FIT2093: Sample Tutorial 4 Solutions

Fundamental Concepts of Symmetric Key Cryptography

Review

1. What are the essential ingredients of a symmetric cipher?

   Answer: Plaintext, encryption algorithm, secret key, ciphertext, decryption algorithm.

2. What are the two principal requirements for the secure use of symmetric encryption?

Answer (1) a strong encryption algorithm;
(2) Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

3. What are the two basic functions used in symmetric encryption algorithms?

   Answer: Permutation and substitution.

4. How many keys are required for two people to communicate via a symmetric cipher? How many keys are required for n people to communicate with each other securely?

   Answer: One secret key. n(n-1)/2 keys

5. What are the two general approaches to attacking a cipher?

   Answer: Cryptanalysis and brute force.

6. Define and distinguish between diffusion and confusion (with respect to encryption).

   Answer: In **diffusion**, the statistical structure of the plaintext is dissipated into long range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits, which is equivalent to saying that each ciphertext digit is affected by many plaintext digits. **Confusion** seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key. Thus, even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was

used to produce that ciphertext is so complex as to make it difficult to deduce the key. This is achieved by the use of a complex substitution algorithm.

7. Why is it important to study the Fiestel cipher?

   Answer: Most symmetric block encryption algorithms in current use are based on the Feistel block cipher structure. Therefore, a study of the Feistel structure reveals the principles behind these more recent ciphers.

8. What is the difference between an unconditionally secure cipher and a computationally secure cipher?

   Answer: **An encryption scheme is unconditionally secure if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. An encryption scheme is said to be computationally secure if: (1) the cost of breaking the cipher exceeds the value of the encrypted information, and (2) the time required to break the cipher exceeds the useful lifetime of the information.**

9. Explain the avalanche effect.

   Answer: The avalanche effect is a property of any encryption algorithm such that a small change in either the plaintext or the key produces a significant change in the ciphertext.

10. Why is the middle portion of 3DES a decryption rather than an encryption?

    Answer: There is no cryptographic significance to the use of decryption for the second stage. Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES by repeating the key.

Problems

1. Prove the following:

   a. $(A \oplus B) \oplus C = A \oplus (B \oplus C)$
   b. $A \oplus A = 0$
   c. $A \oplus 0 = A$
   d. $A \oplus 1$ = bitwise complement of A = A'
   e. $(A \oplus B)' = A' \oplus B = A \oplus B'$
   f. $A' \oplus B' = A \oplus B$

   where

   A, B, C are *n*-bit strings of bits
   0 is an *n*-bit string of zeros

1 is an *n*-bit string of one

Answer: Let us perform the operations on 1 bit numbers and it is true for n bit strings.

a. $(A \oplus B) \oplus C = A \oplus (B \oplus C)$

A	B	C	(A ⊕ B) ⊕ C	A ⊕ (B ⊕ C)
0	0	0	0	0
0	0	1	1	1
0	1	0	1	1
0	1	1	0	0
1	0	0	1	1
1	0	1	0	0
1	1	0	0	0
1	1	1	1	1

b. $A \oplus A = 0$

A	A	A ⊕ A = 0
0	0	0
1	1	0

c. $A \oplus 0 = A$

A		A ⊕ 0 = A
0	0	0
1	0	1

d. $A \oplus 1 = A'$

A		A ⊕ 1 = A'
0	1	1
1	1	0

e. The equality can be shown by listing all 1-bit possibilities:

A	B	A ⊕ B	(A ⊕ B)'	A' ⊕ B
0	0	0	1	1
0	1	1	0	0
1	0	1	0	0
1	1	0	1	1

f. We also need the equality $A \oplus B = A' \oplus B'$, which is easily seen to be true.

2. In the early 20th century Alice and Bob wanted to share a secret new recipe of making a new type of soft drink that can surpass the selling of Coke. They did not know how to encrypt the secret recipe into a ciphertext, they only knew that

somehow they needed to send the recipe inside a box secured by one or more padlocks. Assume that Alice and Bob lived in different towns in Australia and they could not meet in person and a postal service was available during that time.

a. Discuss the process that Alice can use to send the recipe to Bob based on the principle of symmetric key.

Answer: *Main principle, the same key has to be used to lock and open the box.*

Assume that the recipe is with Alice and she wants to send it to Bob.

1. *Alice needs to buy a box that can be locked using a single padlock and this padlock needs to have at least 2 exact copies of the keys.*
2. *Alice sends one of the copies to Bob using postal service but Alice has to make sure that the key is not sent together with the box.*
3. *Once Bob has acknowledged receiving the key, Alice can place the recipe in the box, lock it using the other key. Send the box using the postal service.*
4. *Bob can use the key that Alice sent earlier to open the box and read the recipe.*
5. *In the case Alice buys a combination key, she only needs to send the information on the combination to Bob.*

b. If the postal service was dishonest, is it possible for the postal service to get hold of the secret recipe. How would he/she steal it? (Assume that the padlock is very secure and could not be opened by physical force).

Answer: *If the postal service was dishonest, and intercept the envelope that contains the key and make a copy of the key, and send the original key to Bob so Bob won't be suspicious of not receiving the key at all. In the future when Alice sends the box, then the postal service can open the box and steal the recipe. It will be too late for Bob and Alice to realise that their communication has been compromised.*

3. Discuss how you would use the statistical information on the average occurrence of letters in text for a given language to perform crypto-analysis.

Answer: *Cryptanalysis has a role in checking weaknesses in new algorithms and giving the theory how to design crypto algorithm. Old crypto algorithms are made by substitution and transposition of letters. (modern ciphers work with bits). If there is enough cipher text, monoalphabetic cipher is easy to break since letters have different frequencies. If there is not enough text, like there is only one cipher message, we still can look for likely words or letter combinations. If anything is repeated, it is a common sequence. In English there is a common ending /ation, common word the and so on.*

Statistical analysis can be made stronger by having all frequencies of two, three and four letter combinations in a language. A machine can be used to find the best match.

4. Answer the following:
    a. Eve has tricked Alice into decrypting a bunch of ciphertexts that Alice encrypted last month but forgot about. What type of attack is Eve employing?

        This is a known-plaintext attack.

    b. Eve has an antenna that can pick up Alice's encrypted cell phone conversations. What type of attack is Eve employing?

        This is a ciphertext-only attack.

    c. Eve has bet Bob that she can figure out the AES secret key he shares with Alice if he will simply encrypt 20 messages for Eve using that key. For some unknown reason, Bob agrees. Eve gives him 20 messages, which he then encrypts and emails back to Eve. What kind of attack is Eve using here?

        This is a chosen-plaintext attack.

    d. What is the encryption of the following string using the Caesar cipher: THELAZYFOX.

        WKHODCBIRA.

    e. Bob is arguing that if you use XOR twice in a row to encrypt a long message, M, using the same key each time, it will be more secure. Explain why Bob is wrong in the case of using a binary one-time pad encryption scheme.

        Xor-ing the message M with the same pad twice will give the same message M back again.

    f. What is the plaintext for the following ciphertext, which was encrypted using a simple substitution cipher: CJBT COZ NPON ZJV FTTK TWRTUYTFGT NJ DTN O XJL. Y COZ ZJV CPJVIK DTN O XJL MYUCN.

        SOME SAY THAT YOU NEED EXPERIENCE TO GET A JOB. I SAY YOU SHOULD GET A JOB FIRST.

        Full Alphabet mapping: O = A, L = B, G = C, K = D, T = E, M = F, D = G, P = H, Y = I, X = J, E = K, I = L, B = M, F = N, J = O, R = P, H = Q, U = R, C = S, N = T, V = U, S = V, Q = W, W = X, Z = Y, A = Z.