Perfect Security

Cryptography and Protocols
Andrei Bulatov

Symmetric Encryption Scheme

- A symmetric encryption scheme is a triple of algorithms (K,E,D)
  - K keys generation
  - E encryption algorithm
  - D decryption algorithm
- For simplicity assume that k ← K uniformly at random, $k \in \{0,1\}^l$

  or $k \in U_l$
- $P \in \{0,1\}^m$ plaintext

  $E : \{0,1\}^l \times \{0,1\}^m \rightarrow \{0,1\}^* \quad | \quad E_k(P) = C$

  $D : \{0,1\}^l \times \{0,1\}^* \rightarrow \{0,1\}^m \quad | \quad D_k(C) = P$

- In general, E (and possibly D) are randomized

Perfect Security

- Let (K,E,D) be a symmetric encryption scheme. It is said to be perfectly secure if for any two plaintexts P_1, P_2 and a ciphertext C

$$\Pr[E_k(P_1) = C] = \Pr[E_k(P_2) = C],$$

where the probability is over the random choice $k \leftarrow K$, and also over the coins flipped by E

Security as a Game

- We assume that Eve is almighty
- Game
  - Alice chooses a key k
  - Eve chooses 2 plaintexts and gives them to Alice
  - Alice encrypts one of them and sends to Eve
  - Eve decides which one is encrypted

  Eve wins if her decision is right
- The system is perfectly secure if Eve wins with probability 1/2
- This notion of security is very strong:

  Suppose that Eve can learn something about P. More precisely she can compute a function g(C) = f(P) $\in \{0,1\}$

  Then she chooses P_1, P_2 with $f(P_1) \neq f(P_2)$

Example

- Let (K,E,D) be a substitution cipher over the alphabet Σ consisting of 26 Latin letters. K picks a random permutation of Σ, that is $\pi \leftarrow \mathrm{Perm}(\Sigma)$.

  The set of possible plaintexts is the set of all 3-letters English words.
- This SES is not perfectly secure.
- There are P_1, P_2 such that for some C

$$\Pr[E_k(P_1) = C] \neq \Pr[E_k(P_2) = C],$$

- Take P_1 = \`FEE' and $P_1$ = \`FAR', and C = \`XYY'. Then

$$\Pr[E_k(P_1) = C] = [\text{prob. that } \mathrm{F} \to \mathrm{X}, \mathrm{E} \to \mathrm{Y}] = \frac{24!}{26!} = \frac{1}{25 \cdot 26}$$

$$\Pr[E_k(P_2) = C] = 0$$

One-Time Pad

- The one-time pad is the following cryptosystem (K,E,D):
  - k $\leftarrow$ K uniformly at random from $\{0,1\}^m$
  - the set of possible plaintexts is $\{0,1\}^m$
  - $E: \{0,1\}^m \times \{0,1\}^m \to \{0,1\}^m$

    $$P = P^1 \dots P^m, \qquad k = k^1 \dots k^m$$

    $$C = C^1 \dots C^m, \quad \text{where} \quad C^i = P^i \oplus k^i \pmod 2$$

  - $D: \{0,1\}^m \times \{0,1\}^m \to \{0,1\}^m$

    $$P^i = C^i \oplus k^i \pmod 2$$

Perfect Security of OTP

- **Theorem**.

  The OTP is perfectly secure

- **Proof**.

  For any $P_1, P_2, C \in \{0,1\}^m$ we have to prove that

$$\Pr[E_k(P_1) = C] = \Pr[E_k(P_2) = C],$$

Indeed,

$$\Pr[E_k(P_1) = C] = \Pr[k \oplus P_1 = C]$$

$$= \frac{|\{k \in \{0,1\}^m : k \oplus P_1 = C\}|}{|\{0,1\}^m|} = \frac{1}{2^m}$$

$$\Pr[E_k(P_2) = C] = \frac{1}{2^m}$$

Short Key – No Security

- **Theorem**

  There is no perfectly secure SES with m-bit messages and m – 1 –bit keys

- **Proof**

  Suppose (K,E,D) is such SES.

  Set $S_0 = \{E_k(0^m) \mid k \in \{0,1\}^{m-1}\}$

  Since $|\{0,1\}^{m-1}| = 2^{m-1}$ we have $|S_0| \le 2^{m-1}$

  Choose $C \notin S_0$ and P such that there is key k with $E_k(P) = C$

  Then

  $\Pr[E_k(0^m) = C] = 0$, while

  $\Pr[E_k(P) = C] > 0$