Perfect Secrecy

Wednesday, March 17, 2021 8:43 AM

Recall: Cryptography

- Symmetric
  - Stream cipher
    - shift
    - Substitution
    - Enigma
    - Vigenere
    - XOR (Vernam)
    - One-time pad
  - Block cipher
    - Ideal Block cipher
    - DES
    - AES
- Asymmetric "public-key"
  - RSA
  - ElGamal
  - Diffie-Hellman
  - ⋮

1) Entropy: (Information Theory) (Forouzan § F-2)

used to measure the amount of information (in bits) or the "uncertainty" in some finite sample space S.

$$E(S) = \sum_{x \in S} Prob(x) \cdot \log_2 \left(\frac{1}{Prob(x)} \right) \quad \text{bits}$$

e.g. flipping a fair coin, $c \in \{H, T\} = S$

$$E(S) = Prob(H) \cdot \log_2 \frac{1}{Prob(H)} + Prob(T) \cdot \frac{1}{Prob(T)}$$

$$= \frac{1}{2} \cdot \log_2 (2) + \frac{1}{2} \cdot \log_2 (2)$$

$$= \frac{1}{2} \cdot (1) + \frac{1}{2} (1)$$

$= 1$ bit

e.g. Rolling a die $S = \{1, 2, 3, 4, 5, 6\}$

$$E(S) = \sum_{1}^{6} \frac{1}{6} \cdot \log_2(6) = 6 \cdot \left[\frac{1}{6}(2.58)\right] = 2.58 \text{ bits}$$

e.g. Rolling unfair die, $S = \{2, 2, 2, 4, 5, 6\}$

$$E(S) = \frac{1}{2}\log_2(2) + \left[\frac{1}{6} \cdot \log_2(6)\right] \times 3$$
$$= \frac{1}{2} + \frac{3}{6} \cdot (2.58)$$

$$= 1.79 \text{ bits}$$

2] Shannon Perfect Secrecy. (§1.4.1 + §2.2 Bellare & Rogaway)

Def^n. The cipher is called perfectly secure (or Shannon secure) if given any two plaintext, M_1 and M_2, and a ciphertext C. Then C is just as likely to show up when M_1 is encrypted as when M_2 is encrypted.

i.e $\text{Prob}(E(M_1) = C) = \text{Prob}(E(M_2) = C)$

or $\text{Prob}(M_1) = \text{Prob}(M_1 \mid C)$

(1) e.g. Shift cipher with plaintext of one letter.

$p = B$, key $= 4$

$E(B, 4) = F \leftarrow$ ciphertexts

$E(Q, 4) = U \leftarrow$

② e.g. XOR-scheme : $M_1 = 111000$, $M_2 = 000111$

$C = 101010$

for $M_1 \Rightarrow K = 010010$

for $M_2 \Rightarrow K = 101101$

Can we use shorter key? e.g. $K = 010$ and repeat.

③ e.g. XOR : $|K| = 3$ $|M| = 6$, is it shannon secure?

No. for $M_1 = 100\ 000$ $M_2 = 100\ 100$

$M_2 = 100\ 100$ $K = x\ x$

$C = 001\ 101$ $C = y\ y$

C must be from M_1 with prob = 100%

∴ XOR-scheme is not shannon if $|K| < |P|$

3] One-time-pad : if $|K| = |P|$

XOR-scheme is shannon secure (perfect) as long as K is not repeated.