Gary Hobson

MAT260 Module 4

May 26, 2025

7.7- 2

$$L_0 = R_0 = M$$

Round 1:

$$L_1 = R_0 = M$$

$$R_1 = L_0 \oplus f(R_0, K) = M \oplus (M \oplus K) = K$$

Round 2:

$$L_2 = R_1 = K$$

$$R_2 = L_1 \oplus f(R_1, K) = M \oplus (K \oplus K) = M$$

So the final ciphertext is:

$$C = (L_2, R_2) = (K, M)$$

If Eve captures the ciphertext $C = (K, M)$, then:

- The right half of the ciphertext is the original message M.
- The left half of the ciphertext is the key K.

7.7- 4

If I understand the question correctly, Bob receives:
Ciphertext: C_0, C_1

encryption:

$$C_0 = R$$

$$C_1 = L \oplus f(R) \quad \Rightarrow \quad L = C_1 \oplus f(C_0)$$

Decryption steps are:

- Set $R = C_0$.
- solve $L = C_1 \oplus f(R)$ using the same function f.

This recovers the original L and R

This is my understanding.

From encryption:

$$C_0 = R$$

$$C_1 = L \oplus f(R)$$

From decryption:

$$L = C_1 \oplus f(C_0) = (L \oplus f(R)) \oplus f(R) = L \oplus (f(R) \oplus f(R)) = L \oplus 0 = L$$

and $R = C_0$ is already known.
So, both L and R are recovered correctly.

7.7- 6

Alice uses quadruple DES with keys K_1 = all 1s and K_2 = all 0s. Both are known weak keys in DES, meaning:

$$E_K(E_K(m)) = m$$

This holds for both K_1 and K_2, so Alice's encryption becomes:

$$c = E_{K_1}(E_{K_1}(E_{K_2}(E_{K_2}(m)))) = m$$

The result is that the ciphertext is identical to the plaintext. Eve does not need a meet in the middle attack because the encryption function is effectively the identity the cipher is completely broken with these weak keys.

7.7- 7

Initial Permutation (IP) and its inverse:
These are fixed, linear bit rearrangements complementing bits before or after does not change the property.

Expansion (E):
This is a rearrangement and duplication of bits complementing a bit before expansion simply results in the complement of the expanded version.

Key Mixing (XOR):
If $f(R, K) = S(E(R) \oplus K)$, then:

$$E(\overline{R}) \oplus \overline{K} = \overline{E(R)} \oplus \overline{K} = \overline{E(R) \oplus K}$$

So the input to the S boxes is complemented, but the S boxes are designed so that for every complemented input, the output is also complemented.

Overall Feistel Round:
Each round in DES is:

$$L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

If you flip all bits of L_0, R_0, and each round key, then at each round, the outputs are also flipped this propagates throughout.

Thus, if you encrypt a plaintext P under a key K to get ciphertext C, then:

$$E_K(P) = C \quad \Rightarrow \quad E_{\overline{K}}(\overline{P}) = \overline{C}$$