First Homework of *Introduction to Modern Cryptography*

Jie Feng [1]
Information Security Institute
Johns Hopkins University
jokerfeng2010@gmail.com

September 24, 2013

[1] This is the first time I hand in homework printed with LaTeX

Ex 1.5 Show that the shift, substitution, and Vigenère ciphers are all trivial to break using a known-plaintext attack. (Assuming normal English text is being encrypted in each case.) How much known plaintext is needed to completely recover the key for each of the ciphers (without resorting to any statistics)?

Known-plaintext means the adversary learns one or more pairs of plaintexts/ciphertexts encrypted under the same key.

For *shift cipher*. Say, if the key is k and is unknown. Now, if the adversary has got one pair which is alphabet A_1 mapped to A_2. We can represent alphabet A,..,Z as 0,...,25. So we get the number form of A_1 and A_2, which are N_1 and N_2. Then, by calculation, we get the key, which is $k = (N_2 - N_1 + 26) mod 26$. Here, only one alphabet pair is needed to completely recover the key for each of the ciphers.

For *substitution cipher*. In this situation, each plaintext character is mapped to a different ciphertext character in a arbitrary manner, subject only to the fact that the mapping must one-to-one in order to enable decryption. In this senario, the key k consists of 26 different smaller keys $k_1, k_2, ..., K_{26}$, which are used to encrypt and decrypt 26 different alphabets. Following the method we used in cracking *shift cipher*, it's easy to get 25 among the smaller keys. And then left the last pair of alphabets, and the last key is obvious to get. Hence, we need 25 known alphabet pairs to recover the key.

For *Vigenère cipher*. Let $k = K_1...K_t$ be the key. In order to recover the key, one need a pair of plaintext which is a alphabet string at length of t.

Ex 1.6 Show that the shift, substitution, and Vigenère ciphers are all trivial to break using a chosen-plaintext attack. How much plaintext must be encrypted in order for the adversary to completely recover the key? Compare to the previous question.

Chosen-ciphertext attack stands for that the adversary has the ability to obtain the encryption of any plaintext(s) of its choice.

For *shift cipher*. For any alphabet A_1, we get the enryption of it, which is A_2. Thus, we get one pair of alphabets. Following the conclusion we get of *Ex 1.5*, the adversary can completely recover the key.

For *substitution cipher*. Following the same reasoning, it's obvious that *substituion cipher* is trivial to break and we need to encrypt 26 alphabets to completely recover the key for each of the ciphers.

For *Vigenère cipher*. Le $K = K_1...K_t$ be the key. One need to encrypt a plaintext which is a alphabet string at length of t to recover the key.

Ex 2.2 Prove or refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$:

$$Pr[\mathcal{M} = m | \mathcal{C} = c] = Pr[\mathcal{M} = m' | \mathcal{C} = c].$$

Refute.
Since this encryption scheme is perfectly secret, we have:

$$Pr[\mathcal{M} = m | \mathcal{C} = c] = Pr[\mathcal{M} = m]$$

and

$$Pr[\mathcal{M} = m' | \mathcal{C} = c] = Pr[\mathcal{M} = m']$$

Since the probability distribution over $\mathcal{M}$ may not be uniform distribution, thus $Pr[\mathcal{M} = m]$ may not equal to $Pr[\mathcal{M} = m']$. Hence the conlusion is not true.

Ex 2.3 It's not an improvement. It's not perfectly secret. If it's perfectly secret, then $\forall m \in \mathcal{M}\ and\ \forall c \in \mathcal{C}\ for\ which\ Pr[\mathcal{C} = c] > 0:$

$$Pr[\mathcal{M} = m|\mathcal{C} = c] = Pr[\mathcal{M} = m]$$

For the situation $m = c$, we have $Pr[\mathcal{M} = m|\mathcal{C} = c] = 0$, since $k \neq 0^l$, thus $Pr[\mathcal{M} = m] = 0$. Then $\forall m \in \mathcal{M}$, $Pr[\mathcal{M} = m] = 0$ We've got a contradiction. So it's not perfectly secret.
Since key k is chosen at random, the adversary can't juedge whether key k is 0^l or not by looking at the ciphertext.Perfectly secret does not matter whether plaintext and ciphertext will be the same.

Ex 2.5 **Refute**

Ex 2.8 If a scheme Π is not perfectly secret with respect to Definition 2.1, then there exists a probability distribution over $\mathcal{M}$ and a message $m \in \mathcal{M}$ and a ciphertext $c \in C$ for which $Pr[C = c] > 0$:

$$\mathrm{Pr[M = m|C = c] \neq Pr[M = m]}$$

Using Bayes' theorem, we get the equation:

$$\frac{\mathrm{Pr[C = c||M = m] \cdot Pr[M = m]}}{\mathrm{Pr[C = c]}} \neq \mathrm{Pr[M = m]}$$

Without loss of generality, we assume $\mathrm{P}r[M = m] > 0$, hence we get:

$$\mathrm{Pr[C = c||M = m] \neq Pr[C = c]} \tag{1}$$

We claim that there exists $m_0, m_1 \in \mathcal{M}\ and\ c \in C$, st.

$$\mathrm{Pr[C = c|M = m_1] \neq Pr[C = c|M = m_2]}$$

Otherwise, we have: $\forall m_0, m_1 \in \mathcal{M}, and \forall c \in C$

$$\mathrm{Pr[C = c|M = m_1] = Pr[C = c|M = m_2]} \tag{2}$$

Fix some distribution over $\mathcal{M}$, and arbitrary $m_0 \in \mathcal{M} and c \in C$ Define $\gamma = Pr[C = c||M = m_0]$. We get

$$\begin{align} Pr[C = c] &= \sum_{m \in \mathcal{M}} Pr[C = c|M = m] \cdot Pr[M = m] \tag{3} \\ &= Pr[C = c|M = m] \tag{4} \\ &= \gamma \cdot \sum_{m \in \mathcal{M}} Pr[M = m] \tag{5} \\ &= \gamma \tag{6} \\ &= Pr[C = c|M = m] \tag{7} \end{align}$$

, which contradicts to (1) . So, our claim is true. Use these $m_0 and m_1$, it is trivial to construct $\mathcal{A}$ for which $\mathrm{Pr[PrivK^{eav}_{\mathcal{A},\Pi}]} > \frac{1}{2}$ Hence, Definition 2.4 implies Definition 2.1.

Ex 2.9 Consider the distribution with the condition that $Pr[M = m \wedge M' = m']! = 0$ over $\mathcal{M}$ since we can choose any distribution. Take $m \neq m'$ but $c = c'$. Since decrypt the same ciphertext should get the same plaintext. Thus $Pr[M = m \wedge M' = m'|C = c \wedge C' = C'] = 0$, So we get $Pr[M = m \wedge M' = m'|C = c \wedge C' = C']! = Pr[M = m \wedge M' = m']$. Hence, no encryption scheme satisfies this definition.