Fall 2021 2021-10-06

Solutions for Assignment 2

Roopa Vishwanathan *CS 380/525: Intro to Crypto*

1. In CBC mode, if a single bit is flipped in ciphertext block C_i, then plaintext blocks M_i and M_{i+1} will be decrypted incorrectly. But rest of the blocks will be decrypted fine. Even if a bit is flipped in IV, which is usually transmitted unencrypted, only M_1 will be decrypted incorrectly, all other blocks will be decrypted correctly (see assign 1 solution 4, 5 for the equations, etc.).

   IN OFB and CTR modes, if a single bit is flipped in ciphertext block C_i, only plaintext block M_i will be decrypted wrongly (since errors are localized). But if a bit is flipped in the initial Nonce of OFB mode and the initial CTR value of CTR mode, all blocks in both modes will be wrongly decrypted.

   This resistance to initial IV corruption is actually one of the advantages of CBC over OFB and CTR.

2. OFB mode IND-CPA game:

   (a) Adversary picks (m_1^0, m_1^1), gives to challenger.

   (b) m_1^b is used by challenger as m_1 in encryption of $M = (m_1, m_2)$. The encryption takes place thus: $c_1 = E_K(\text{Nonce}) \oplus m_1$, and $c_2 = E_K(E_K(\text{Nonce})) \oplus m_2$.

   (c) Nonce, c_1, c_2 are given to adversary.

   (d) Adversary picks an $m_3 = (\text{Nonce} \oplus m_1^0 \oplus c_2)$.

   (e) m_3 is used as first block of $M' = (m_3, m_4)$. M' is encrypted thus: $c_3 = E_K(E_K(E_K(\text{Nonce})))\oplus m_3$, and $c_4 = E_K(E_K(E_K(E_K(\text{Nonce})))) \oplus m_4$.

   (f) Substituting for m_3 we get: $c_3 = E_K(E_K(E_K(\text{Nonce}))) \oplus \text{Nonce} \oplus m_1^0 \oplus c_2$. There's no way Nonce or c_2 will cancel out and render $E_K(m_3) = E_K(m_1)$ as was the case in CBC mode. Hence the game and adversary fail.

   CTR mode IND-CPA game:

   (a) Adversary picks (m_1^0, m_1^1), gives to challenger.

   (b) m_1^b is used by challenger as m_1 in encryption of $M = (m_1, m_2)$. The encryption takes place thus: $c_1 = E_K(\text{ctr+1}) \oplus m_1$, and $c_2 = E_K(\text{ctr+2}) \oplus m_2$.

   (c) ctr, c_1, c_2 is given to adversary.

   (d) Adversary picks an $m_3 = (\text{ctr+3} \oplus m_1^0 \oplus c_2)$.

   (e) m_3 is used as first block of $M' = (m_3, m_4)$. M' is encrypted thus: $c_3 = E_K(ctr + 3) \oplus m_3$, and $c_4 = E_K(ctr + 4) \oplus m_4$.

   (f) Substituting for m_3 we get: $c_3 = E_K(ctr + 3) \oplus \text{ctr+3} \oplus m_1^0 \oplus c_2$. There's no way ctr or c_2 will cancel out and render $E_K(m_3) = E_K(m_1)$ as was the case in CBC mode. Hence the game and adversary fail.

   In both games, m_3 could be constructed by adversary in Step (d) using other parameters too (e.g., put c_1 in it, or remove c_2 from it). The point is there is no way adversary can include factors inside m_3 that will cancel out in the encryption of m_3 – as long as she does not key K.

3. CBC mode $IV' = IV + 1$ game:

   (a) Adversary picks (m_1^0, m_1^1), gives to challenger.

(b) m_1^b is used by challenger as m_1 in encryption of $M = (m_1, m_2)$. The encryption takes place thus: $c_1 = E_K(IV \oplus m_1)$, and $c_2 = E_K(c_1 \oplus m_2)$.

(c) IV, c_1, c_2 is given to adversary.

(d) Adversary picks an $m_3 = IV + 1 \oplus m_1^0 \oplus IV$.

(e) m_3 is used as first block of $M' = (m_3, m_4)$. M' is encrypted thus: $c_3 = E_K(IV + 1 \oplus m_3)$, and $c_4 = E_K(c_3 \oplus m_4)$.

(f) Substituting for m_3 we get: $c_3 = E_K(IV + 1 \oplus IV + 1 \oplus m_1^0 \oplus IV)$, which is the same as the encryption of m_1^0. Hence $c_3 = c_1$ if $m_1 = m_1^0$.

(g) If $c_3 = c_1$, adversary outputs $m_1 = m_1^0$, else it outputs $m_1 = m_1^1$. Either way adversary wins.

4. The 2 formulas for the output of a single round of Feistel network encryption can be written as (see "des" slide 5):

$$L_{i+1} = R_i \tag{1}$$
$$R_{i+1} = f(K_{i+1}, R_i) \oplus L_i \tag{2}$$

(a) Try finding out $(L_1, R_1), (L_2, R_2) \ldots$. Using the formula for Feistel network encryption we get:

$$L_1 = R_0,\ R_1 = L_0 \oplus f_1(R_0) = L_0 \oplus 0 = L_0 \tag{3}$$
$$L_2 = R_1 = L_0,\ R_2 = L_1 = R_0 \tag{4}$$

So, we can say that if n is even, the output is (L_0, R_0), if n is odd, the output is (R_0, L_0).

(b) Ignore the round key in this. In general, if you are not told the round key, assume it is a string of 0s. Try finding out $(L_1, R_1), (L_2, R_2) \ldots$.

$$L_1 = R_0,\ R_1 = L_0 \oplus f(R_0) = L_0 \oplus R_0 \tag{5}$$
$$L_2 = R_1 = L_0 \oplus R_0,\ R_2 = L_1 \oplus R_1 = L_0 \tag{6}$$
$$L_3 = R_2 = L_0,\ R_3 = R_0 \tag{7}$$

The sequence repeats in rounds of 3. You can check this sequence for the $4^{th}, 5^{th}, 6^{th}$ rounds, etc. The 3 outputs that will repeat in rounds of 3, i.e., mod 3, are (L_0, R_0), $(R_0, L_0 \oplus R_0)$, and $(L_0 \oplus R_0, L_0)$.

5. Same as in previous question assume round key is a string of 0s, since it is not provided. Try finding out $(L_1, R_1), (L_2, R_2) \ldots$, since we are given it is a 2-round Feistel cipher. First compute $\mathsf{Feistel}_{f_1,f_2}(L_0, R_0)$. $L_1 = R_0$, $R_1 = L_0 \oplus f_1(R_0)$. $L_2 = R_1 = L_0 \oplus f_1(R_0)$, and $R_2 = L_1 \oplus f_2(R_1)$.

Next compute $\mathsf{Feistel}_{f_2,f_1}(R_2, L_2)$. Denote $\mathsf{Feistel}_{f_2,f_1}(R_2, L_2)$ as $\mathsf{Feistel}_{f_2,f_1}(L_0', R_0')$. Here $L_1' = R_0'$, $R_1' = L_0' \oplus f_2(R_0')$, $L_2' = L_0' \oplus f_2(R_0')$, and $R_2' = R_0' \oplus f_1(R_1')$.

Question says that for the first Feistel cipher, $R_0 = R_2$, so $R_2 \oplus f_2(R_1) = R_0$ (by transitivity of XOR), and we know that $L_2' = R_0$. Also substitute $R_0' = L_2$, and we get $R_2' = L_2 \oplus f_1(L_2') = L_2 \oplus f_1(R_0) = L_0$. So $R_2' = L_0$. Hence $\mathsf{Feistel}_{f_2,f_2}(R_2, L_2) = (R_0, L_0)$.