Lecture 8 - Cryptography and Information Theory

Jan Bouda

FI MU

April 22, 2010

Part I

Cryptosystem

Cryptosystem

- The traditional main goal of cryptography is to preserve secrecy of the message, i.e. to transform it in the way that no unauthorized person can read the message while it is easily readable by authorized persons.
- First applications of message secrecy are known from ancient times and served to keep secret military and diplomatic secrets, craftsmanship methods and also love letters.
- Craftsmanship secrets on earthen tablets in Ancient Summer.
- Secret love letters in Kamasutra.
- Spartian Scytale.
- Secrets hidden in a wax table or under hair of a slave.
- Caesar cipher.

Cryptosystem

Definition

A encryption system (cipher) is a five-tuple $(\mathbf{P}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$, where

1. $\mathbf{P}$ is a finite set of possible plaintexts
2. $\mathbf{C}$ is a finite set of possible ciphertexts
3. $\mathbf{K}$ is a finite set of possible keys
4. For each $k \in \mathbf{K}$ there is an encryption rule $e_k \in \mathbf{E}$ and a corresponding decryption rule $d_k \in \mathbf{D}$. Each $e_k : \mathbf{P} \to \mathbf{C}$ and $d_k : \mathbf{C} \to \mathbf{P}$ are functions such that $d_k(e_k(x)) = x$ for every $x \in \mathbf{P}$.

Shift Cryptosystem

Example

Example is e.g. the **shift cryptosystem**, sometimes known as the Caesar cipher. In this case $\mathbf{P} = \mathbf{C} = \mathbf{K} = \mathbb{Z}_{26}$. For $0 \leq k \leq 25$ we define

$$e_k(x) = (x + k) \bmod 26 \tag{1}$$

and

$$d_k(y) = (y - k) \bmod 26 \tag{2}$$

for $x, y \in \mathbb{Z}_{26}$.

Perfect Secrecy

To derive a definition of perfect secret we assume that there is some a priori distribution on plaintexts described by the random variable X with distribution $P(X = x)$. The key is chosen independently from the plaintext and described by the random variable K. Finally, ciphertext is described by the random variable Y that will be derived from X and K. Also, for $k \in \mathbf{K}$ we define $\mathbf{C}_k = \{e_k(x)|x \in \mathbf{X}\}$ as the set of all ciphertexts provided k is the key.

Now we can explicitly calculate the probability distribution of Y as

$$P(Y = y) = \sum_{k:y \in \mathbf{C}_k} P(K = k)P(X = d_k(y)). \tag{3}$$

Another quantity of interest is the probability of a particular ciphertext given a particular plaintex, easily derived as

$$P(Y = y|X = x) = \sum_{k:x=d_k(y)} P(K = k). \tag{4}$$

Perfect Secrecy

Definition

We say that the cryptosystem $(\mathbf{P}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ achieves **perfect (unconditional) secrecy** if and only if for every $x \in \mathbf{X}$ and $y \in \mathbf{Y}$ it holds that

$$P(X = x|Y = y) = P(X = x). \tag{5}$$

In words, the a posteriori probability distribution of plaintext given the knowledge of ciphertext is the same as the a priori probability distribution of the plaintext.

Following our previous analysis we calculate the conditional probability of a (possibly insecure) cryptosystem as

$$P(X = x|Y = y) = \frac{P(X = x)\sum_{k:x=d_k(y)} P(K = k)}{\sum_{k:y\in\mathbf{C}_k} P(K = k)P(X = d_k(y))}. \tag{6}$$

Perfect Secrecy

Theorem

Suppose the 26 keys in the Shift cipher are used with equal probability 1/26. Then for any plaintext distribution the Shift cipher achieves perfect secrecy.

Proof.

Recall that $\mathbf{P} = \mathbf{C} = \mathbf{K} = \mathbb{Z}_{26}$. First we compute the distribution of ciphertexts as

$$\begin{aligned} P(Y = y) &= \sum_{k \in \mathbb{Z}_{26}} P(K = k) P(X = d_k(y)) \\ &= \sum_{k \in \mathbb{Z}_{26}} \frac{1}{26} P(X = y - k) \\ &= \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = y - k). \end{aligned} \tag{7}$$

Perfect Secrecy

Proof.

For fixed y the values $(y - k) \bmod 26$ are a permutation of $\mathbb{Z}_{26}$ and we have that

$$\sum_{k \in \mathbb{Z}_{26}} P(X = y - k) = \sum_{x \in \mathbb{Z}_{26}} P(X = x) = 1. \tag{8}$$

Thus for any $y \in \mathbf{Y}$ we have

$$P(Y = y) = \frac{1}{26}.$$

Next, we have that

$$P(Y = y | X = x) = P(K \equiv (y - x) \pmod{26}) = \frac{1}{26}$$

for every x and y. □

Perfect Secrecy

Proof.

Using the Bayes' theorem we have

$$\begin{aligned} P(X = x|Y = y) =& \frac{P(X = x)P(Y = y|X = x)}{P(Y = y)} = \frac{P(X = x)\frac{1}{26}}{\frac{1}{26}} \\ =& p(X = x) \end{aligned} \tag{9}$$

what completes the proof. □

The previous result shows that the shift cipher is unbreakable provided we use an independent key for each plaintext character.

Perfect Secrecy

- If $P(X = x_0) = 0$ for some $x_0 \in \mathbf{P}$, then we trivially obtain $P(X = x_0|Y = y) = P(X = x_0)$. Therefore we consider only elements such that $P(X = x) > 0$.
- For such plaintexts we observe that $P(X = x|Y = y) = P(X = x)$ is equivalent to $P(Y = y|X = x) = P(Y = y)$.
- Let us suppose that $P(Y = y) > 0$ for all $y \in \mathbf{C}$. Otherwise y can be excluded from $\mathbf{C}$ since it is useless.
- Fix $x \in \mathbf{P}$. For each $y \in \mathbf{C}$ we have $P(Y = y|X = x) = P(Y = y) > 0$. Therefore for each $y \in \mathbf{C}$ there must be some key $k \in \mathbf{K}$ such that $y = e_k(x)$. It follows that $|\mathbf{K}| \geq |\mathbf{C}|$.
- The encryption is injective giving $|\mathbf{C}| \geq |\mathbf{P}|$.

Perfect Secrecy

Theorem (Shannon)

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

Proof.

Let us suppose the given cryptosystem achieves a perfect secrecy. As argued above for each x and y there must be at least one key such that $e_k(x) = y$. We have the inequalities

$$|\mathbf{C}| = |\{e_k(x) : k \in \mathbf{K}\}| \leq |\mathbf{K}|. \tag{10}$$

Perfect Secrecy

Proof.

We assume that $|\mathbf{C}| = |\mathbf{K}|$ and therefore

$$|\{e_k(x) : k \in \mathbf{K}\}| = |\mathbf{K}|$$

giving there do not exist two different keys $k_1, k_2 \in \mathbf{K}$ such that $e_{k_1}(x) = e_{k_2}(x) = y$. hence, for every x and y there is exactly one k such that $e_k(x) = y$.
Denote $n = |\mathbf{K}|$, let $\mathbf{P} = \{x_i | 1 \leq i \leq n\}$ and fix a ciphertext element y. We can name keys $k_1, k_2, \ldots, k_n$ in the way that $e_{k_i}(x_i) = y$. Using Bayes' theorem we have

$$\begin{aligned} P(X = x_i | Y = y) &= \frac{P(Y = y | X = x_i) P(X = x_i)}{P(Y = y)} \\ &= \frac{P(K = k_i) P(X = x_i)}{P(Y = y)}. \end{aligned} \tag{11}$$

Perfect Secrecy

Proof.

The perfect secrecy condition gives $P(X = x_i|Y = y) = P(X = x_i)$ and we have $P(K = k_i) = P(Y = y)$. This gives that all keys are used with the same probability. Since there are $|\mathbf{K}|$ keys, the probability is $1/|\mathbf{K}|$. Conversely, suppose the conditions are satisfied and we want to show perfect secrecy. The proof is analogous to the proof of perfect secrecy of the Shift cipher. □

Part II

Spurious Key and Unicity Distance

Spurious Key

Theorem

Let $(\mathbf{P}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ *be a cryptosystem. Then*

$$H(K|C) = H(K) + H(P) - H(C).$$

Proof.

First observe that $H(K, P, C) = H(C|K, P) + H(K, P)$. Now, the key and the plaintext determine the ciphertext uniquely, since $y = e_k(x)$. This implies $H(C|K, P) = 0$. Hence, $H(K, P, C) = H(K, P)$, but K and P are independent and we have

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

Spurious Key

Proof.

Analogously, since the key and ciphertext determine the plaintext uniquely, we have $H(P|C,K) = 0$ and hence $H(K,P,C) = H(K,C)$. We compute

$$\begin{aligned} H(K|C) &= H(K,C) - H(C) \\ &= H(K,P,C) - H(C) \\ &= H(K) + H(P) - H(C) \end{aligned} \tag{12}$$

what is the desired result. □

Spurious Key

Let us discuss now per symbol entropy of the plaintext.Let us consider that our plaintext is an English text. As a first approximation of the entropy per symbol we can take the entropy of the probability distribution of letters in English text. This gives us entropy estimate around 4.19 However, letters in an English text are not independent, their probability greatly varies depending on their predecessors. Therefore we should consider probability of all n-grams with $n \rightarrow \infty$ and divide it by n, much like in the case of the entropy rate. As an approximation we can take .e.g bigrams or trigrams.

Spurious Key

Definition

Let L be a natural language described by random variables $P_1, P_2, \ldots$. The **entropy** of the language is defined as

$$H_L = \lim_{n \to \infty} \frac{H(P_1, P_2, \ldots, P_n)}{n}$$

and the **redundancy** of the language is defined to be

$$R_L = 1 - \frac{H_L}{\log_2 |\mathbf{P}|},$$

where $\mathbf{P}$ here denotes $\Im(P_I)$.

Spurious Key

A random language would require entropy $\log_2 |\mathbf{P}|$ and the redundancy therefore measures the fraction of "excess" characters that we consider to be redundant. Various experiments for the English language gave
$1.0 \leq H_l \leq 1.5$
Let us denote

$$P^{(n)} = (P_1, P_2, \ldots, P_n),$$

i.s. the random variable describing possible n-grams of plaintext. Given probability distribution of $P^{(n)}$ and K we can compute the induced probability on $C^{(n)}$, what is the random variable describing all possible n-grams of ciphertext. For a given $y \in \Im(C^{(n)})$ we define

$$K_y = \{k \in \mathbf{K} | \exists x \in P^{(n)} \text{ such that } P(X = x) > 0 \text{ and } e_k(x) = y\},$$

i.e. K_y is the set of keys such that y is an encryption of a meaningful plaintext.

Spurious Key

If we observe the ciphertext y, we know that there is only one real key and K_y is the set of possible candidates to the key. The other keys are said to be **spurious**. Therefore for a particular y there are $|K_y| - 1$ spurious keys. The average number of spurious keys over all possible ciphertexts of length n is

$$\begin{aligned} s_n &= \sum_{y \in \mathbf{C}^n} P(C^{(n)} = y)(|K_y| - 1) \\ &= \sum_{y \in \mathbf{C}^n} P(C^{(n)} = y)|K_y| - \sum_{y \in \mathbf{C}^n} P(C^{(n)} = y) \\ &= \sum_{y \in \mathbf{C}^n} P(C^{(n)} = y)|K_y| - 1. \end{aligned} \tag{13}$$

Using the theorem from the beginning of the section we have

$$H(K|C^{(n)}) = H(K) + H(P^{(n)}) - H(C^{(n)}).$$

Spurious Key

We can estimate for sufficiently large n

$$H(P^{(n)}) \approx nH_L = n(1 - R_L) \log_2 |\mathbf{P}|.$$

Obviously,

$$H(C^{(n)}) \leq n \log_2 |\mathbf{C}|.$$

Then, if $|\mathbf{C}| = |\mathbf{P}|$, it follows that

$$H(K|C^{(n)}) \geq H(K) - nR_L \log_2 |\mathbf{P}|. \tag{14}$$

Spurious Key

Next, we want to relate $H(K|C^{(n)})$ to the number of spurious keys s_n. We compute

$$\begin{aligned} H(K|C^{(n)}) &= \sum_{y \in \mathbf{C}^n} P(C^{(n)} = y) H(K|C^{(n)} = y) \\ &\leq \sum_{y \in \mathbf{C}^n} P(C^{(n)} = y) \log_2 |K_y| \\ &\overset{\text{Jensen's inequality}}{\leq} \log_2 \sum_{y \in \mathbf{C}^n} P(C^{(n)} = y) |K_y| \\ &= \log_2(s_n + 1). \end{aligned} \tag{15}$$

Combining with (14) we obtain

$$H(K) - nR_L \log_2 |\mathbf{P}| \leq \log_2(s_n + 1). \tag{16}$$

Spurious Key

In the case when keys are chosen with uniform probability we obtain

Theorem

Suppose $(\mathbf{P}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ *is a cryptosystem where* $|\mathbf{C}| = |\mathbf{P}|$ *and keys are chosen equiprobably. Let* R_L *denotes the redundancy of the underlying language. Then, given a ciphertext string of sufficient length* n *the expected number of spurious keys satisfies*

$$s_n \geq \frac{|\mathbf{K}|}{|\mathbf{P}|^{nR_l}} - 1.$$

Note that the quantity s_n approaches 0 exponentially quickly as n increases. Also, the estimate may be not accurate for small values of n.

Unicity distance

Definition

The **unicity distance** of a cryptosystem is the value n_0 at which the expected number of spurious keys becomes 0.

If we set $s_n = 0$ and solve the equation we get the estimate

$$n_0 \approx \frac{\log_2 |\mathbf{K}|}{R_L \log_2 |\mathbf{P}|}. \tag{17}$$

In case of the substitution cipher $|\mathbf{P}| = 26$ and $|\mathbf{K}| = 26!$. If we take $R_L = 0.75$ we obtain $n_0 \approx 25$.