

# Criptografie și Securitate

## - Prelegerea 21.2 - Sistemul de criptare ElGamal

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică  
Universitatea din București

# Cuprins

1. Scurt istoric
2. Sistemul de criptare ElGamal
3. Securitate

# Sistemul de criptare ElGamal

- ▶ 1976 - Diffie și Hellman definesc conceptul de criptografie asimetrică;

# Sistemul de criptare ElGamal

- ▶ 1976 - Diffie și Hellman definesc conceptul de criptografie asimetrică;
- ▶ 1977 - R.Rivest, A.Shamir și Leonard Adleman introduc sistemul RSA;

# Sistemul de criptare ElGamal

- ▶ 1976 - Diffie și Hellman definesc conceptul de criptografie asimetrică;
- ▶ 1977 - R.Rivest, A.Shamir și Leonard Adleman introduc sistemul RSA;
- ▶ 1985 - T.ElGamal propune un nou sistem de criptare.

# Sistemul de criptare ElGamal

- ▶ Se bazează pe DLP ...

# Sistemul de criptare ElGamal

- ▶ Se bazează pe DLP ...
- ▶ ... sau mai exact pe dificultatea problemei DDH...

# Sistemul de criptare ElGamal

- ▶ Se bazează pe DLP ...
- ▶ ... sau mai exact pe dificultatea problemei DDH...
- ▶ ... și pe următoarea observație simplă:



# Sistemul de criptare ElGamal

- ▶ Se bazează pe DLP ...
- ▶ ... sau mai exact pe dificultatea problemei DDH...
- ▶ ... și pe următoarea observație simplă:

## Observație

*Fie  $\mathbb{G}$  un grup finit și  $m \leftarrow^R \mathbb{G}$ . Dacă  $g \leftarrow^R \mathbb{G}$ , atunci  $g' = m \cdot g$  rămâne aleator în  $\mathbb{G}$ :*

$$Pr[m \cdot g = g'] = 1/|\mathbb{G}|$$

*unde probabilitatea este dată de alegerea aleatoare a lui  $g$ .*

# Sistemul de criptare ElGamal

- ▶ Dacă emitătorul și receptorul folosesc  $g$  drept cheie secretă, atunci un mesaj  $m \in \mathbb{G}$  se criptează ca:

$$g' = m \cdot g$$

# Sistemul de criptare ElGamal

- ▶ Dacă emitătorul și receptorul folosesc  $g$  drept cheie secretă, atunci un mesaj  $m \in \mathbb{G}$  se criptează ca:

$$g' = m \cdot g$$

- ▶ Receptorul decriptează:

$$m = g' \cdot g^{-1}$$

# Sistemul de criptare ElGamal

- ▶ Dacă emitătorul și receptorul folosesc  $g$  drept cheie secretă, atunci un mesaj  $m \in \mathbb{G}$  se criptează ca:

$$g' = m \cdot g$$

- ▶ Receptorul decriptează:

$$m = g' \cdot g^{-1}$$

- ▶ Abordarea este asemănătoare cu OTP, unde se folosea grupul secvențelor de lungime fixată împreună cu operația XOR;

# Sistemul de criptare ElGamal

- ▶ Dacă emitătorul și receptorul folosesc  $g$  drept cheie secretă, atunci un mesaj  $m \in \mathbb{G}$  se criptează ca:

$$g' = m \cdot g$$

- ▶ Receptorul decriptează:

$$m = g' \cdot g^{-1}$$

- ▶ Abordarea este asemănătoare cu OTP, unde se folosea grupul secvențelor de lungime fixată împreună cu operația XOR;
- ▶ O astfel de construcție este deci perfect sigură (dacă  $g$  este total aleator!).

# Sistemul de criptare ElGamal

- ▶ În criptografia cu cheie publică, se folosește  $g$  **pseudoaleator**, deci se pierde securitatea perfectă;

# Sistemul de criptare ElGamal

- ▶ În criptografia cu cheie publică, se folosește  $g$  **pseudoaleator**, deci se pierde securitatea perfectă;
- ▶ Ideea de bază este alegerea lui  $g$  astfel încât la recepție să poată fi *calculat* pe baza cheii secrete...

# Sistemul de criptare ElGamal

- ▶ În criptografia cu cheie publică, se folosește  $g$  **pseudoaleator**, deci se pierde securitatea perfectă;
- ▶ Ideea de bază este alegerea lui  $g$  astfel încât la recepție să poată fi *calculat* pe baza cheii secrete...
- ▶ ... dar  $g$  să *pară aleator* pentru un adversar;



# Sistemul de criptare ElGamal

- ▶ În criptografia cu cheie publică, se folosește  $g$  **pseudoaleator**, deci se pierde securitatea perfectă;
- ▶ Ideea de bază este alegerea lui  $g$  astfel încât la recepție să poată fi *calculat* pe baza cheii secrete...
- ▶ ... dar  $g$  să *pară aleator* pentru un adversar;
- ▶ Pentru aceasta se folosește prezumția DDH, construcția fiind imediată din schimbul de chei Diffie-Hellman.

# Sistemul de criptare ElGamal

- ▶ Definim sistemul de criptare *ElGamal* pe baza ideii prezentate anterior;
- 1. Se generează  $(\mathbb{G}, q, g)$ , se alege  $x \xleftarrow{R} \mathbb{Z}_q$  și se calculează  $h = g^x$ ;
  - ▶ Cheia publică este:  $(\mathbb{G}, q, g, h)$ ;
  - ▶ Cheia privată este  $(\mathbb{G}, q, g, x)$ ;
- 2. **Enc:** dată o cheie publică  $(\mathbb{G}, q, g, h)$  și un mesaj  $m \in \mathbb{G}$ , alege  $y \xleftarrow{R} \mathbb{Z}_q$  și întoarce  $c = (c_1, c_2) = (g^y, m \cdot h^y)$ ;
- 3. **Dec:** dată o cheie secretă  $(\mathbb{G}, q, g, x)$  și un mesaj criptat  $c = (c_1, c_2)$ , întoarce  $m = c_2 \cdot c_1^{-x}$ .

# Securitate - Problema 1

## Problema 1: Determinismul

- **Întrebare:** Este sistemul ElGamal determinist?

# Securitate - Problema 1

## Problema 1: Determinismul

- ▶ **Întrebare:** Este sistemul ElGamal determinist?
- ▶ **Răspuns:** NU! Sistemul este nedeterminist, datorită alegerii aleatoare a lui  $y$  la fiecare criptare.

# Securitate - Problema 1

## Problema 1: Determinismul

- ▶ **Întrebare:** Este sistemul ElGamal determinist?
- ▶ **Răspuns:** NU! Sistemul este nedeterminist, datorită alegerii aleatoare a lui  $y$  la fiecare criptare.
- ▶ Un același mesaj  $m$  se poate cripta diferit, pentru  $y \neq y'$ :

$$c = (c_1, c_2) = (g^y, m \cdot h^y)$$

$$c' = (c'_1, c'_2) = (g^{y'}, m \cdot h^{y'})$$

# Securitate - Problema 1

## Problema 1: Determinismul

- ▶ **Întrebare:** Este sistemul ElGamal determinist?
- ▶ **Răspuns:** NU! Sistemul este nedeterminist, datorită alegerii aleatoare a lui  $y$  la fiecare criptare.
- ▶ Un același mesaj  $m$  se poate cripta diferit, pentru  $y \neq y'$ :

$$c = (c_1, c_2) = (g^y, m \cdot h^y)$$

$$c' = (c'_1, c'_2) = (g^{y'}, m \cdot h^{y'})$$

- ▶ În caz contrar, sistemul NU ar putea fi CPA-sigur.

# Securitate - Problema 2

## Problema 2: Dificultatea DLP

- **Întrebare:** Rămâne ElGamal sigur dacă problema DLP este simplă?

# Securitate - Problema 2

## Problema 2: Dificultatea DLP

- ▶ **Întrebare:** Rămâne ElGamal sigur dacă problema DLP este simplă?
- ▶ **Răspuns:** NU! Se determină  $x$  a.î.  $h = g^x$ , apoi se decriptează orice mesaj pentru că se cunoaște cheia secretă.



## Securitate - Problema 3

### Problema 3: Proprietatea de homomorfism

- Fie  $m_1, m_2$  2 texte clare și  $c_1 = (c_{11}, c_{12}), c_2 = (c_{21}, c_{22})$  textele criptate corespunzătoare;

# Securitate - Problema 3

## Problema 3: Proprietatea de homomorfism

- Fie  $m_1, m_2$  2 texte clare și  $c_1 = (c_{11}, c_{12}), c_2 = (c_{21}, c_{22})$  textele criptate corespunzătoare;

- Atunci:

$$c_1 \cdot c_2 = (c_{11} \cdot c_{21}, c_{12} \cdot c_{22}) = (g^{y_1} \cdot g^{y_2}, m_1 h^{y_1} \cdot m_2 h^{y_2})$$

## Securitate - Problema 3

### Problema 3: Proprietatea de homomorfism

- ▶ Fie  $m_1, m_2$  2 texte clare și  $c_1 = (c_{11}, c_{12}), c_2 = (c_{21}, c_{22})$  textele criptate corespunzătoare;
- ▶ Atunci:
$$c_1 \cdot c_2 = (c_{11} \cdot c_{21}, c_{12} \cdot c_{22}) = (g^{y_1} \cdot g^{y_2}, m_1 h^{y_1} \cdot m_2 h^{y_2})$$
- ▶ **Întrebare:** Dacă un adversar cunoaște  $c_1$  și  $c_2$  criptările lui  $m_1$ , respectiv  $m_2$ , ce poate spune despre  $c_1 \cdot c_2$ ?

## Securitate - Problema 3

### Problema 3: Proprietatea de homomorfism

- ▶ Fie  $m_1, m_2$  2 texte clare și  $c_1 = (c_{11}, c_{12})$ ,  $c_2 = (c_{21}, c_{22})$  textele criptate corespunzătoare;
- ▶ Atunci:  
$$c_1 \cdot c_2 = (c_{11} \cdot c_{21}, c_{12} \cdot c_{22}) = (g^{y_1} \cdot g^{y_2}, m_1 h^{y_1} \cdot m_2 h^{y_2})$$
- ▶ **Întrebare:** Dacă un adversar cunoaște  $c_1$  și  $c_2$  criptările lui  $m_1$ , respectiv  $m_2$ , ce poate spune despre  $c_1 \cdot c_2$ ?
- ▶ **Răspuns:**  $c_1 \cdot c_2$  este criptarea lui  $m_1 \cdot m_2$  folosind  $y = y_1 + y_2$ :  
$$c_1 \cdot c_2 = (g^{y_1+y_2}, m_1 m_2 h^{y_1+y_2})$$

# Securitate - Problema 3

## Problema 3: Proprietatea de homomorfism

- ▶ Fie  $m_1, m_2$  2 texte clare și  $c_1 = (c_{11}, c_{12}), c_2 = (c_{21}, c_{22})$  textele criptate corespunzătoare;
- ▶ Atunci:  
$$c_1 \cdot c_2 = (c_{11} \cdot c_{21}, c_{12} \cdot c_{22}) = (g^{y_1} \cdot g^{y_2}, m_1 h^{y_1} \cdot m_2 h^{y_2})$$
- ▶ **Întrebare:** Dacă un adversar cunoaște  $c_1$  și  $c_2$  criptările lui  $m_1$ , respectiv  $m_2$ , ce poate spune despre  $c_1 \cdot c_2$ ?
- ▶ **Răspuns:**  $c_1 \cdot c_2$  este criptarea lui  $m_1 \cdot m_2$  folosind  $y = y_1 + y_2$ :  
$$c_1 \cdot c_2 = (g^{y_1+y_2}, m_1 m_2 h^{y_1+y_2})$$
- ▶ Un sistem de criptare care satisface  
$$Dec_{sk}(c_1 \cdot c_2) = Dec_{sk}(c_1) \cdot Dec_{sk}(c_2)$$
 se numește sistem de criptare **homomorfic**.  
(homomorfismul este deseori o proprietate utilă în criptografie)

# Securitate - Problema 4

## Problema 4: Utilizarea multiplă a parametrilor publici

- Este comun în practică pentru un administrator să fixeze parametrii publici  $(\mathbb{G}, q, g)$ , apoi fiecare utilizator să își genereze doar cheia secretă  $x$  și să publice  $h = g^x$ ;

# Securitate - Problema 4

## Problema 4: Utilizarea multiplă a parametrilor publici

- ▶ Este comun în practică pentru un administrator să fixeze parametrii publici  $(\mathbb{G}, q, g)$ , apoi fiecare utilizator să își genereze doar cheia secretă  $x$  și să publice  $h = g^x$ ;
- ▶ **Întrebare:** Este corect să se utilizeze de mai multe ori aceiași parametrii publici  $(\mathbb{G}, q, g)$ ?

# Securitate - Problema 4

## Problema 4: Utilizarea multiplă a parametrilor publici

- ▶ Este comun în practică pentru un administrator să fixeze parametrii publici  $(\mathbb{G}, q, g)$ , apoi fiecare utilizator să își genereze doar cheia secretă  $x$  și să publice  $h = g^x$ ;
- ▶ **Întrebare:** Este corect să se utilizeze de mai multe ori aceiași parametrii publici  $(\mathbb{G}, q, g)$ ?
- ▶ **Răspuns:** Se consideră că DA. Cunoașterea parametrilor publici pare să nu conducă la rezolvarea DDH.



# Securitate - Problema 4

## Problema 4: Utilizarea multiplă a parametrilor publici

- ▶ Este comun în practică pentru un administrator să fixeze parametrii publici  $(\mathbb{G}, q, g)$ , apoi fiecare utilizator să își genereze doar cheia secretă  $x$  și să publice  $h = g^x$ ;
- ▶ **Întrebare:** Este corect să se utilizeze de mai multe ori aceiași parametrii publici  $(\mathbb{G}, q, g)$ ?
- ▶ **Răspuns:** Se consideră că DA. Cunoașterea parametrilor publici pare să nu conducă la rezolvarea DDH.
- ▶ **Atenție!** Acest lucru nu se întâmplă și la RSA, unde modulul NU trebuie utilizat de mai multe ori.

# Securitate - teoremă

## Teoremă

*Dacă problema decizională Diffie-Hellman (DDH) este dificilă în grupul  $\mathbb{G}$ , atunci schema de criptare ElGamal este CPA-sigură.*

# Securitate - teoremă

## Teoremă

*Dacă problema decizională Diffie-Hellman (DDH) este dificilă în grupul  $\mathbb{G}$ , atunci schema de criptare ElGamal este CPA-sigură.*

- Notăm cu  $\Pi$  schema de criptare ElGamal. E suficient să arătăm că schema este sigură la interceptare simplă;

# Securitate - teoremă

## Teoremă

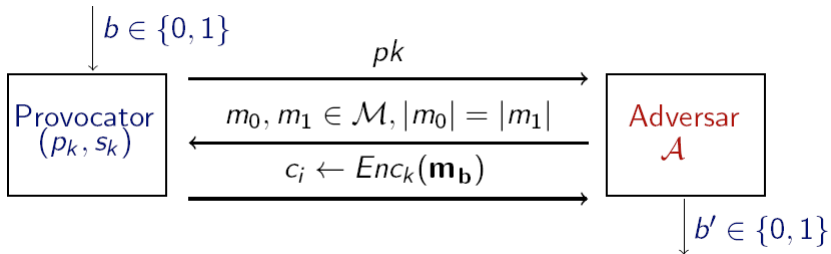
*Dacă problema decizională Diffie-Hellman (DDH) este dificilă în grupul  $\mathbb{G}$ , atunci schema de criptare ElGamal este CPA-sigură.*

- ▶ Notăm cu  $\Pi$  schema de criptare ElGamal. E suficient să arătăm că schema este sigură la interceptare simplă;
- ▶ Fie  $\mathcal{A}$  un adversar PPT; notăm cu

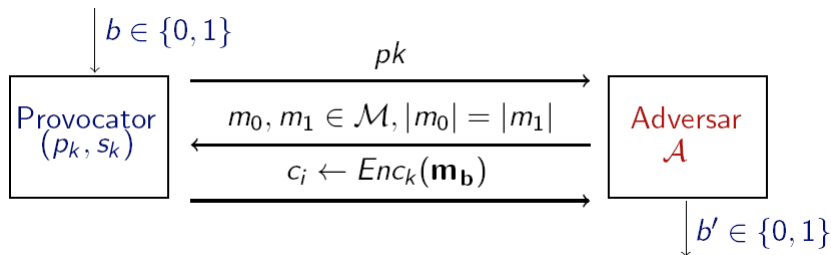
$$\epsilon(n) = \Pr[\text{PubK}_{\mathcal{A}, \Pi}^{\text{eav}}(n) = 1]$$

probabilitatea ca  $\mathcal{A}$  să câștige experimentul de mai jos folosit pentru a defini securitatea la interceptare simplă.

# Demonstrație



# Demonstrație



- Considerăm schema modificată  $\tilde{\Pi}$  care diferă de schema  $\Pi$  prin faptul că algoritmul de criptare alege aleator  $y, z \leftarrow \mathbb{Z}_q$  și întoarce textul criptat

$$(g^y, g^z \cdot m)$$

# Demonstrație

- ▶ A doua componentă a textului criptat din  $\tilde{\Pi}$  este un element uniform distribuit din  $\mathbb{G}$  și independent de  $m$ ;

# Demonstrație

- ▶ A doua componentă a textului criptat din  $\tilde{\Pi}$  este un element uniform distribuit din  $\mathbb{G}$  și independent de  $m$ ;
- ▶ Prima componentă este și ea independentă de  $m$ ; rezultă că

$$\Pr[\text{PubK}_{\mathcal{A}, \tilde{\Pi}}^{\text{eav}}(n) = 1] = \frac{1}{2}$$



# Demonstrație

- ▶ A doua componentă a textului criptat din  $\tilde{\Pi}$  este un element uniform distribuit din  $\mathbb{G}$  și independent de  $m$ ;
- ▶ Prima componentă este și ea independentă de  $m$ ; rezultă că

$$\Pr[PubK_{\mathcal{A}, \tilde{\Pi}}^{eav}(n) = 1] = \frac{1}{2}$$

- ▶ Deși  $\tilde{\Pi}$  nu e o schemă de criptare (nu se poate decripta), experimentul  $PubK_{\mathcal{A}, \tilde{\Pi}}^{eav}(n)$  este bine-definit pentru că folosește doar algoritmul de criptare;

# Demonstrație

- ▶ A doua componentă a textului criptat din  $\tilde{\Pi}$  este un element uniform distribuit din  $\mathbb{G}$  și independent de  $m$ ;
- ▶ Prima componentă este și ea independentă de  $m$ ; rezultă că

$$\Pr[PubK_{\mathcal{A}, \tilde{\Pi}}^{eav}(n) = 1] = \frac{1}{2}$$

- ▶ Deși  $\tilde{\Pi}$  nu e o schemă de criptare (nu se poate decripta), experimentul  $PubK_{\mathcal{A}, \tilde{\Pi}}^{eav}(n)$  este bine-definit pentru că folosește doar algoritmul de criptare;
- ▶ Aratăm că  $\mathcal{A}$  poate fi folosit de un algoritm  $\mathcal{D}$  ca o subrutină pentru a rezolva problema DDH cu probabilitate  $\epsilon(n)$ ;

# Demonstrație

- ▶ Algoritmul  $\mathcal{D}$  primește la intrare tuplul  $(\mathbb{G}, q, g, g_1, g_2, g_3)$ , unde  $g_1 = g^x, g_2 = g^y$  și  $g_3 = g^{xy}$  sau  $g_3 = g^z$  pentru  $x, y, z$  aleatoare, după care:

# Demonstrație

- ▶ Algoritmul  $\mathcal{D}$  primește la intrare tuplul  $(\mathbb{G}, q, g, g_1, g_2, g_3)$ , unde  $g_1 = g^x, g_2 = g^y$  și  $g_3 = g^{xy}$  sau  $g_3 = g^z$  pentru  $x, y, z$  aleatoare, după care:
  1. Alege  $pk = (\mathbb{G}, q, g, g_1)$  și execută  $\mathcal{A}(pk)$  și obține două mesaje  $m_0$  și  $m_1$ ;

# Demonstrație

- ▶ Algoritmul  $\mathcal{D}$  primește la intrare tuplul  $(\mathbb{G}, q, g, g_1, g_2, g_3)$ , unde  $g_1 = g^x$ ,  $g_2 = g^y$  și  $g_3 = g^{xy}$  sau  $g_3 = g^z$  pentru  $x, y, z$  aleatoare, după care:
  1. Alege  $pk = (\mathbb{G}, q, g, g_1)$  și execută  $\mathcal{A}(pk)$  și obține două mesaje  $m_0$  și  $m_1$ ;
  2. Alege un bit aleator  $b$  și notează  $c_1 = g_2$  și  $c_2 = g_3 \cdot m_b$ ;

# Demonstrație

- ▶ Algoritmul  $\mathcal{D}$  primește la intrare tuplul  $(\mathbb{G}, q, g, g_1, g_2, g_3)$ , unde  $g_1 = g^x, g_2 = g^y$  și  $g_3 = g^{xy}$  sau  $g_3 = g^z$  pentru  $x, y, z$  aleatoare, după care:
  1. Alege  $pk = (\mathbb{G}, q, g, g_1)$  și execută  $\mathcal{A}(pk)$  și obține două mesaje  $m_0$  și  $m_1$ ;
  2. Alege un bit aleator  $b$  și notează  $c_1 = g_2$  și  $c_2 = g_3 \cdot m_b$ ;
  3. Îi dă textul criptat  $(c_1, c_2)$  lui  $\mathcal{A}$  și obține de la el un bit  $b'$ . Dacă  $b' = b$ ,  $\mathcal{D}$  întoarce 1, altfel întoarce 0.

# Demonstrație

- ▶ Algoritmul  $\mathcal{D}$  primește la intrare tuplul  $(\mathbb{G}, q, g, g_1, g_2, g_3)$ , unde  $g_1 = g^x, g_2 = g^y$  și  $g_3 = g^{xy}$  sau  $g_3 = g^z$  pentru  $x, y, z$  aleatoare, după care:
  1. Alege  $pk = (\mathbb{G}, q, g, g_1)$  și execută  $\mathcal{A}(pk)$  și obține două mesaje  $m_0$  și  $m_1$ ;
  2. Alege un bit aleator  $b$  și notează  $c_1 = g_2$  și  $c_2 = g_3 \cdot m_b$ ;
  3. Îi dă textul criptat  $(c_1, c_2)$  lui  $\mathcal{A}$  și obține de la el un bit  $b'$ . Dacă  $b' = b$ ,  $\mathcal{D}$  întoarce 1, altfel întoarce 0.
- ▶ În continuare, analizăm comportamentul lui  $\mathcal{D}$  considerând două cazuri:

## Demonstrație

- **Cazul 1:** Să presupunem că tuplul pe care  $\mathcal{D}$  îl primește la intrare este generat alegând aleator  $x, y, z \leftarrow \mathbb{Z}_q$  și calculând  $g_1 = g^x, g_2 = g^y$  și  $g_3 = g^z$ .



# Demonstrație

- **Cazul 1:** Să presupunem că tuplul pe care  $\mathcal{D}$  îl primește la intrare este generat alegând aleator  $x, y, z \leftarrow \mathbb{Z}_q$  și calculând  $g_1 = g^x, g_2 = g^y$  și  $g_3 = g^z$ .
- Atunci  $\mathcal{D}$  execută  $\mathcal{A}$  cu cheia publică  $pk = (\mathbb{G}, q, g, g^x)$  și textul criptat construit  $(c_1, c_2) = (g^y, g^z \cdot m_b)$ ;

# Demonstrație

- ▶ **Cazul 1:** Să presupunem că tuplul pe care  $\mathcal{D}$  îl primește la intrare este generat alegând aleator  $x, y, z \leftarrow \mathbb{Z}_q$  și calculând  $g_1 = g^x, g_2 = g^y$  și  $g_3 = g^z$ .
- ▶ Atunci  $\mathcal{D}$  execută  $\mathcal{A}$  cu cheia publică  $pk = (\mathbb{G}, q, g, g^x)$  și textul criptat construit  $(c_1, c_2) = (g^y, g^z \cdot m_b)$ ;
- ▶ În acest caz,  $\mathcal{A}$  nu poate distinge între cele două situații: atunci când este executat ca o subrutină a lui  $\mathcal{D}$  interacționând cu el sau atunci când efectuează experimentul  $\text{PubK}_{\mathcal{A}, \tilde{\Pi}}^{\text{eav}}(n)$

# Demonstrație

- ▶ **Cazul 1:** Să presupunem că tuplul pe care  $\mathcal{D}$  îl primește la intrare este generat alegând aleator  $x, y, z \leftarrow \mathbb{Z}_q$  și calculând  $g_1 = g^x, g_2 = g^y$  și  $g_3 = g^z$ .
- ▶ Atunci  $\mathcal{D}$  execută  $\mathcal{A}$  cu cheia publică  $pk = (\mathbb{G}, q, g, g^x)$  și textul criptat construit  $(c_1, c_2) = (g^y, g^z \cdot m_b)$ ;
- ▶ În acest caz,  $\mathcal{A}$  nu poate distinge între cele două situații: atunci când este executat ca o subrutină a lui  $\mathcal{D}$  interacționând cu el sau atunci când efectuează experimentul  $PubK_{\mathcal{A}, \Pi}^{eav}(n)$
- ▶ Cum  $\mathcal{D}$  întoarce 1 exact atunci când output-ul  $b'$  al lui  $\mathcal{A}$  este egal cu  $b$ , rezultă că:

## Demonstrație

$$\Pr[D(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] = \Pr[\text{PubK}_{\mathcal{A}, \tilde{\Pi}}^{\text{eav}}(n) = 1] = \frac{1}{2}$$

# Demonstrație

$$\Pr[D(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] = \Pr[\text{PubK}_{\mathcal{A}, \tilde{\Pi}}^{\text{eav}}(n) = 1] = \frac{1}{2}$$

- **Cazul 2:** Să presupunem că tuplul pe care  $\mathcal{D}$  îl primește la intrare este generat alegând aleator  $x, y \leftarrow \mathbb{Z}_q$  și calculând  $g_1 = g^x, g_2 = g^y$  și  $g_3 = g^{xy}$ .

# Demonstrație

$$\Pr[D(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] = \Pr[\text{PubK}_{\mathcal{A}, \tilde{\Pi}}^{\text{eav}}(n) = 1] = \frac{1}{2}$$

- **Cazul 2:** Să presupunem că tuplul pe care  $\mathcal{D}$  îl primește la intrare este generat alegând aleator  $x, y \leftarrow \mathbb{Z}_q$  și calculând  $g_1 = g^x, g_2 = g^y$  și  $g_3 = g^{xy}$ .
- Atunci  $\mathcal{D}$  execută  $\mathcal{A}$  cu cheia publică  $pk = (\mathbb{G}, q, g, g^x)$  și textul criptat construit

$$(c_1, c_2) = (g^y, g^{xy} \cdot m_b) = (g^y, (g^x)^y \cdot m_b)$$

# Demonstrație

$$\Pr[D(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] = \Pr[\text{PubK}_{\mathcal{A}, \Pi}^{\text{eav}}(n) = 1] = \frac{1}{2}$$

- **Cazul 2:** Să presupunem că tuplul pe care  $\mathcal{D}$  îl primește la intrare este generat alegând aleator  $x, y \leftarrow \mathbb{Z}_q$  și calculând  $g_1 = g^x, g_2 = g^y$  și  $g_3 = g^{xy}$ .
- Atunci  $\mathcal{D}$  execută  $\mathcal{A}$  cu cheia publică  $pk = (\mathbb{G}, q, g, g^x)$  și textul criptat construit

$$(c_1, c_2) = (g^y, g^{xy} \cdot m_b) = (g^y, (g^x)^y \cdot m_b)$$

- În acest caz,  $\mathcal{A}$  nu poate distinge între următoarele două situații: atunci când este executat ca o subrutină a lui  $\mathcal{D}$  sau atunci când efectuează experimentul  $\text{PubK}_{\mathcal{A}, \Pi}^{\text{eav}}(n)$

## Demonstrație

- Cum  $\mathcal{D}$  întoarce 1 exact atunci când output-ul  $b'$  al lui  $\mathcal{A}$  este egal cu  $b$ , rezultă că:

$$Pr[D(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1] = Pr[PubK_{\mathcal{A}, \Pi}^{eav}(n) = 1] = \epsilon(n)$$



## Demonstrație

- ▶ Cum  $\mathcal{D}$  întoarce 1 exact atunci când output-ul  $b'$  al lui  $\mathcal{A}$  este egal cu  $b$ , rezultă că:

$$Pr[D(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1] = Pr[PubK_{\mathcal{A}, \Pi}^{eav}(n) = 1] = \epsilon(n)$$

- ▶ Dar cum problema DDH este dificilă, rezultă că există o funcție neglijabilă  $\text{negl}$  a.î.

$$\begin{aligned} \text{negl}(n) &\geq \\ |Pr[D(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] - Pr[D(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1]| \\ &= \left| \frac{1}{2} - \epsilon(n) \right| \end{aligned}$$

## Demonstrație

- ▶ Cum  $\mathcal{D}$  întoarce 1 exact atunci când output-ul  $b'$  al lui  $\mathcal{A}$  este egal cu  $b$ , rezultă că:

$$Pr[D(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1] = Pr[PubK_{\mathcal{A}, \Pi}^{eav}(n) = 1] = \epsilon(n)$$

- ▶ Dar cum problema DDH este dificilă, rezultă că există o funcție neglijabilă  $\text{negl}$  a.î.

$$\begin{aligned} \text{negl}(n) &\geq \\ |Pr[D(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] - Pr[D(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1]| \\ &= \left| \frac{1}{2} - \epsilon(n) \right| \end{aligned}$$

- ▶ Adică  $\epsilon(n) \leq \frac{1}{2} + \text{negl}(n)$

□.

# Important de reținut!

- ▶ Sistemul de criptare ElGamal
- ▶ Proprietatea de homomorfism