Written Assignment 1

CS 458/558: Introduction to Computer Security

Instructor:

Guanhua Yan

Problem 1

An affine cipher is a type of simple substitution where each letter is encrypted according to the following rule $c = (a\,p + b)$ mod 26. Here, p, c, a, and b are each numbers in the range of 0 to 25, where p represents the plaintext letter, c the ciphertext letter, and a and b are constants. For the plaintext and ciphertext, 0 corresponds to "a," 1 corresponds to "b," and so on. Consider the ciphertext **QJKES REOGH GXXRE OXEO**, which was generated using an affine cipher. Determine the constants a and b and decipher the message. **Hint**: Plaintext "t" encrypts to ciphertext "H" and plaintext "o" encrypts to ciphertext “E.”

Problem 2

Consider a Feistel cipher with four rounds. Then the plaintext is denoted as $P = (L_0, R_0)$ and the corresponding ciphertext is $C = (L_4, R_4)$. What is the ciphertext C, in terms of L_0, R_0, and the subkey, for each of the following round functions? (You should get the most concise solution.)

- A. $F(R_{i-1}, K_i) = 0$
- B. $F(R_{i-1}, K_i) = R_{i-1}$
- C. $F(R_{i-1}, K_i) = K_i$
- D. $F(R_{i-1}, K_i) = R_{i-1} \oplus K_i$

(Note that for each of cases A – D, the cipher uses four rounds.)

Problem 3

Suppose that we use a block cipher to encrypt according to the rule :

$C_0 = IV \oplus E(P_0, K)$,

$C_1 = C_0 \oplus E(P_1, K)$,

$C_2 = C_1 \oplus E(P_2, K)$,

...

- a. What is the corresponding decryption rule?
- b. Give two security disadvantages of this mode as compared to CBC mode.