# Homework Assignment #2

**Fall 2020**

**Due:** Friday, October 18, *before* 11:59 PM

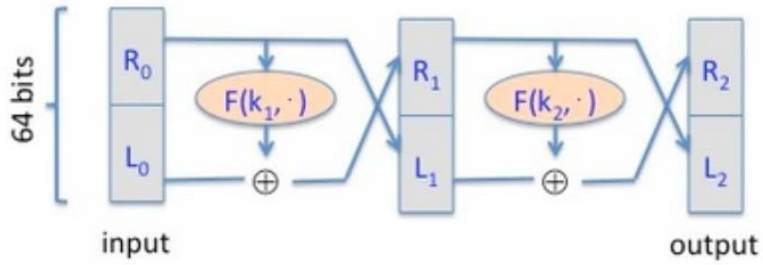
***Note!***
Please, submit your work via Canvas!
Submissions by e-mail will not be accepted!
Late submissions are not accepted!

**1)** Recall that the Luby-Rackoff theorem discussed in The Data Encryption Standard lecture states that applying a **three** round Feistel network to a secure PRF gives a secure block cipher. Let's see what goes wrong if we only use a **two** round Feistel.

Let F: $K \times \{0,1\}^{32} \rightarrow \{0,1\}^{32}$ be a secure PRF.

Recall that a 2-round Feistel defines the following PRP

$F2$: $K^2 \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$:




Here $R0$ is the right 32 bits of the 64-bit input and $L0$ is the left 32 bits.

One of the following lines is the output of this PRP $F2$ using a random key, while the other three are the output of a truly random permutation $f: \{0,1\}^{64} \rightarrow \{0,1\}^{64}$. All 64-bit outputs are encoded as 16 hex characters.

Can you say which is the output of the PRP? Note that since you are able to distinguish the output of $F2$ from random, $F2$ is not a secure block cipher, which is what we wanted to show. [5 points]

**Hint:** First argue that there is a detectable pattern in the xor of $F2(\cdot, 0^{64})$ and $F2(\cdot, 1^{32}0^{32})$. Then try to detect this pattern in the given outputs.

- On input $0^{64}$ the output is "e86d2de2 e1387ae9". On input $1^{32}0^{32}$ the output is "1792d45d b645c008".
- On input $0^{64}$ the output is " 5f67abaf 5210722b". On input $1^{32}0^{32}$ the output is "a09033c0 0bc9330e".
- On input $0^{64}$ the output is "7c2822eb fdc48bfb". On input $1^{32}0^{32}$ the output is "83d032a9 c5e2364b".
- On input $0^{64}$ the output is "7b50baab 07640c3d". On input $1^{32}0^{32}$ the output is "84af4554 cea46d60".

**2)** Nonce-based encryption has been implemented in HTTPS and IPSec design. Please explain how nonce has been implemented in these two protocols. [10 point]

**HTTPS:**

**IPSec:**

**3)** Let m be a message consisting of $\ell$ AES blocks (say $\ell$=100). Alice encrypts *m* using CBC mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number $\ell/2$ is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted? [5 points]

**4)** Let m be a message consisting of $\ell$ AES blocks (say $\ell$=100). Alice encrypts *m* using randomized counter mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number $\ell/2$ is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted? [5 points]

**5)** Nonce-based CBC. Recall that we said that if one wants to use CBC encryption with a non-random unique nonce then the nonce must first be encrypted with an **independent** PRP key and the result then used as the CBC IV.

Let's see what goes wrong if one encrypts the nonce with the **same** PRP key as the key used for CBC encryption.

Let $F:K\times\{0,1\}^{\ell}\rightarrow\{0,1\}^{\ell}$ be a secure PRP with, say, $\ell$=128. Let *n* be a nonce and suppose one encrypts a message m*m* by first computing $IV=F(k,n)$ and then using this IV in CBC encryption using $F(k,\cdot)$. Note that the same key *k* is used for computing the IV and for CBC encryption. We show that the resulting system is not nonce-based CPA secure.

The attacker begins by asking for the encryption of the two block message $m=(0^{\ell},0^{\ell})$with nonce $n=0^{\ell}$. It receives back a two block ciphertext ($c0$,$c1$). Observe that by definition of CBC we know that $c1=F(k,c0)$.

Next, the attacker asks for the encryption of the one block message $m1=c0 \oplus c1$ with nonce $n=c0$. It receives back a one block ciphertext $c0'$.

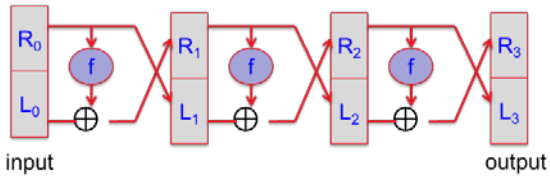
What relation holds between $c0, c1, c0'$? Note that this relation lets the adversary win the nonce-based CPA game with advantage 1. [5 points]

- $c_1=c_0 \oplus c_0'$
- $c_0'=c_0 \oplus 1^{\ell}$
- $c_0=c_1 \oplus c_0'$
- $c_1 = c_0'$

**6)** What is the corresponding ciphertext for the below message if the simplified version of DES is used for encryption. [10 points]

**Note:**

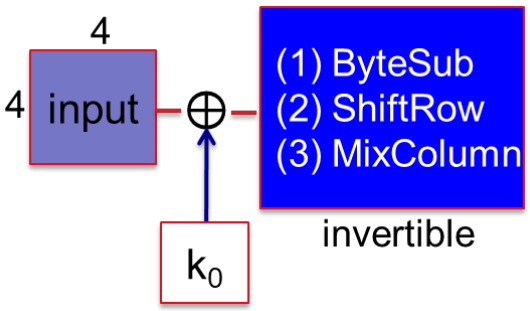
i. *The f(k,·) function shifts the content of each individual cell, 1 bit to the left (multiply the content of cell by 2),*
ii. *Suppose each item in the array cell is just one byte,*
iii. *The simplified DES has just three rounds of feistel network*




Message:

| 4 | 5 | 2 | 6 | 9 | 2 | 1 | 3 |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

**7)** What is the corresponding ciphertext for the below message if the simplified version of AES is used for encryption. [15 points]



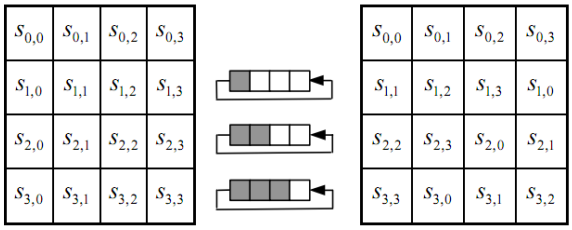

**Note:**

*i. The ByteSub replaces each element in the matrix with the elements given in the below s-box,*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

*ii. Suppose each item in the array cell is just one byte,*

*iii. The ShiftRow operation performs cyclic rotation per each row as determined be below figure,*




*iv. The MixColumn operation multiplies the third column of the generated matrix in step iii by 2.*

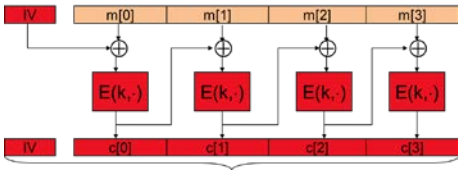
Message:

| | | | |
|---|---|---|---|
| 1A | 2B | 2C | 4C |
| A2 | A3 | 32 | 20 |
| A3 | 1B | B2 | 25 |
| 4A | 54 | 54 | BA |

Key:

| | | | |
|---|---|---|---|
| 1A | 2B | 1E | 7A |
| 82 | 2B | 32 | 04 |
| A5 | 4A | A4 | 25 |
| 13 | 23 | 25 | 26 |

**8)** What is the corresponding ciphertext for the below message if CBC with random IV is used for encryption. [15 points]




**Note:**

i. *Suppose that the underlying block cipher is 3DES,*
ii. *The E(k,·) function shifts the input, 1 bit to the left,*
iii. *IV is a true random number. No encryption on IV is required.*
iv. *Suppose each item in the array cell is just one byte,*
v. *Make sure that you append the padding block first to your message, then encrypt it.*

Message:

| 4 | 6 | 2 | 8 | 9 | 1 | 0 | 2 | 1 | 3 | 5 | 6 | 4 | 5 | 7 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

IV:

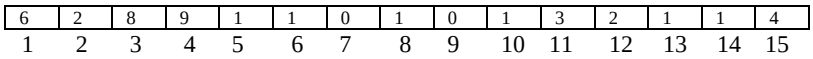
| 2 | 6 | 8 | 2 | 6 | 7 | 0 | 1 |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

**9)** What is the corresponding ciphertext for the below message if CBC with random IV is used for encryption. [10 points]

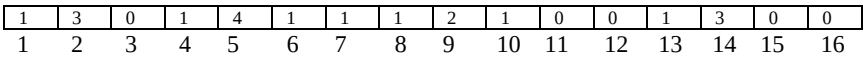
**Note:**

v. *Suppose that the underlying block cipher is AES,*
*vi.* *The E(k,·) function shifts the input, 1 bit to the left,*
*vii.* *Suppose each item in the array cell is just one byte,*
*viii.* *Make sure that you append the padding block first to your message, then encrypt it.*

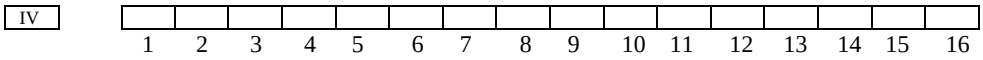
Message:



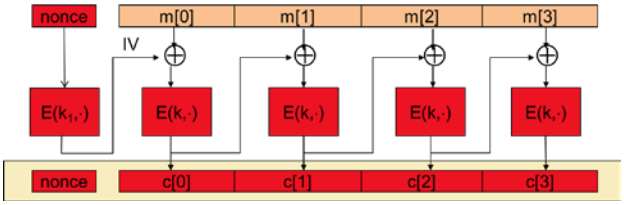

IV:




Ciphertext:



**10)** What is the corresponding ciphertext for the below message if nonce-based CBC is used for encryption. [15 points]




**Note:**

i. *Suppose that the underlying block cipher is 3DES,*
ii. *The* $\boldsymbol{E(k_1,\cdot)}$ *function shifts the nonce, 1 bit to the left,*
iii. *The* $\boldsymbol{E(k,\cdot)}$ *function shifts the input, 1 bit to the right,*
iv. *Nonce should be encrypted first, and then used as IV in the next round,*
v. *Suppose each item in the array cell is just one byte,*
vi. *Make sure that you append the padding block first to your message, then encrypt it.*

Message:

| 2 | 1 | 0 | 2 | 3 | 0 | 1 | 4 | 1 | 0 | 1 | 0 | 1 | 3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |

nonce:

| 1 | 0 | 2 | 3 | 0 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

**11)** Given the following messages with different length for encryption through CBC mode, ***identify the padding block size and content for each message***. *Suppose that the underlying block cipher is AES*. In addition, suppose each character is one byte. [5 points]

| Message | Padding block size | Content of padding block |
|---|---|---|
| **H E L L O W O R L D** | | |
| A C K N O W L E D G E M E N T S | | |
| A C C O M M O D A T I V E N E S S | | |