Cryptography
ECE 5632
Sheet 2
Solutions

Spring 2024

Problem 1

(a) 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. That is, no matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there.
Computationally secure encryption ensures that breaking the cipher is practically infeasible within a reasonable timeframe and cost, given the available computational resources

(b) 1. Brute-force attack that involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.
2. Cryptanalysis attacks that rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

(c) One-time pad uses a random key that is as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new message. Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.
There are two main limitations:
1. There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
2. Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

(d) 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.
On the other hand, confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible. This is achieved by the use of a complex substitution algorithm.

(e) The avalanche effect means that a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext.

Problem 2

Consider the 5-bit permutation function $P = [2\ 1\ 5\ 3\ 4]$.

(a) $P^{-1} = [21453]$

(b) $[10001], [11001], [10010]$

(c) From (b) verify that P^{-1} in (a) is the inverse of P.

Problem 3

Given the function F shown in Figure . The expansion permutation E = [4 1 2 3 2 3 4 1], the permutation P = [2 1 4 3], and the S-boxes are given as:

$$S_0 = \begin{bmatrix} 1 & 0 & 2 & 3 \\ 3 & 1 & 0 & 2 \\ 2 & 0 & 3 & 1 \\ 1 & 3 & 2 & 0 \end{bmatrix} \quad S_1 = \begin{bmatrix} 0 & 3 & 1 & 2 \\ 3 & 2 & 0 & 1 \\ 1 & 0 & 3 & 2 \\ 2 & 1 & 3 & 0 \end{bmatrix}$$

If you know that the 4-bit input R = [0 1 1 0] and the 4-bit output C = [1 0 0 1]; perform simple cryptanalysis to find the possible keys K.

Problem 4

Solution

(a) $s(x1) \oplus s(x2) = 1110$
$s(x1 \oplus x2) = s(x2) = 0000 \neq 1110$

(b) $s(x1) \oplus s(x2) = 1001$
$s(x1 \oplus x2) = s(x2) = 1000 \neq 1001$

(c) $s(x1) \oplus s(x2) = 1010$
$s(x1 \oplus x2) = s(x2) = 1101 \neq 1010$

Problem 5

Worst-Case: 2^{56} keys.
Average: $2^{56}/2 = 2^{55}$ keys.

Problem 6

S1(0) = 14 = 1110
S2(0) = 15 = 1111
S3(0) = 10 = 1010
S4(0) = 7 = 0111
S5(0) = 2 = 0010
S6(0) = 12 = 1100
S7(0) = 4 = 0100
S8(0) = 13 = 1101

P(S) = D8D8 DBBC
(L1, R1) = 0000 0000 D8D8 DBBC