Scribe: Cryptography and Network Security

Ashish Kumar Singh(20CS60R48)

25-Sep-2020

1 Introduction

- Unbounded computational power of the attacker concerns the security of Cryptosystem.
- C.E Shannon define a secrecy system in "a mathematically acceptable system".
- He considered Cipher-Text only attack, ie., attacker knows only the cipher text.

++

2 *A Priori* and *A Posteriori* Probabilities

- Plain-Text (P) and Key(K) has a Probability Distribution , and both are having independent distribution.
- $p_P(X)$ and $p_K(K)$ are a priori probability distribution of plain-text and Key respectively.
- y=$e_K(X)$ is the Cipher text generated by applying encryption function.
- Probability Distribution on Cipher Text,C is induced by the distribution of P and K.
- Posteriori probability is the probability of plain-text after knowing the cipher.

$$p_P(x|y) = \frac{p_P(x)\sum_{K:x=d_K(y)} p_k K)}{\sum_{K:y\in C(K)} p_k(K) p_P(d_K(y))}$$

3 Theorem

Suppose (P,C,K,E,D) be a cryptosystem, where $|K| = |C| = |P|$. The cryptosystem,offers perfect secrecy if and only if every key is used with probability 1/—K—, and for every xP and every y C, there is a unique key, such that y=$e_K(X)$.

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 cipher text can be decoded as a given plain-text, that is, $|K| >= |C|$, but by supposition, equality must hold. Hence there is a unique key for every x y pair.

Let keys k1, k2, ... are the unique keys such that $d_{ki}(y) = x_i$. Using Bayes rule:

$$p(x_i|y) = \frac{(p(y|x_i)p(x_i))}{p(y)}$$

Using the assumption of perfect secrecy, we have: $p(y|x_i) = p(y)$ hence each ki 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.

$$p(x|y) = \frac{(p(y|x)p(x))}{p(y)}.$$

By the uniqueness of keys, $p(y|x) = \frac{1}{K}$.

We also calculate,

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

$$= \frac{1}{K} \sum_k p(d_k(y))$$

$$= \frac{1}{K} \sum_x p(x)$$

$$= \frac{1}{K}$$

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

4 Cryptographic Properties

- $p_C(y|x) > 0$, this means for every cipher text, there is a key.
- There is exactly one key , such that $y = E_k(X)$.
- There is no cipher text y, for which there are two or more keys.

5 Conclusion

- So, Shannon described that a Cryptosystem has Perfect Secrecy
if $p_c(x|y) = p_c(y)$ for all x P,y C., that is the a posteriori probability that the plain-text is x, given that the cipher-text y is known, is equal to the a priori probability that the plain text is x.
- Shift Cipher has perfect Secrecy.
  - 26 Keys in the Shift Cipher are used with equal probability $\frac{1}{26}$