COMP90043: Cryptography and security
Week 4: Workshop Questions with solutions

Preparation:

(1) Please read the file OneTimePad.pdf uploaded to Week 3 document area.
(2) Please read the notes on modes of using block cipher.

Questions: Part A

(1) Consider an experiment of a random throw of a pair of dice as discussed in the lecture. The outcome of the experiment can be modeled as a random variable R defined on the set given by

$$R = \{1, 2, 3, 4, 5, 6\} \times \{1, 2, 3, 4, 5, 6\}.$$

Consider a uniform probability distribution for the outcome so that $Pr[(i, j)] = 1/36$, for all (i, j) belonging to the set.

(a) Now consider the events formed by the sum of the two dice. Let S_j be the event when the sum of two dice is j. How many such events are possible in the experiment and determine the probability of each event.

$S_2 = \{(1, 1)\}$
$S_3 = \{(1, 2), (2, 1)\}$
$S_4 = \{(1, 3), (2, 2), (3, 1)\}$
$S_5 = \{(1, 4), (2, 3), (3, 2), (4, 1)\}$
$S_6 = \{(1, 5), (2, 4), (3, 3), (4, 2), (5, 1)\}$
$S_7 = \{(1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1)\}$
$S_8 = \{(2, 6), (3, 5), (4, 4), (5, 3), (6, 2)\}$
$S_9 = \{(3, 6), (4, 5), (5, 4), (6, 3)\}$
$S_{10} = \{(4, 6), (5, 5), (6, 4)\}$
$S_{11} = \{(5, 6), (6, 5)\}$
$S_{12} = \{(6, 6)\}$

$Pr[S_2] = 1/36$
$Pr[S_3] = 2/36$
$Pr[S_4] = 3/36$
$Pr[S_5] = 4/36$
$Pr[S_6] = 5/36$
$Pr[S_7] = 6/36$
$Pr[S_8] = 5/36$

$Pr[S_9] = 4/36$
$Pr[S_{10}] = 3/36$
$Pr[S_{11}] = 2/36$
$Pr[S_{12}] = 1/36$

(b) Now consider a new random variable, X, obtained by the sum of the two dice in the above experiment. Let Y be a random variable which takes a value of D if the two dice are same and N otherwise. Determine all the joint and conditional probabilities, $Pr[x, y], Pr[x \mid y]$ and $Pr[y|x]$, where $x \in \mathcal{X}$ (set consisting all possible sums) and $y \in \mathcal{Y} = \{D, N\}$.
$\mathcal{X} = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

$Pr[y = D] = 1/6; Pr[y = N] = 5/6$

$$Pr[x = 2, y = D] = Pr[x = 2|y = D]Pr[y = D] = 1/6 \times 1/6 = 1/36$$
$$= Pr[y = D|x = 2]Pr[x = 2] = 1 \times 1/36 = 1/36$$
$$Pr[x = 2, y = N] = 0$$
$$Pr[x = 3, y = D] = 0$$
$$Pr[x = 3, y = N] = Pr[x = 3|y = N]Pr[y = N] = 1/15 \times 5/6 = 1/18$$
$$= Pr[y = N|x = 3]Pr[x = 3] = 1 \times 1/18 = 1/18$$

etc.

(2) State the condition for perfect secrecy.
$\mathbf{Pr}[\mathbf{M} = \mathbf{x}|\mathbf{C} = \mathbf{y}] = \mathbf{Pr}[\mathbf{M} = \mathbf{x}]$

(3) Let C_1 and C_2 are two n bit ciphertexts obtained by encrypting using one-time pad key K on plaintexts M_1 and M_2 respectively. Show that $M_1 \oplus M_2 = C_1 \oplus C_2$. What is the consequence of Chosen Plaintext attack on the one-time pad encryption?

$$C_1 = M_1 \oplus K$$
$$C_2 = M_2 \oplus K$$
$$C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K)$$
$$= M_1 \oplus M_2 \oplus K \oplus K$$
$$= M_1 \oplus M_2$$

If a key is used more than once, it leaks the statistics of the plain text.

Questions: Part B: Block Cipher Modes

(1) If a bit error occurs in the transmission of a ciphertext character in OFB mode, how far does the error propagate? (Question 6.8)

(2) In discussing OFB, it was mentioned that if it was known that two different messages had an identical block of plaintext in the identical position, it is possible to recover the corresponding Oi block? (Question 6.9)

(3) Why do some block cipher modes of operations only use encryption while others use both encryption and decryption? (Question 6.5)

(4) Question 6.1 and 6.2 (see below)

- **6.8:** Only the plaintext unit corresponding to the ciphertext character is affected. In OFB method, the bit errors in transmission do not propagate. For example, if a bit error occurs in C_1, only the recovered value of P_1 is affected; subsequent plaintext units are not corrupted.

- **6.9:** Let message M1 have plaintext blocks $P1_j$ and ciphertext blocks $C1_j$. Similarly for message M2. If the same IV and key are used in Ofb mode for both messages, then both messages have the same output blocks O_j. Suppose an attacker can observe the ciphertext blocks for M1 and M2 and that the attacker knows the exact contects of $P1_q$. Then,

$$\begin{aligned} C1_q &= P1_q \oplus O_q && \text{by definition of OFB} \\ C1_q \oplus P1_q &= P1_q \oplus O_q \oplus P1_q && \text{add to both sides} \\ O_q \oplus P1_q \oplus P1_q &= C1_q \oplus P1_q && \text{rearrange} \\ O_q &= C1_q \oplus P1_q && \text{cancel terms} \end{aligned}$$

$$\begin{aligned} C2_q &= P2_q \oplus O_q && \text{by definition of OFB} \\ C2_q \oplus O_q &= P2_q \oplus O_q \oplus O_q && \text{add to both sides} \\ P2_q &= C2_q \oplus O_q && \text{add to both sides} \end{aligned}$$

- **6.5:** In some modes, the plaintext does not pass through the encryption function, but is XORed with the output of the encryption function. The math works out that for decryption in these cases, the encryption function must also be used.

- **6.1.a:** If the IVs are kept secret, the 3-loop case has more bits to be determined and is therefore more secure than 1-loop for brute force attacks.

- **6.1.b:** For software implementations, the performance is equivalent for most measurements. One-loop has two fewer XORs per block. Three-loop might benefit from the ability to do a large set of blocks with a single key before switching. The performance difference from choice of mode can be expected to be smaller than the differences induced by normal variation in programming style.

  For hardware implementations, three-loop is three times faster than one-loop, because of pipelining. That is: Let P_i be the stream of input plaintext blocks, X_i the output of the first DES, Y_i the output of the second DES and C_i the output of the final DES and therefore the whole system's ciphertext.

  In the 1-loop case, we have:

$$\begin{aligned} X_i &= DES(XOR(P_i, C_{i-1})) \\ Y_i &= DES(X_i) \\ C_i &= DES(Y_i) \end{aligned}$$

  where C_0 is the single IV.

  If P_1 is presented at $t = 0$ (where time is measured in units of DES operations), X_1 will be available at $t = 1$, Y_1 at $t = 2$ and C_1 at $t = 3$. At $t = 1$, the first DES is free to do more work, but that work will be: $X_2 = DES(XOR(P_2, C_1))$ but C_1 is not available until $t = 3$, therefore X_2 can not be available until $t = 4$, Y_2 at $t = 5$ and C_2 at $t = 6$.

  In the 3-loop case, we have:

$$\begin{aligned} X_i &= DES(XOR(P_i, X_{i-1})) \\ Y_i &= DES(XOR(X_i, Y_{i-1})) \\ C_i &= DES(XOR(Y_i, C_{i-1})) \end{aligned}$$

  where X_0, Y_0 and C_0 are three independent IVs.

  If P_1 is presented at $t = 0$, X_1 is available at $t = 1$. Both X_2 and Y_1 are available at $t = 4$. X_3, Y_2 and C_1 are available at $t = 3$. X_4, Y_3 and C_2 are available at $t = 4$. Therefore, a new ciphertext block is produced every 1 tick, as opposed to every 3 ticks in the single-loop case. This gives the three-loop construct a throughput three times greater than one-loop construct.

- **6.2:** Instead of $CBC[CBC(CBC(X))]$, use $ECB[CBC(CBC(X))]$. The final IV was not needed for security. The lack of feedback loop prevents the chosen-ciphertext differential cryptanalysis attack. The extra IVs still become part of a key to be determined during any known plaintext attack.

Part C: Homework

The following are a list of questions for students to attempt at home to get a better grasp of the concepts discussed during the workshop.

(1) What is reversible mapping? What is irreversible mapping? Think about why Fiestels algorithm works for any function F, even for the irreversible ones.
(2) What is the difference between a block cipher and a stream cipher?
(3) What is a product cipher?
(4) What is the difference between diffusion and confusion? How diffusion and confusion is achieved in Fiestels encryption algorithm?
(5) What parameters and design choices determine the actual algorithm of a Feistel Cipher?
(6) The following are a list of questions for students to attempt at home to get a better grasp of the concepts discussed during the workshop.
    (a) Complete any questions that were not completed during the workshop.
    (b) What is avalanche effect? Why it is desired in encryption algorithms?
    (c) Write the block diagram for DES decryption algorithm.