FIT2093: Tutorial 4

Fundamental Concepts of Symmetric Key Cryptography

Review

1. What are the essential ingredients of a symmetric cipher?
2. What are the two principal requirements for the secure use of symmetric encryption?
3. What are the two basic functions used in symmetric encryption algorithms?
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?
5. What are the two general approaches to attacking a cipher?
6. Define and distinguish between diffusion and confusion (with respect to encryption).
7. Why is it important to study the Fiestel cipher?
8. What is the difference between an unconditionally secure cipher and a computationally secure cipher?
9. Explain the avalanche effect.
10. Why is the middle portion of 3DES a decryption rather than an encryption?

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

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.
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).

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.
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?
    b. Eve has an antenna that can pick up Alice's encrypted cell phone conversations. What type of attack is Eve employing?
    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?
    d. What is the encryption of the following string using the Caesar cipher: THELAZYFOX.
    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.
    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.