Principles of information security - Assignment 1

Siddharth Bhat

January 31, 2019

1 Q1

Let the mono alphabetic substitution ciphers used be $f_0, f_1, \dots f_t : A \to A$ where A is the alphabet.

If t is known, then one simply needs to perform a frequency analysis attack on the subsequence of the messages

$$m_k \equiv \left[a_i \mid i\%t = k, i \in [0, len(a))\right]$$

.

To discover t, we can use Kasiski's attack.

Alternatively, to discover t, Let the probability of the occurence of plaintext $a \in A$ be $p(a)$. Consider the quantity $sig = \sum_{a \in A} p^2(a)$.

Now, let us try all possible potential key lengths $\tau \in \mathbb{N}$. For a given τ, we extract out the subsequences for each k

$$a(k, \tau) \equiv \left[a[i] \mid i\%\tau = k, i \in \mathbb{N}\right]$$

Now, for each subsequence, we compute the quantity $q(k, \tau)$, the probability distribution of the alphabet in $a(k, \tau)$. From this, we compute the value $sig(k, \tau) \equiv \sum_{a \in A} q(k, \tau)(a)^2$.

2 Q3

If plain text and cipher is known:

For Ceasar, $\mathrm{Enc}(x) = x + \delta$, so compute $\mathrm{Enc}(x) - x = \delta$. So, with 1 letter, we can break the cipher.

For Vigenere cipher, $a'[i] = a[i] + k[i\%|k|]$. So, $a'[i] - a[i] = k[i\%|k|]$. We need to read the first $|k|$ letters to break the encryption.

3 Q4

Exactly the same as Q3 (known plaintext attack). We will need to find the keys, and we are using number of queries = entropy of key, which is optimal.

4 Q5

If an encryption scheme is perfectly secret, then $\Pr[M = m \mid C = c] = \Pr[M = m]$.

$$\Pr[M = m \mid C = c] = \frac{\Pr[M = m, C = c]}{\Pr[C = c]} = \Pr[M = m]$$
$$\Pr[M = m] \Pr[C = c] = \Pr[M = m, C = c]$$

Hence, the probabilities are independent.

So, $\Pr[M = m \mid C = c] = \Pr[M = m]$, and $\Pr[M = m', C = c |=] \Pr[M = m']$. But the given statement would imply that $\Pr[M = m] = \Pr[M = m']$ which is untrue.

For example, consider $\mathcal{M} \equiv \{0, 1\}$, $\Pr[M = 0] = p, \Pr[M = 1] = (1 - p)$. Let the ciphertext be independent of the message. The encryption function is $(\mathrm{Enc}(m) \equiv 0 \text{ or } 1 \text{ with equal probability})$. In this case, it is clearly perfectly secure, since the adversary can learn nothing about the plaintext from the ciphertext. However, our definition would have us prove that the probability of the *plaintext* being 0 is the same as the probability of the *plaintext* being 1 which is clearly wrong.

5 Q6

Yes, it is still perfectly secret, for the adversary does not know that the message was sent with the key 0^l. For example, let us assume that the message m was the cleartext message that was sent. It is just as likely that the cleartext message was the complement of m, $\overline{m}$, and the ciphertext was 1^l.

6 Q7

False. Consider $\mathtt{Enc}_k(m) = m$. In this case, $\Pr[M = m \mid C = m] = 1$, while $\Pr[M = m] = 1/|M|, \Pr[C = m] = 1/|M|$. Hence, $\Pr[M = m \mid C = m] \neq \Pr[M = m]\Pr[C = m]$. They're not independent, and is therefore not perfectly secret.

7 Q8

Instantiate $m = m' = m_0$, $c = c_0, c' = c_1, c_0 \neq c_1$ for the given inequality. This yields

$$\Pr\left[M = m_0 \wedge M' = m_0 \mid C = c_0 \wedge c' = c_1\right] = \Pr\left[M = m_0 \wedge M' = m_0\right]$$

If $M = m_0$, then $c_0 = \mathtt{ENC}(m_0)$. Similarly, $c_1 = \mathtt{ENC}(m_0)$. But we assumed that $c_0 \neq c_1 \implies \mathtt{ENC}(m_0) \neq \mathtt{ENC}(m_0)$ which is clearly false. Hence, the LHS has probability 0.

On the other hand, the RHS has probability $1/|M|^2 \neq 0$. Hence, this inequality is possible to be satisfied by any encoding scheme.

8 Q9

9 Q10

We can use a regular encoding scheme, and then chop off a single bit at the end. Now, each value can collide with at most another value, and the probability of a collision is 2^{-l}, with key space $|K|/2$.

If this encryption is not secure, then we can use this to beat the original cryptosystem, by trying $\langle \mathtt{m0} \rangle$ and $\langle \mathtt{m1} \rangle$.