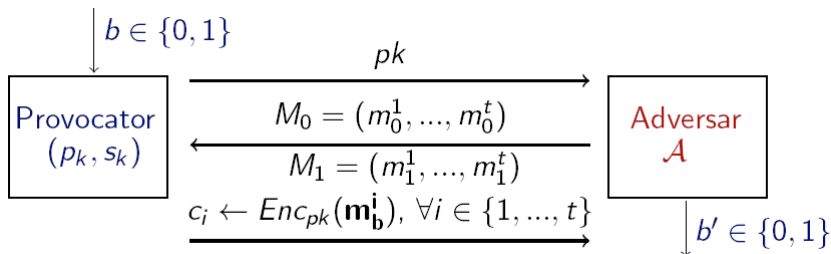


## Experimentul $\text{PubK}_{\mathcal{A}, \pi}^{\text{mult}}(n)$



- Output-ul experimentului este 1 dacă  $b' = b$  și 0 altfel;

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



- 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.

# Securitate pentru interceptare multiplă

## Definiție

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

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



# Securitate pentru interceptare multiplă

## Definiție

*O schemă de criptare  $\pi = (Enc, Dec)$  este indistinctibilă în prezența unui adversar (este semantic sigură) 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

*Dacă o schemă de criptare cu cheie publică este sigură la interceptare simplă, atunci ea este sigură și la interceptare multiplă.*

# Criptarea mesajelor de lungime arbitrară

- Consecință a rezultatului anterior: o schemă de criptare sigură pentru mesaje de *lungime fixă* este sigură și pentru mesaje de *lungime arbitrară*;

## Criptarea mesajelor de lungime arbitrară

- Consecință a rezultatului anterior: o schemă de criptare sigură pentru mesaje de *lungime fixă* este sigură și pentru mesaje de *lungime arbitrară*;
- Dacă  $\pi = (\text{Enc}, \text{Dec})$  este o schemă de criptare cu spațiul mesajelor  $\mathcal{M} = \{0, 1\}$ , putem construi o schemă sigură peste spațiul mesajelor  $\mathcal{M} = \{0, 1\}^*$  definind  $\text{Enc}'$ :

$$\text{Enc}'_{pk}(m) = \text{Enc}_{pk}(m_1), \dots, \text{Enc}_{pk}(m_t)$$

unde  $m = m_1 \dots m_t$

## Criptarea mesajelor de lungime arbitrară

- ▶ Consecință a rezultatului anterior: o schemă de criptare sigură pentru mesaje de *lungime fixă* este sigură și pentru mesaje de *lungime arbitrară*;
- ▶ Dacă  $\pi = (\text{Enc}, \text{Dec})$  este o schemă de criptare cu spațiul mesajelor  $\mathcal{M} = \{0, 1\}$ , putem construi o schemă sigură peste spațiul mesajelor  $\mathcal{M} = \{0, 1\}^*$  definind  $\text{Enc}'$ :

$$\text{Enc}'_{pk}(m) = \text{Enc}_{pk}(m_1), \dots, \text{Enc}_{pk}(m_t)$$

unde  $m = m_1 \dots m_t$

- ▶ Rezultatul este adevărat pentru atacuri CPA dar nu este adevărat pentru atacuri CCA.

# Securitate CCA

- ▶ Noțiunea de securitate CCA rămâne identică cu cea de la sistemele simetrice;

# Securitate CCA

- ▶ Noțiunea de securitate CCA rămâne identică cu cea de la sistemele simetrice;
- ▶ Capabilitățile adversarului: el poate interacționa cu un **oracol de decriptare**, fiind un adversar *activ* care poate rula atacuri în timp polinomial;

# Securitate CCA

- ▶ Noțiunea de securitate CCA rămâne identică cu cea de la sistemele simetrice;
- ▶ Capabilitățile adversarului: el poate interacționa cu un **oracol de decriptare**, fiind un adversar *activ* care poate rula atacuri în timp polinomial;
- ▶ Adversarul poate transmite către oracolul de decriptare *anumite* mesaje  $c$  și primește înapoi mesajul clar corespunzător;

# Securitate CCA

- ▶ Noțiunea de securitate CCA rămâne identică cu cea de la sistemele simetrice;
- ▶ Capabilitățile adversarului: el poate interacționa cu un **oracol de decriptare**, fiind un adversar *activ* care poate rula atacuri în timp polinomial;
- ▶ Adversarul poate transmite către oracolul de decriptare *anumite* mesaje  $c$  și primește înapoi mesajul clar corespunzător;
- ▶ Ca și în cazul securității CPA, adversarul nu mai necesită acces la oracolul de criptare pentru că deține cheia publică  $pk$  și poate realiza singur criptarea oricărui mesaj  $m$ .



# Important de reținut!

- ▶ În criptografia cu cheie publică:
  - ▶ NU există securitate perfectă
  - ▶ securitate semantică = securitate CPA