CS553 Cryptography

BitBees

Question 8

Question 8

Suppose (P,C,K,E,D) is a cryptosystem with $\|P\| = \|C\| = \|K\|$, then the cryptosystem provides perfect secrecy if and only if every key is used with equal probability $1/\|K\|$, and $\forall \quad x \quad \epsilon \quad P \quad and \quad \forall \quad y \quad \epsilon \quad C$, there is a unique K such that $e_K(x) = y$.

We may recall that a cryptosystem is said to have perfect secrecy if $\mathbf{Pr}[x|y] = \mathbf{Pr}[x] \ \forall \quad x \quad \epsilon \quad P \quad and \quad \forall \quad y \quad \epsilon \quad C$

First proving the forward direction: If the system provides perfect secrecy, there is **at least** one key $\epsilon \ \ K$ such that $e_K(x) = y$. So we have,

$$\|C\| = \|\{e_k(x) : k \ \ \epsilon \ \ K\}\|$$

However, it is assumed that $\|C\| = \|K\|$, thus:

$$\|C\| = \|K\| = \|\{e_k(x) : k \ \ \epsilon \ \ K\}\|$$

This implies that two distinct keys **cannot** give the same ciphertext on a given plaintext. Therefore, for any $x \quad \epsilon \quad P \quad and \quad y \quad \epsilon \quad C$, there is **exactly one** key such that $e_k(x) = y$

Let us denote:
$\|K\| = n$
$P = \{x_i : 1 \leq i \leq n\}$
Using Bayes' theorem for the ciphertext element $y \ \ \epsilon \ \ C$ and $\forall \ \ 1 \leq i \leq n \ \ K_i$, we get:

$$\mathbf{Pr}[x_i|y] = \frac{\mathbf{Pr}[y|x_i]\mathbf{Pr}[x_i]}{\mathbf{Pr}[y]}$$

A key, k_i is fixed with probability $1/\|K\| = \mathbf{Pr}[K = k_i] = \mathbf{Pr}[y|x_i]$

$$\mathbf{Pr}[x_i|y] = \frac{\mathbf{Pr}[K = k_i]\mathbf{Pr}[x_i]}{\mathbf{Pr}[y]}$$

Since a cryptosystem is said to have perfect secrecy if $\mathbf{Pr}[x_i|y] = \mathbf{Pr}[x_i]$, we get:

$$\mathbf{Pr}[K_i] = \mathbf{Pr}[y]$$

Indicating that all keys $K_i \quad \forall \quad 1 \leq i \leq n$ are used with equal probability $(= 1/\|K\|)$.

Coming to the proof in reverse direction:
If every key is used with equal probability $1/\|K\|$, and $\forall \quad x \quad \epsilon \quad P \quad and \quad \forall \quad y \quad \epsilon \quad C$, there is a unique K such that $e_K(x) = y$.
Using Bayes' theorem for the ciphertext element we get:

$$\mathbf{Pr}[x_i|y] = \frac{\mathbf{Pr}[y|x_i]\mathbf{Pr}[x_i]}{\mathbf{Pr}[y]} \tag{1}$$

Since $\|P\| = \|K\|$ and the encryption function is defined such that for each unique key in K there is a unique mapping from any $x_i \ \epsilon \ P$ to a fixed $y \ \epsilon \ C$ with probability $1/\|K\|$. So the probability distribution of y given a plaintext x_i or in the absence of the plaintext is the same. Substituting the above in (1), we get the condition for perfect secrecy, as follows:

$$\mathbf{Pr}[x_i|y] = \mathbf{Pr}[x_i]$$