Semester 1 **Exercises for Week 7** 2004

Modes of Operation (Reprise)

Block ciphers can be applied to longer ciphertexts using one of various *modes of operation*. We assume that the input is plaintext $M = M_1M_2\ldots$, the block enciphering map for given key K is E_K, and the output is $C = C_1C_2\ldots$. The following gives a summary of the major modes of operation.

Electronic Codebook Mode. For a fixed key K, the output ciphertext is given by $C_j = E_K(M_j)$ with output $C_1C_2\ldots$.

Ciphertext Block Chaining Mode. For input key K, and initialization vector C_0, the output ciphertext is given by $C_j = E_K(C_{j-1} \oplus M_j)$, with output $C_0C_1C_2\ldots$.

Ciphertext Feedback Mode. Given plaintext $M_1M_2\ldots$ in r-bit blocks, a key K, an n-bit cipher E_K, and an n-bit initialization vector $I = I_1$, the ciphertext is computed as:

$$\begin{aligned} C_j &= M_j \oplus L_r(E_K(I_j)) \\ I_{j+1} &= R_{n-r}(I_j) \,||\, C_j \end{aligned}$$

where R_{n-r} and L_r are the operators which take the right-most $n-r$ bits and the left-most r bits, respectively, and $||$ is concatenation.

Output Feedback Mode. Given plaintext $M_1M_2\ldots$ in r-bit blocks, a key K, an n-bit cipher E_K, and an n-bit initialization vector $I = I_0$, the ciphertext is computed as:

$$\begin{aligned} I_j &= E_K(I_{j-1}) \\ C_j &= M_j \oplus L_r(I_j), \end{aligned}$$

where L_r is the operator which takes the left-most r bits.

1. What mode of operation has been used in the assignment and in class up to this point, and why? What are the security disadvantages of this mode of operation?

2. Let E_K be the 4-bit cipher defined by:

$$E_K(M) = (K \oplus M)\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = (X_1 + X_3, X_2 + X_4, X_2 + X_3, X_1 + X_4)$$

where $X = K \oplus M = (X_1, X_2, X_3, X_4)$. Encipher the message M given by

$$1101011011100111001001000 1001000,$$

using the key $K = 1011$, in (i) ECB mode, in (ii) CBC mode with initialization vector 1001, and in (iii) CFB mode with initialization vector 1001 and $r = 1$.

3. How many steps are required for error recovery from a ciphertext transmission error in ECB and CBC modes?

4. If $n = 64$ and $r = 8$, how many steps in CFB mode does it take to recover from an error in a ciphertext block? What about in OFB mode?