Perfect Security

Foundation of Cryptography

Pei-yih Ting
NTOUCS

Contents

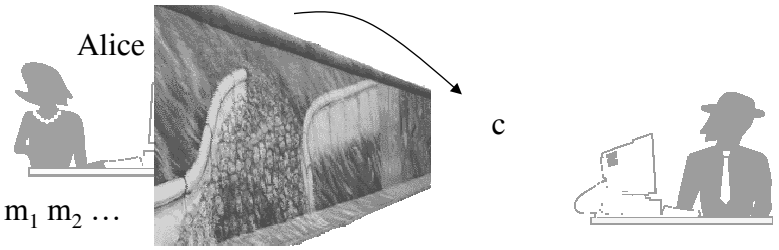
Perfect Secrecy

✧ $\forall\ m_1, m_2 \in \text{MsgSp}, c \in C$

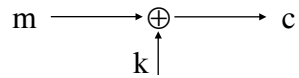
$$\Pr\{E_k(m_1) = c\} = \Pr\{E_k(m_2) = c\}$$

over k and coin tosses of E

✶ The adversary sees the same distribution of ciphertext, regardless of the message sent



One-time-pad is Perfectly Secure



For any message $m \in \text{MsgSp}$, if $k \in_R \{0,1\}^\ell$ uniformly and independently $\Rightarrow c = m \oplus k$ is uniformly distributed in $\{0,1\}^\ell$

$$\Pr\{\ m \oplus k = c\ \} = \sum_{\substack{m \in \text{MsgSp} \\ k \in \{0,1\}^\ell \\ m \oplus k = c}} \Pr\{m, k\} = \sum_{\substack{m \in \text{MsgSp} \\ k \in \{0,1\}^\ell \\ m \oplus k = c}} \Pr\{m\} \cdot \Pr\{k|m\}$$

m and k are independent

$$= \sum_{\substack{m \in \text{MsgSp} \\ k \in \{0,1\}^\ell \\ m \oplus k = c}} \Pr\{m\} \cdot \Pr\{k\}$$

for each m, c There is only one k satisfies $m \oplus k = c$

$$= \frac{1}{2^\ell} \sum_{\substack{m \in \text{MsgSp} \\ k \in \{0,1\}^\ell \\ m \oplus k = c}} \Pr\{m\} = \frac{1}{2^\ell} \sum_{m \in \text{MsgSp}} \Pr\{m\} = \frac{1}{2^\ell}$$

Shannon Secrecy

$\mathcal{M}$ is a distribution on MsgSp

An encryption scheme satisfies Shannon Secrecy with respect to $\mathcal{M}$ if $\forall\ m \in$ MsgSp, $\forall\ c \in C$

$$\Pr\{ M = m \mid E_k(M) = c \} = \Pr\{ M = m \}$$

over k, M and coin tosses of E

- Given a ciphertext c, the probability of the message distribution is the same as though the ciphertext is unknown
- Are there messages that do not give the same distribution of ciphertext $\Pr\{ E_k(m_1) = c \mid M = m_1 \} \neq \Pr\{ E_k(m_2) = c \mid M = m_2 \}$ yet $\Pr\{ M = m \mid E_k(m) = c \} = \Pr\{ M = m \}$??? No.

Perfect Secrecy Implies Shannon Secrecy

$$\Pr\{ M = m \mid E_k(M) = c \} =$$

$$\frac{\Pr\{ E_k(M) = c \mid M = m \} \cdot \Pr\{ M = m \}}{\Pr\{ E_k(M) = c \}} = \Pr\{ M = m \}$$

perfect secrecy $\Rightarrow \Pr\{ E_k(M) = c \mid M = m \} = \Pr\{ E_k(M) = c \}$

Shannon Secrecy Implies Perfect Secrecy

$$\Pr\{ E_k(M) = c \mid M = m \} =$$

$$\frac{\Pr\{ M = m \mid E_k(M) = c \} \cdot \Pr\{ E_k(M) = c \}}{\Pr\{ M = m \}} = \Pr\{ E_k(M) = c \}$$

Shannon secrecy $\Rightarrow \Pr\{ M = m \mid E_k(M) = c \} = \Pr\{ M = m \}$

$\Rightarrow$ Shannon Secrecy == Perfect Secrecy

Perfect Secrecy $\Rightarrow$ # Keys $\geq |\text{MsgSp}|$

- Deterministic encryption system

	m_1	m_2	…	$m_{\lvert MsgSp\rvert}$
k_1	$E_{k_1}(m_1)$	$E_{k_1}(m_2)$	…	
k_2	$E_{k_2}(m_1)$	…		
k_3	⋮			
⋮				

a. In one row, i.e. consider a fixed k_i, in order to decrypt,

$|\text{MsgSp}|$ = # of distinct ciphertexts for each key k_i

b. Perfect secrecy implies that every column has the same set of ciphertexts

every ciphertext in any row must be in some column, therefore, be in the same set of ciphertexts in each column

# of distinct ciphertexts for each key k_i $\leq$ # of distinct ciphertexts for each message m_j

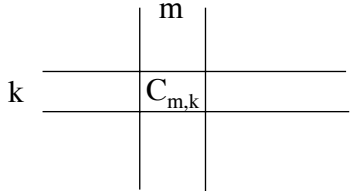
Keys ≥ |MsgSp| (2/4)

c. Consider a fixed message m_j in one column,

# of distinct ciphertexts for the message m_j	≤	# of keys

a, b, c ⇒ |MsgSp| ≤ # of keys

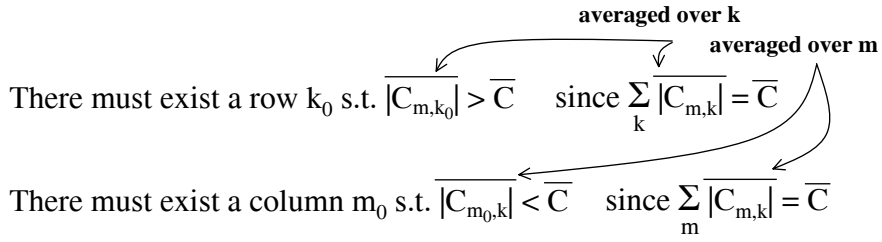
✧ Non-deterministic encryption system



$C_{m,k}$ is the set of ciphertexts $\{E_k(m)\}$ for different coin tosses of E

Keys ≥ |MsgSp| (3/4)

$\overline{C}$: the average count of members of $C_{m,k}$ (i.e. average $|C_{m,k}|$)



a. In one row, consider the key k_0 s.t. $\overline{|C_{m,k_0}|} > \overline{C}$, in order to decrypt,

$\overline{C}$ * |MsgSp| ≤ # of total distinct ciphertexts for k_0

since each entry C_{m,k_0} m=1,2,…,|MsgSp| has to be disjoint

Keys ≥ |MsgSp| (4/4)

b. Perfect secrecy implies that every column has the same set of ciphertexts

every ciphertext in $C_{m,k}$ is in the set of ciphertexts of the m-th column, therefore,

# of distinct ciphertexts for each key k_i	≤	# of distinct ciphertexts for each message m_j

c. Consider a message m_0 in one column such that $\overline{|C_{m_0,k}|} < \overline{C}$

# of distinct ciphertexts for each message m_0	≤	$\overline{C}$ * # of keys

a, b, c ⇒ |MsgSp| ≤ # of keys

Perfect Secrecy vs. Computational Secrecy

✧ One time pad is perfect, end of course!!!???

- ✡ key must change for every message block
- ✡ equally difficult to exchange key as to exchange message

✧ In a system that uses RSA algorithm as the basic block, if the key for RSA algorithm is "selected randomly for each message block", will the new encryption system be perfectly secure?

- ✡ Yes, key is uniformly random, RSA is permutation
- ✡ Why bother using RSA?
  - ➢ Use the same key for many messages

References

- C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal,* vol. 27, pp. 379-423 and 623-656, July and October, 1948
- C. E. Shannon, “Communication in the presence of noise,” Proc. IRE. 1949;37:10–21
- C. E. Shannon, “Communication theory of secrecy systems,” 1949