Cryptography And Network Security (Lec 13: Shannon's Theory of Perfect Ciphers)

Maniteja Tallapally

25-Sep-2020

1 Perfect Secrecy

A cryptosystem (P,C,K,E,D) has perfect secrecy if for a message x and encipherment y, $p(x|y) = p(x)$.
This implies that there must be for any message, cipher pair at least one key that connects them. Hence:

$$|K| >= |C| >= |P|$$

In the boundary case of equality we have the following theorem:

1.1 Theorem: Shannon Perfect Secrecy

Shannon's Theorem of Perfect Secrecy states that, a cryptosystem (P,C,K,E,D) with $|K| = |C| = |P|$. The cryptosystem has perfect secrecy if and only if

- each key is used with equal probability $1/|K|$.

- for every plaintext x and ciphertext y there is a unique key k such that $y = e_k(x)$.

1.1.1 Proof

Suppose perfect secrecy, i.e. $p(x|y) = p(x)$ for all x and y. Unless $p(x) = 0$, there must be enough keys so that any ciphertext can be decoded as a given plaintext, that is, $|K| >= |C|$, but by supposition, equality must hold. Hence there is a unique key for every x y pair.
Suppose keys $k_1, k_2, ...$ are the unique keys such that $d_{ki}(y) = x_i$. Using Bayes law:

$$p(x_i|y) = (p(y|x_i)p(x_i))/p(y)$$

Using the assumption of perfect secrecy, we have:

$$p(y|x_i) = p(y)$$

hence each k_i must occur with the same probability
We now assume that $p(k) = 1/|K|$ and that there is a unique key relating any plaintext-ciphertext pair.

$$p(x|y) = (p(y|x)p(x))/p(y)$$

By the uniqueness of keys, $p(y|x) = 1/|K|$. We also calculate

$$p(y) = sum_k p(k)p(d_k(y))$$

$$= (1/|K|)sum_k p(d_k(y))$$

$$= (1/|K|)sum_x p(x)$$

$$= 1/|K|$$

Cancelling the $1/|K|$ gives the result $p(x|y) = p(x)$, that is, perfect secrecy.