ECE Information and Network Security
Homework 2 solutions
Spring 2006

Chapter 4 problems

1. (a) Switch left and right halves and use the same procedure as encryption. The switch the left and right of the final output. Verification is the same as that on pages 115-116.

(b, c) 1st round: $M_0M_1 \to M_1[M_0 \oplus K \oplus M_1]$

2nd round: $[M_0 \oplus K \oplus M_1][M_1 \oplus M_0 \oplus K \oplus M_1 \oplus K] = [M_0 \oplus K \oplus M_1][M_0]$

3rd round: $[M_0][M_0 \oplus K \oplus M_1 \oplus K \oplus M_0] = [M_0][M_1]$, which is the plaintext.

Therefore 3 rounds is very insecure! After 2 rounds, the ciphertext alone lets you determine M_0 and therefore $M_1 \oplus K$, but not M_1 or K individually. If you also know the plaintext, you know M_1 are therefore can deduce K.

3. CBC: We have $D_K(C_j) \oplus C_{j-1} = D_K(E_K(P_j \oplus C_{j-1})) \oplus C_{j-1} = P_j \oplus C_{j-1} \oplus C_{j-1} = P_j$.

CFB: $C_j \oplus L_8(E_K(X_j)) = (P_j \oplus L_8(E_K(X_j))) \oplus L_8(E_K(X_j)) = P_j$.

4. Let I denote the string of all 1's. Note that the expansion $E(\overline{R_{i-1}}) = \overline{E(R_{i-1})} = E(R_{i-1}) \oplus I$. Therefore $E(\overline{R_{i-1}}) \oplus \overline{K_i} = E(R_{i-1}) \oplus I \oplus K_i \oplus I = E(R_{i-1}) \oplus K_i$, so the input to the S-boxes doesn't change. Therefore the output doesn't change. But $\overline{L_{i-1}} = L_{i-1} \oplus I$, so the resulting right side is $\overline{L_{i-1}} \oplus f(R_{i-1}, K_i) = R_i \oplus I = \overline{R_i}$. Also, clearly the new left side is the complementary string. So each round of DES gives the complementary string, so this is true for the final result.

7. (a) To perform the meet in the middle attack, you need a plaintext m and ciphertext c pair (its a known plaintext attack). So, make two lists. The left list consists of encryptions using the second encryption E^2 with different choices for K_2. Similarly, the right side contains decryptions using different keys for the first encryption algorithm. Thus, the lists look like:

$$\begin{array}{ll} E_1^2(m) = y_1 & z_1 = D_1^1(c) \\ E_2^2(m) = y_2 & z_2 = D_2^1(c) \\ \vdots & \vdots \\ E_{788}^2(m) = y_{788} & z_{788} = D_{788}^1(c) \\ \vdots & \vdots \end{array}$$

Note: The two lists need not be the same size, as the different algorithms might have different key lengths, and hence different amount of keys (see part b). Now, look for matches between y_j and z_l. A match using K_2' for E^2 and K_1' for D^1 indicates

$$E_{K_2'}^2(m) = y = D_{K_1'}^1(c)$$

and hence

$$E_{K_1'}^1\left(E_{K_2'}^2(m)\right) = c.$$

(b) Observe that there are 26 possibilities for β and 12 possibilities for α. Let $E_\alpha^2(x) = \alpha x \pmod{26}$ and let $E_\beta^1(x) = x + \beta \pmod{26}$. The composition of these two gives the affine cipher. The total computation needed involves producing 26 encryptions for E^2 and 12 decryptions for E^1. The total is 38.