T-79.5501 Cryptology

http://www.tcs.hut.fi/Studies/T-79.5501/

Spring 2007

Lecture 2

Topics covered:

- Stinson:Theorem 2.4
- Stinson: Sections 2.4 - 2.7

Entropy - Summary

- X random variable with n values $x_1, x_2, \ldots, x_n$ and probability distribution $p_1, p_2, \ldots, p_n$; Y random variable; then
  - entropy $H(X) = - \Sigma_{i=1}^{n} p_i \log_2 p_i$
  - conditional entropy $H(Y|X) = \Sigma_{i=1}^{n} p_i H(Y|x_i)$
  - the pair X,Y is a random variable, and $H(X,Y) = H(X) + H(Y|X) \leq H(X) + H(Y)$ with equality if and only if X and Y are independent.
- X random variable with two values 0,1; p= Pr[x=0]; then $H(X) = - p \log_2 p - (1-p) \log_2 (1-p)$

Entropy of a secrecy system

P, C, K random variables; P and K independent

Total entropy:

$H(P,K,C) = H(K,C) = H(P,K) = H(P) + H(K)$, where

$H(K,C) = H(K) + H(C|K) \leq H(K) + H(C)$

$\Rightarrow\ H(P) \leq\ H(C).$

Typically $H(P) <\ H(C)$. How much bigger is uncertainty about C than uncertainty about P? Theorem 2.10 states:

$H(C) - H(P) = H(K) – H(K|C).$

Theorem 2.4

Assumption: $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$

Claim: The following are equivalent:

(i) Cryptosystem achieves perfect secrecy.

(ii) Keys are chosen equiprobably:

$\Pr[K] = 1/|\mathcal{K}|$, for all $K \in \mathcal{K}$,

and for each pair (x, y), $x \in \mathcal{P}$, $y \in \mathcal{C}$, there is exactly one key $K \in \mathcal{K}$ such that $e_K(x) = y$.

Proof. (i) => (ii): See the text-book.

(ii) => (i): We express (i) and (ii) in terms of entropy. Then

(i) means that H(P|C) = H(P) (P and C independent)

(ii) means that H(K|PC) = 0 and H(K) ≥ H(C), as the sets $\mathcal{C}$ and $\mathcal{K}$ are of the same size, and K has maximum entropy.

Assume (ii) holds. Then H(PCK) = H(PC). On the other hand H(PCK) = H(PK) always. Hence H(PC) = H(PK), from where we get

(*) H(C) + H(P|C) = H(K) + H(P) as K and P are independent. It follows that H(K) ≤ H(C). On the other hand, we have by (ii) that H(K) ≥ H(C). It follows that H(K) = H(C). Then (i) follows from (*).

Shannon's pessimistic inequality

Theorem: If a secrecy system achieves perfect secrecy, then the entropy of the key must be at least as large as the entropy of the plaintext.

Proof. For any secrecy system, we have

$$H(C) + H(P|C) = H(PC) \leq H(PCK) = H(CK) \leq H(C) + H(K),$$

from where we get: $H(P|C) \leq H(K)$. If the system achieves perfect secrecy, then by definition, $H(P|C) = H(P)$, from where the claim follows.