Solutions to Homework 2

October 17, 2016

1. Why is it important to study the Feistel cipher?

   Solutions: 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.

2. What is the difference between diffusion and confusion?

   Solutions: 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.

3. Which parameters and design choices determine the actual algorithm of a Feistel cipher?

   Solutions: Block size: Larger block sizes mean greater security (all other things being equal) but reduced encryption/decryption speed. Key size: Larger key size means greater security but may decrease encryption/decryption speed. Number of rounds: The essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. Subkey generation algorithm: Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis. Round function: Again, greater complexity generally means greater resistance to cryptanalysis. Fast software encryption/decryption: In many cases, encryption is embedded in applications or utility functions in such a way as to preclude a hardware implementation. Accordingly, the speed of execution of the algorithm becomes a concern. Ease of analysis: Although we would like to make our algorithm as difficult as possible to cryptanalyze, there is great benefit in making the algorithm easy to analyze. That is, if the algorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities and therefore develop a higher level of assurance as to its strength.

4. (10 points) What is the purpose of the S-boxes in DES?

Solutions: In general, an S-box takes some number of input bits, m, and transforms them into some number of output bits, n, where n is not necessarily equal to m. S-box from DES, mapping 6-bit input into a 4-bit output

5. This problem provides a numerical example of encryption using a one-round version of DES. We start with the same bit pattern for the key and the plaintext, namely:

   Hexadecimal notation: 0 1 2 3 4 5 6 7 8 9 A B C D E F

   Binary notation: 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

   (a) Derive K_1, the first-round subkey.

   Solutions: First, pass the 64-bit input through PC-1 (Slides Page 28) to produce a 56-bit result. Then perform a left circular shift separately on the two 28-bit halves. Finally, pass the 56-bit result through PC-2 (Slides Page 29, 30) to produce the 48-bit K1.:

   (b) Derive L_0 and R_0.

   Solutions:

   L0 = 0000 0001 0010 0011 0100 0101 0110 0111

   R0 = 1000 1001 1010 1011 1100 1101 1110 1111

6. (10 points) What is the effect of a single-bit (transmission) error in the ciphertext when using the ECB and CBC modes of operation? More precisely, answer the following question: The ciphertext is $c = \{c_0, c_1, \cdots, c_t\}$. Suppose c_q contains a transmission error for some $0 < q < t$. Which plaintext blocks will be recovered incorrectly?

   Solutions: ECB: p_q; CBC: $p_q \cdots, p_{q+1}$.