



Criptografie și Securitate

- Prelegerea 4 - Securitate perfectă

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

1. Definiție

2. One Time Pad

Securitate perfectă

- Primul curs: Sisteme de criptare istorice (substitutie, transpoziție, etc.) care pot fi sparte cu **efort computațional foarte mic**

Securitate perfectă

- ▶ Primul curs: Sisteme de criptare istorice (substitutie, transpoziție, etc.) care pot fi sparte cu **efort computațional foarte mic**
- ▶ Cursul de azi: Scheme perfect sigure care rezistă în fața unui adversar cu **putere computațională nelimitată**

Securitate perfectă

- ▶ Primul curs: Sisteme de criptare istorice (substitutie, transpoziție, etc.) care pot fi sparte cu **efort computațional foarte mic**
- ▶ Cursul de azi: Scheme perfect sigure care rezistă în fața unui adversar cu **putere computațională nelimitată**
- ▶ Însă...limitările sunt inevitabile

Securitate perfectă (Shannon 1949)

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 pentru care $\Pr[C = c] > 0$, următoarea egalitate este îndeplinită:

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

Securitate perfectă (Shannon 1949)

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 pentru care $\Pr[C = c] > 0$, următoarea egalitate este îndeplinită:

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

- ▶ $\Pr[M = m]$ - probabilitatea *a priori* ca Alice să aleagă mesajul m ;

Securitate perfectă (Shannon 1949)

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 pentru care $\Pr[C = c] > 0$, următoarea egalitate este îndeplinită:

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

- ▶ $\Pr[M = m]$ - probabilitatea *a priori* ca Alice să aleagă mesajul m ;
- ▶ $\Pr[M = m|C = c]$ - probabilitatea *a posteriori* ca Alice să aleagă mesajul m , chiar dacă textul criptat c a fost văzut;

Securitate perfectă (Shannon 1949)

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 pentru care $\Pr[C = c] > 0$, următoarea egalitate este îndeplinită:

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

- ▶ $\Pr[M = m]$ - probabilitatea *a priori* ca Alice să aleagă mesajul m ;
- ▶ $\Pr[M = m|C = c]$ - probabilitatea *a posteriori* ca Alice să aleagă mesajul m , chiar dacă textul criptat c a fost văzut;
- ▶ **securitate perfectă** - dacă Oscar afla textul criptat nu are nici un fel de informație în plus decât dacă nu l-ar fi aflat.

Securitate perfectă (Shannon 1949)

Definiție echivalentă

O schemă de criptare (Enc, Dec) este perfect sigură dacă pentru orice mesaje $m_0, m_1 \in \mathcal{M}$ cu $|m_0| = |m_1|$ și $\forall c \in \mathcal{C}$ următoarea egalitate este îndeplinită:

$$Pr[Enc_k(m_0) = c] = Pr[Enc_k(m_1) = c]$$

unde $k \in \mathcal{K}$ este o cheie aleasă uniform.

Securitate perfectă (Shannon 1949)

Definiție echivalentă

O schemă de criptare (Enc, Dec) este perfect sigură dacă pentru orice mesaje $m_0, m_1 \in \mathcal{M}$ cu $|m_0| = |m_1|$ și $\forall c \in \mathcal{C}$ următoarea egalitate este îndeplinită:

$$Pr[Enc_k(m_0) = c] = Pr[Enc_k(m_1) = c]$$

unde $k \in \mathcal{K}$ este o cheie aleasă uniform.

- fiind dat un text criptat, este imposibil de ghicit dacă textul clar este m_0 sau m_1

Securitate perfectă (Shannon 1949)

Definiție echivalentă

O schemă de criptare (Enc, Dec) este perfect sigură dacă pentru orice mesaje $m_0, m_1 \in \mathcal{M}$ cu $|m_0| = |m_1|$ și $\forall c \in \mathcal{C}$ următoarea egalitate este îndeplinită:

$$Pr[Enc_k(m_0) = c] = Pr[Enc_k(m_1) = c]$$

unde $k \in \mathcal{K}$ este o cheie aleasă uniform.

- ▶ fiind dat un text criptat, este imposibil de ghicit dacă textul clar este m_0 sau m_1
- ▶ cel mai puternic adversar nu poate deduce nimic despre textul clar dat fiind textul criptat

Un exemplu de cifru sigur - One Time Pad (OTP)

- ▶ Patentat in 1917 de Vernam (mai poartă denumirea de Cifrul Vernam)
- ▶ Algoritmul:
 1. Fie $l > 0$ iar $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^l$
 2. Cheia k se alege cu distribuție uniformă din spațiul cheilor \mathcal{K}
 3. **Enc:** dată o cheie $k \in \{0, 1\}^l$ și un mesaj $m \in \{0, 1\}^l$, întoarce $c = k \oplus m$.
 4. **Dec:** dată o cheie $k \in \{0, 1\}^l$ și un mesaj criptat $c \in \{0, 1\}^l$, întoarce $m = k \oplus c$.

Un exemplu de cifru sigur - One Time Pad (OTP)

mesaj:	0	1	1	0	0	1	1	1	1	\oplus
cheie:	1	0	1	1	0	0	1	1	0	
<hr/>										
text criptat:	1	1	0	1	0	1	0	0	1	

Un exemplu de cifru sigur - One Time Pad (OTP)

mesaj:	0	1	1	0	0	1	1	1	1	\oplus
cheie:	1	0	1	1	0	0	1	1	0	
<hr/>										
text criptat:	1	1	0	1	0	1	0	0	1	

- **avantaj** - criptare și decriptare rapide

Un exemplu de cifru sigur - One Time Pad (OTP)

mesaj:	0	1	1	0	0	1	1	1	1	\oplus
cheie:	1	0	1	1	0	0	1	1	0	
<hr/>										
text criptat:	1	1	0	1	0	1	0	0	1	

- ▶ **avantaj** - criptare și decriptare rapide
- ▶ **dezavantaj** - cheia foarte lungă (la fel de lungă precum textul clar)

Un exemplu de cifru sigur - One Time Pad (OTP)

mesaj:	0	1	1	0	0	1	1	1	1	\oplus
cheie:	1	0	1	1	0	0	1	1	0	
<hr/>										
text criptat:	1	1	0	1	0	1	0	0	1	

- ▶ **avantaj** - criptare și decriptare rapide
- ▶ **dezavantaj** - cheia foarte lungă (la fel de lungă precum textul clar)
- ▶ Este OTP sigur?

Teoremă

Schema de criptare OTP este perfect sigură.

- ▶ securitatea perfectă nu este imposibilă dar...

Teoremă

Schema de criptare OTP este perfect sigură.

- ▶ securitatea perfectă nu este imposibilă dar...
- ▶ cheia trebuie să fie la fel de lungă precum mesajul

Teoremă

Schema de criptare OTP este perfect sigură.

- ▶ securitatea perfectă nu este imposibilă dar...
- ▶ cheia trebuie să fie la fel de lungă precum mesajul
- ▶ inconveniente practice (stocare, transmitere)

Teoremă

Schema de criptare OTP este perfect sigură.

- ▶ securitatea perfectă nu este imposibilă dar...
- ▶ cheia trebuie să fie la fel de lungă precum mesajul
- ▶ inconveniente practice (stocare, transmitere)
- ▶ cheia trebuie să fie folosită o singură dată - **one time** pad - de ce?

Teoremă

Schema de criptare OTP este perfect sigură.

- ▶ securitatea perfectă nu este imposibilă dar...
- ▶ cheia trebuie să fie la fel de lungă precum mesajul
- ▶ inconveniente practice (stocare, transmitere)
- ▶ cheia trebuie să fie folosită o singură dată - **one time** pad - de ce?

Exercițiu Ce se întâmplă dacă folosim o aceeași cheie de două ori cu sistemul OTP ?

Limitările securității perfecte

Teoremă

Fie (Enc, Dec) o schemă de criptare perfect sigură peste un spațiu al mesajelor \mathcal{M} și un spațiu al cheilor \mathcal{K} . Atunci $|\mathcal{K}| \geq |\mathcal{M}|$.

Sau altfel spus:

Limitările securității perfecte

Teoremă

Fie (Enc, Dec) o schemă de criptare perfect sigură peste un spațiu al mesajelor \mathcal{M} și un spațiu al cheilor \mathcal{K} . Atunci $|\mathcal{K}| \geq |\mathcal{M}|$.

Sau altfel spus:

Teoremă

Nu există nici o schemă de criptare (Enc, Dec) perfect sigură în care mesajele au lungimea n biți iar cheile au lungimea (cel mult) $n - 1$ biți.

Important de reținut!

- ▶ Schema OTP are securitate perfectă, dar este nepractică pentru majoritatea aplicațiilor;
- ▶ Securitate perfectă \Rightarrow lungimea cheii \geq lungimea mesajului.