Cryptography - Fri. 12. May. 2017

\[ X = \{ x_1, \ldots, x_n \} \quad P(X = x_i) = \Phi_i \]

\[ H(X) = \begin{cases} 
\frac{-\sum_{i=1}^{n} \Phi(x_i) \log \Phi(x_i)}{2} & \text{Single letter information} \\
\frac{-\sum_{i=1}^{n} \Phi(x_i) \log \Phi(x_i)}{n \log n} & \text{K bits} 
\end{cases} \]

\[ P(X = x_i) = 0 \implies P(X = x_i) \log P(X = x_i) = 0 \]

\[ H(X) = \sum_{x_i=1}^{n} \Phi(x_i) \log \Phi(x_i) \]

\[ H(X|Y) = \sum_{x_i,y} \Phi(x_i, y) \log \Phi(x_i|y) \]

\[ H(X|Y) \leq H(X) \]

\( H(X) \) is uncertainty we have about \( X \) in average
Shannon proved that $H(X)$ is a lower bound for the average codeword length of any uniquely decodable code.

$X = \{ X_1, \ldots, X_n \}$ \quad $P(X=x_i) = P_i$.

The worst case is when you have uniform distribution.

$$H(X) = \frac{1}{|X|} = \frac{1}{n} \Rightarrow H(X) = \log n$$

Hence $R = 1 - \frac{H(X)}{\log n}$ is called redundancy of a source.

4.2 Perfect secrecy

Consider the cryptosystem $(M, K, E, D, C)$

$M = \{ M_1, \ldots, M_m \}$ message space

$K = \{ K_1, \ldots, K_k \}$ key space

$C = \{ C_1, \ldots, C_n \}$ ciphertext space.

$E(M_k, K_j) = C_2$

Assume that $M$ and $K$ are independent RV with their support $M, K$.

$P(M = M_i) = P_i$ and $P(K = K_j) = q_j$. 
these prob. distributions model the occurrence of messages and keys.

Encryption: \( C = e(M, K) \):

\[
\mathbb{P}(C = c_0) = \sum \mathbb{P}(M_i, K_j) \\
\quad e(M_i, K_j) = c_0
\]

\[
= \sum \theta_i q_j \\
\quad e(M_i, K_j) = c_0
\]

\[
H(M) = -\sum_{i=1}^{m} \theta_i \log \theta_i \\
H(K) = -\sum_{j=1}^{n} q_j \log q_j
\]

\[
H(C) = -\sum_{c} \mathbb{P}(C = c_0) \log \mathbb{P}(C = c_0)
\]

\( H(K \oplus C) \) is called key equivocation.

\( H(M \oplus C) \) is called message equivocation.

Example Let \( M = K = C = \{0, 1\} \)

\( \hat{x} \sim \text{Bern}(p) \rightarrow \mathbb{P}(M = 1) = p \text{ and } \mathbb{P}(M = 0) = 1 - p \)

\( \hat{k} \sim \text{Bern}(q) \rightarrow \mathbb{P}(K = 1) = q \text{ and } \mathbb{P}(K = 0) = 1 - q \)

\( C = e(M, K) = (M + K) \mod 2 \)
\[ \vec{C} = (\hat{M} + \hat{K}) \mod 2 \]

1) Probability distributions

\[ \hat{M}, \hat{K} \]

\[ P(\hat{C} = 0), \quad P(\hat{C} = 1) \]

\[ P(\hat{C} = 0) = P(\hat{C} = 0, \hat{M} = 0) + P(\hat{C} = 0, \hat{M} = 1) \]
\[ = P(\hat{C} = 0 | \hat{M} = 0) P(\hat{M} = 0) \]
\[ + P(\hat{C} = 0 | \hat{M} = 1) P(\hat{M} = 1) \]

\[ P(\hat{C} = 0 | \hat{M} = 0) = P(B = 0) = 1 - \phi \]

\[ P(\hat{C} = 0 | \hat{M} = 1) = P(B = 1) = \phi \]

\[ P(\hat{C} = 0) = \phi - \theta + (1 - \phi)(1 - \phi) \]

\[ P(\hat{C} = 1) = (1 - \phi) \theta + \phi(1 - \phi) \]

\[ \phi \theta = 0 \]

\[ \phi \theta = \phi \theta \]

\[ P(\hat{C} = 0, \hat{M} = 0) = (1 - \phi) \cdot (1 - \theta) \]

\[ P(\hat{M} = 0) = 1 - \phi \]

\[ P(\hat{C} = 0) = \phi(1 - \theta) + (1 - \phi)(1 - \phi) \]
In general $M$ and $\hat{C}$ are not statistically independent. 

$P(\hat{C} = 0, \hat{M} = 0) \neq P(\hat{C} = 0)P(\hat{M} = 0)$

$q_h = \frac{1}{2} \Rightarrow P(\hat{C} = 0) \leq P(\hat{C} = 0) + (1-p)\frac{1}{2} = \frac{1}{2}

P(\hat{C} = 0, \hat{M} = 0) = \frac{1}{2} \times (1-p)

P(\hat{M} = 0) = 1 - p$

$\Rightarrow P(\hat{C} = 0, \hat{M} = 0) = P(\hat{C} = 0) \times P(\hat{M} = 0)

q_h = \frac{1}{2} \Rightarrow$ the key $K$ is uniformly distributed.

$H(M | \hat{C}) \leq H(M) \Rightarrow H(M | \hat{C}) = H(M)$

$\hat{M}$ and $\hat{C}$ are statistically independent.

* Definition 4.9) a cryptosystem $(M, E, C, D)$ is said to have perfect secrecy if $H(M | \hat{C}) = H(M)$

Interpretation: The knowledge of cryptogram $C$ does not decrease uncertainty about $M$ or does not increase information about $M$. 
Corollary 4.11. A cryptosystem has perfect secrecy.

\[ \iff \hat{M} \text{ and } \hat{C} \text{ are stochastically independent.} \]

\[ \iff \Pr(\hat{M} = M_i | \hat{C} = C_j) = \Pr(\hat{M} = M_i) \forall M_i, C_j \]

\[ \Pr(\hat{C} = C_j) > 0 \]

\[ \iff \Pr(\hat{C} = C_j | \hat{M} = M_i) = \Pr(C = C_j) \forall M_i, C_j \text{ with } \Pr(M = M_i) > 0 \]

The above conditions are all tedious to check, easy sufficient conditions are given in the following.

Theorem 4.14. A cryptosystem \((M, K, E, e, d)\) has perfect secrecy if:

(i) \(\Pr(\hat{K} = K) = \frac{1}{|K|}\) for all \(K \in K\)

(ii) for all \(M \in M\) and \(C \in C\), there is a unique \(K \in K\) at. \(e(M, K) = C\).

Proof:

\[ \Pr(\hat{C} = C | \hat{M} = M) = \frac{\Pr(e(\hat{M}, \hat{K}) = C, \hat{M} = M)}{\Pr(\hat{M} = M)} = \frac{\Pr(e(M, K) = C, M = M)}{\Pr(M = M)} \]
(iii) \( \exists K \)

\[ K = \hat{K}(M, C) \]

\[ \mathbb{P}(C(M, \hat{K}) = C) = \frac{\mathbb{P}(M = M)}{\mathbb{P}(M = M)} = \mathbb{P}(C(M, \hat{K}) = C) \]

\[ = \mathbb{P}(C(M, \hat{K}) = C) = \frac{1}{|K|} \]

\[ \mathbb{P}(C = C) = \sum \mathbb{P}(C = C | \hat{M} = M) \mathbb{P}(\hat{M} = M) = \frac{1}{|K|} \]

\[ \Rightarrow \mathbb{P}(\hat{C} = C | \hat{M} = M) = \frac{1}{|K|} \]

Hence perfect secrecy.

Vernam Ciphers

\( X = \{0, \ldots, m-1\} \)

\( M_N = E_N = K_N = X^N \)

\( e(M, K) = (a_1 + s_1) \mod m, \ldots, (a_N + s_N) \mod m \)

\( M = (a_1, \ldots, a_N) \)

\( \hat{M}_N \) i.i.d. \( \mathbb{P}(\hat{k}_i = i) = \frac{1}{m} \)

\( i = 1, \ldots, m \)
Theorem 4.15 The Vernam cipher has perfect secrecy.

Proof) Thm. 4.14)

i) \( P(\hat{K}_N = K) = P(\hat{K}_1 = S_1, \ldots, \hat{K}_N = S_N) \)

\[ \frac{1}{m} \times \ldots \times \frac{1}{m} = \frac{1}{m^N} \]

\[ \Rightarrow \frac{1}{|K_N|} \]

ii) \( M, C \rightarrow \text{unique } K \)

\( M \in \mathbb{Z}_{mN} \) and \( C \in \mathbb{Z}_N \)

\( C = (c_1, \ldots, c_N) \)

\( M = (a_1, \ldots, a_N) \)

\( c_i = (a_i + s_i) \mod m \)

\( s_i = (c_i - a_i) \mod m \)

Therefore

\( K = (c_1 - a_1) \mod m, \ldots, (c_N - a_N) \mod m \)

unique
5) Fast Block Ciphers.

5.1) The Data Encryption Standard (DES)

15 May 1973: The national Bureau of standards (NBS), national Institute of standards and Technology (NIST) solicited proposals for a cryptosystem.

An algorithm prepared by IBM was chosen.

Based on a predecessor LUCIFER

17 March 1975: DES was published, and publications started.

15 Jan 1979: DES was adopted for unclassified applications.

Reviewed every 5 years

Last official renewal 1999.

19.5.2005 NIST suspended DES as a standard.