Perfect Secrecy

Math 4175

§3.3. Probability Distributions on Cryptosystems

In this section, we will define the perfect secrecy of a cryptosytem. Informally it means that one cannot obtain any information about the plaintext by simply obtaining the cyber text.

We can suppose that there is a probability distribution on the plaintext space $\mathcal{P}$. For example, the frequencies of English alphabets produce a probability distribution. But one may have any other distribution.

We will denoted $Pr[X = x]$ simply by $p[x]$ for each $x \in \mathcal{P}$ where X is the random variable on $\mathcal{P}$.

§3.3. Probability Distributions on Cryptosystems

We will also suppose that a key $k \in \mathcal{K}$ is selected (by Alice and Bob) by using a fixed (their favorite) probability distribution on $\mathcal{K}$. We will denote the probability that the key k is selected by $pr[K = k]$ or simply by $p[k]$.

Claim: Two selected probability distributions on $\mathcal{P}$ and $\mathcal{K}$ induce a probability distribution on $\mathcal{C}$.

For each $k \in \mathcal{K}$, define $C(k) = \{e_k(x) : x \in \mathcal{P}\} \subseteq \mathcal{C}$.

Now for every $y \in \mathcal{C}$, we have that

$$Pr[Y = y] = p[y] = \sum_{\{k:y \in C(k)\}} p[k]p[x = d_k(y)]$$

§3.3. Probability Distributions on Cryptosystems

Example*: For easy computation, let us take small size of $\mathcal{P}$, $\mathcal{K}$, and $\mathcal{C}$.

Let $\mathcal{P} = \{a, b\}$ with $p[a] = 1/4$ and $p[b] = 3/4$.

Let $\mathcal{K} = \{k_1, k_2, k_3\}$ with $p[k_1] = 1/2$, $p[k_2] = 1/4$, and $p[k_3] = 1/4$.

The encryption rules of this cryptosystem are given in the following table:

	a	b
k_1	1	2
k_2	2	3
k_3	3	4

That is, for example, $e_{k_1}(b) = 2$ and $e_{k_3}(a) = 3$.

§3.3. Probability Distributions on Cryptosystems

Now the induced probability distribution on $\mathcal{C}$ is given by:

$$p[1] = p[k_1]p[a] = (1/2)(1/4) = 1/8$$

$$p[2] = p[k_1]p[b] + p[k_2]p[a] = (1/2)(3/4) + (1/4)(1/4) = 7/16$$

$$p[3] = p[k_2]p[b] + p[k_3]p[a] = (1/4)(3/4) + (1/4)(1/4) = 1/4$$

$$p[4] = p[k_3]p[b] = (1/4)(3/4) = 3/16$$

§3.3. Probability Distributions on Cryptosystems

We can compute the conditional probability $p[y|x]$, that is, the probability of y is the cipher text given that x is the plaintext, as follows:

$$p[y|x] = \sum_{\{k:x=d_k(y)\}} p[k]$$

In our example,

$$p[1|a] = 1/2, \qquad p[1|b] = 0$$
$$p[2|a] = 1/4, \qquad p[2|b] = 1/2$$
$$p[3|a] = 1/4, \qquad p[3|b] = 1/4$$
$$p[4|a] = 0, \qquad p[4|b] = 1/4$$

§3.3. Probability Distributions on Cryptosystems

Recall Baye's Theorem:

$$p[x|y] = \frac{p[x]p[y|x]}{p[y]}$$

By applying Baye's theorem, we obtain:

$$\begin{aligned} p[a|1] &= 1, & p[b|1] &= 0 \\ p[a|2] &= 1/7, & p[b|2] &= 6/7 \\ p[a|3] &= 1/4, & p[b|3] &= 3/4 \\ p[a|4] &= 0, & p[b|4] &= 1 \end{aligned}$$

§3.3. Perfect Secrecy

Now we are in position to define the concept of perfect secrecy of a cryptosystem.

> A cryptosystem has perfect secrecy if $p[x|y] = p[x]$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.

In other words, a cryptosystem has perfect secrecy if X and Y are independent random variables, that is, the probability of plaintext x does not vary by knowing the cipher text y.

In our example, the perfect secrecy property is satisfied only for $y = 3$, but not for other three cipher texts.

So the system in our example does not have perfect secrecy.

§3.3. Perfect Secrecy

We noticed that the Shift Cipher can be decrypted easily if a single key is used to encrypt all plaintext characters, because there are only 26 possible keys.

Now we will show that the Shift Cipher has perfect secrecy or "unbreakable" if a new random key is used to encrypt every plaintext character.

Theorem: Suppose that the 26 keys in the Shift Cipher are used with equal probability 1/26. Then for any plaintext probability distribution, the Shift Cipher has perfect secrecy.

§3.3. Perfect Secrecy

Proof: Remember that $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$ in the Shift Cipher. Suppose that $\mathcal{K}$ has the equal probability, that is, $p[k] = 1/26$ for each key $k \in \mathcal{K}$.

First notice that for each $k \in \mathcal{K}$, we have $C(k) = \{e_k(x) : x \in \mathcal{P}\} = \mathbb{Z}_{26}$.

Now for every fixed $y \in \mathcal{C}$, we have that

$$\begin{aligned} p[y] &= \sum_{\{k:y\in C(k)\}} p[k]p[x = d_k(y)] \\ &= \sum_{k\in\mathbb{Z}_{26}} p[k]p[x = d_k(y)] \\ &= \frac{1}{26} \sum_{k\in\mathbb{Z}_{26}} p[x = y - k] \end{aligned}$$

§3.3. Perfect Secrecy

For any fixed $y \in \mathcal{C}$, the function $k \to (y - k) \mod 26$ yields a permutation of $\mathbb{Z}_{26}$.

So we have,

$$\sum_{k \in \mathbb{Z}_{26}} p[x = y - k] = \sum_{x \in \mathbb{Z}_{26}} p[x] = 1$$

Hence, for any fixed $y \in \mathcal{C}$, we have that $p[y] = 1/26$. That is, $\mathcal{C}$ also has equal probability.

Next notice that for any fixed $x \in \mathcal{P}$ and $y \in \mathcal{C}$, there exists unique key $k = (y - x) \mod 26$ such that $e_k(x) = y$.

So for any fixed $y \in \mathcal{C}$, we have $p[y|x] = p[k = (y - x) \mod 26] = 1/26$.

§3.3. Perfect Secrecy

Now, by using Baye's theorem, we get:

$$p[x|y] = \frac{p[x]p[y|x]}{p[y]} = \frac{p[x]\frac{1}{26}}{\frac{1}{26}} = p[x]$$

So we have perfect secrecy.

Indeed, there is a more general theorem by Shannon (1949):

Theorem: Suppose $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is a cryptosystem where $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$. Then the cryptosystem provides perfect secrecy if and only if every key is used with equal probability $1/|\mathcal{K}|$ and for every $x \in \mathcal{P}$ and every $y \in \mathcal{C}$, there is a unique key k such that $e_k(x) = y$.

§3.3. One-time Pad

A well-known application of previous theorem was actually developed more than 30 years earlier by Gilbert Vernam (1917) for use in automatic encryption and decryption of telegraph messages.

His method is called One-time Pad and we describe it by using binary system $\mathbb{Z}_2$.

One-time Pad is a cryptosystem where $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$ for a fixed integer $n \geq 1$. For each $k = (k_1, \cdots, k_n) \in \mathcal{K}$, the encryption and decryption rules are identical and given by

$$e_k(x) = (x_1 + k_1, \cdots, x_n + k_n) \mod 2$$

$$d_k(y) = (y_1 + k_1, \cdots, y_n + k_n) \mod 2$$

§3.3. One-time Pad

- Previous theorem proves that One-time Pad has perfect secrecy against cipher text only attack.
- However the unconditional security depends on the fact that each key is used for only one encryption. It is the reason for the name "One-time Pad".
- Hence, a new key needs to be generated and communicated over a secure channel for every new message, which creates severe key management problem for commercial use.
- This system is also vulnerable for known plaintext attack.
- However, One-time Pad has been employed in military and diplomatic contexts, where unconditional security is more important over key management and plaintexts can be kept secret.

§3.3. One-time Pad

- If the plaintext is a string of characters of length m in One-time Pad, then both the cipher text and the key are also strings of characters of length m. There are 2^m keys, each equally likely.
- As mentioned, the One-time Pad encryption method is completely unbreakable for a ciphertext only attack.
- For example, suppose the cipher text is FIOWPSLQNTISJQL, then the plaintext could be
  we will win the war
  or it could be
  the duck wants out.
  Each one is equally likely, along with any other messages of the same length. Therefore the cipher text gives no information about the plaintext (except for its at most length).