COMP5631: Cryptography and Security
2024 Spring – Written Assignment Number 2
Sample Solutions

Q1. Please read the transposition cipher documented in the Appendix of Lecture 2. You are given a piece of ciphertext with 1000 English letters whose original plaintext is a piece of English writing. You are told that the encryption was with either a transposition cipher or a simple substitution cipher. How do you detect the type of the cipher used for the encryption? Justify your answer please. $\boxed{\text{20 marks}}$

Solution: Count the frequencies of single English letters in the ciphertext and the frequencies of digraphs (also bigrams). Then compare them with the standard frequency distribution of single English letters in the English language. If they match, it must be a transposition cipher. If they differ by a large extent, it must be simple substitution cipher. If they differ by a small extent, we compare the set of the frequencies of digraphs in the ciphertext with that in the English language. If they differ, it is a transposition cipher. Otherwise it is a simple substitution cipher.

This method works as transposition ciphers do not change the frequencies of single English letters when it is used to encrypt the plaintext, while simple substitution ciphers usually do.

Q2. There are ten pieces of ciphertext in the following URL:
[Click here]
Each of them is obtained by encrypting an English article with a simple substitution cipher. According to the last digit in your student ID number, please choose the corresponding ciphertext and recover the original message.

You may write your own computer programs or use the following online software to compute the frequencies of single letters, digraphs and trigraphs in the ciphertext for you:

```
https://www.cryptoclub.org/#vCiphers
```

Please write down certain details of your decryption process. You need to write down your decrypted text (i.e., the readable text), but do not need to write down the one-to-one function used for encryption. $\boxed{\text{30 marks}}$

Solution: Omitted here.

Q3. Cryptography is a tricky business. The following problem illustrates how easy it is to turn a strong scheme into a weak one with minor modifications.

The system described below is a variant of DES, called DESA. Its secret key is a pair (k, k_1), where k has 56 bits and k_1 has 64 bits. So the key size of DESA is 120 bits. The encryption transformation is defined by

$$\mathrm{DESA}_{(k,k_1)}(x) = \mathrm{DES}_k(x) \oplus k_1.$$

Show that breaking DESA is roughly as difficult as a brute force attack against single DES. Assume that you have a few pairs of plaintext/ciphertext. $\boxed{\text{15 marks}}$

Solution: Suppose we have two plaintext/ciphertext pairs (x_1, y_1) and (x_2, y_2), then

$$\begin{aligned} \mathrm{DES}_k(x_1) \oplus k_1 &= y_1, \qquad (1) \\ \mathrm{DES}_k(x_2) \oplus k_1 &= y_2 \qquad (2) \end{aligned}$$

(1)$\oplus$(2), we get

$$\mathrm{DES}_k(x_1) \oplus \mathrm{DES}_k(x_2) = y_1 \oplus y_2$$

A brute force attack will reveal k, then substituting k into (1), we will get k_1.

Q4. In real-world security systems, a one-key block cipher is not used in the ECB mode, but in the CBC or the Counter mode for encrypting data. Please explain briefly why this is the practice. $\boxed{\text{20 marks}}$

Solution: When the ECB mode is used for encrypting a message m_1m_1 of two message blocks, the corresponding two blocks in the ciphertext are always the same, as the ciphertext blocks depend only on the message blocks and the secret key.

When any of the CBC and Counter modes is used for encrypting a message m_1m_1 of two message blocks, the corresponding two blocks in the ciphertext are in general different, as the ciphertext blocks depend on the message blocks, the secret key and a time-variable parameter u stored in a memory device.

Hence, the obtained stream cipher can destroy statistical properties of a message to a much more extent then the original block cipher. This is why one-key block ciphers are usually used in one of the two modes for encrypting data.

Q5. Show that the Diffie-Hellman Key Exchange (Agreement) Protocol is insecure with respect to active attacks. $\boxed{\text{15 marks}}$

Solution: This protocol is not secure with respect to active attacks because it does not provide mutual authentication for the two parties involved.

The attacker is standing in the middle of the communication, and can use the protocol to establish a secret key k_1 with Alice by impersonating Bob, and another secret key k_2 with Bob. by impersonating Alice Then any encrypted message with key k_1 from Alice in transmission will be decrypted by the attacker first, and then be encrypted again with key k_2 and finally sent to Bob. The attacker will do the same for any ciphertext from Bob to Alice.