CIS4362.01 Homework 2 Due: 10/13/19

Brandon Thompson 5517

October 13, 2019

1. Let G:K $\rightarrow \{0,1\}^n$ be a secure PRG. Define $G'(k_1, k_2) = G(k_1) \oplus G(k_2)$.
   Consider the following statistical test A on $\{0,1\}^n$,
   $A(x)$ outputs $LSB(x)$, the least significant bit if x.
   What is $Adv_{PRG}[A, G']$?
   You may assume that $LSB(G(k))$ is 0 for exactly half the seeds $k \in K$.

   Advantage Formula:
   $Adv_{PRG}[A, G] = \left|Pr_{k \leftarrow K}[A(G(k)) = 1] - Pr_{r \leftarrow \{0,1\}^n}[A(r) = 1]\right| \in [0, 1]$

$$Pr[A(G(k_1)) = 1] = \frac{1}{2}$$

$$Pr[A(G(k_2)) = 1] = \frac{1}{2}$$

$$Pr[A(G(k_1) \oplus G(k_2)) = 1] = \frac{1}{2}$$

$$Pr[A(r) = 1] = \frac{1}{2}$$

$$\mathbf{Adv_{PRG}} = \left|\mathbf{\frac{1}{2}} - \mathbf{\frac{1}{2}}\right| = 0$$

2. Recall that the Luby-Rackoff theorem discussed in *The Data Encryption Standard lecture* states that applying a **three** round Feistal network to a secure PRF gives a secure block cipher. Let's see what goes wrong if we only use a **two** round Feistal. Let F:K $\times \{0,1\}^{32} \rightarrow \{0,1\}^{32}$ be a secure PRF.
Recall that a 2-round Feistal defins the following PRP
$F_2 : K^2 \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$

Here R_0 is the right 32 bits of the 64-bit input and L_0 i the left 32-bits.

One of the following lines is the output of this PRP F_2 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 F_2 from random, F_2 is not a secure block cipher, which is what we wanted to show.
Hint: First argue that there is detectable pattered in the xor of F_2

On input 0^{64} the output is "e86d2de2 e1387ae9". On input $1^{32}0^{32}$ the output is "1792d21d b645c008".

3. Nonce-based encryption has been implemented in HTTPS and IPSec design. Please explain how nonce has been implemented in these two protocols.

HTTPS: Nonce is used to validate credentials of clients and servers, calculate MD5 hashes for passwords. Because the nonce is different every time it makes replay attacks virtually impossible.

IPSec: Nonce is used to allow repeated use of private Diffie Hellman parameters

4. Let m be a message consisting of ℓ 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 $\frac{\ell}{2}$ 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?

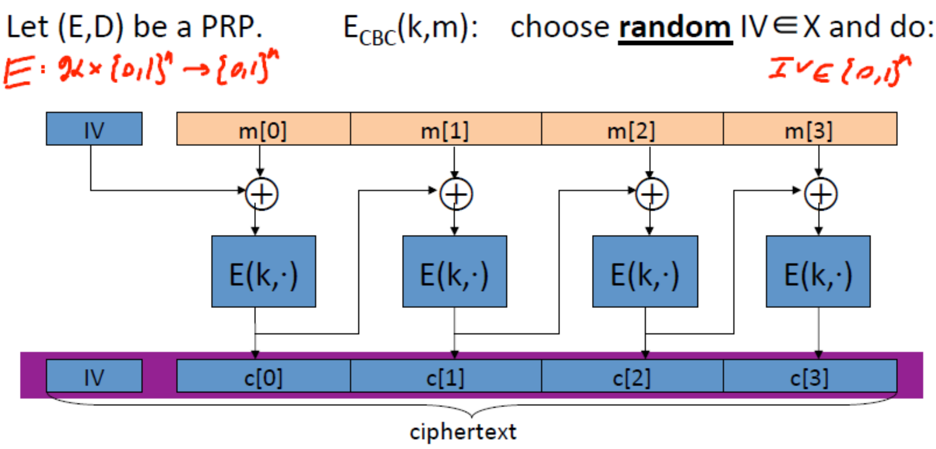

Figure 1: CBC Mode

Because the previous ciphertext is used in the calculating the next ciphertext, if one is corrupted in transmission then it is used in decrypting two ciphertexts.

5. Let m be a message consisting of ℓ 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 $\frac{\ell}{2}$ is corrupted during transmission. All other ciphertext blocks are transmitted and recieved correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?

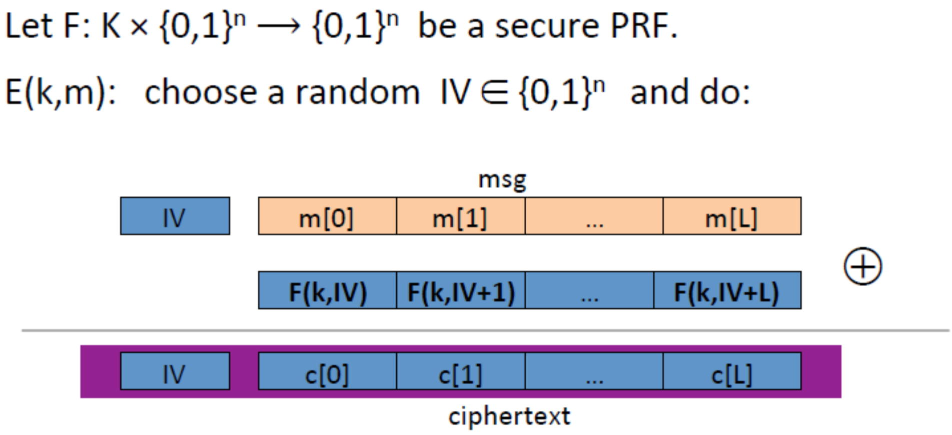

Figure 2: Randomized Counter Mode

Because no previous ciphertexts are used in encrypting, if one is corrupted during transmission it will only effect the same message block.

6. 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 $F : K \times \{0,1\}^{\ell} \to \{0,1\}^{\ell}$ be a secure PRP with, say $\ell = 128$. Let n be a nonce and suppose one encrypts a message 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 (c_0, c_1). Observe that by definition of CBC we know that $c_1 = F(k, c_0)$.

Next, the attacker asks for the encryption of the one block message $m_1 = c_0 \oplus c_1$ with nonce $n = c_0$. It receives back a once block ciphertext c_0'.

What relation holds between c_0, c_1, c_0'? Note that this relation lets the adversary win the nonce-based CPA game with advantage 1.

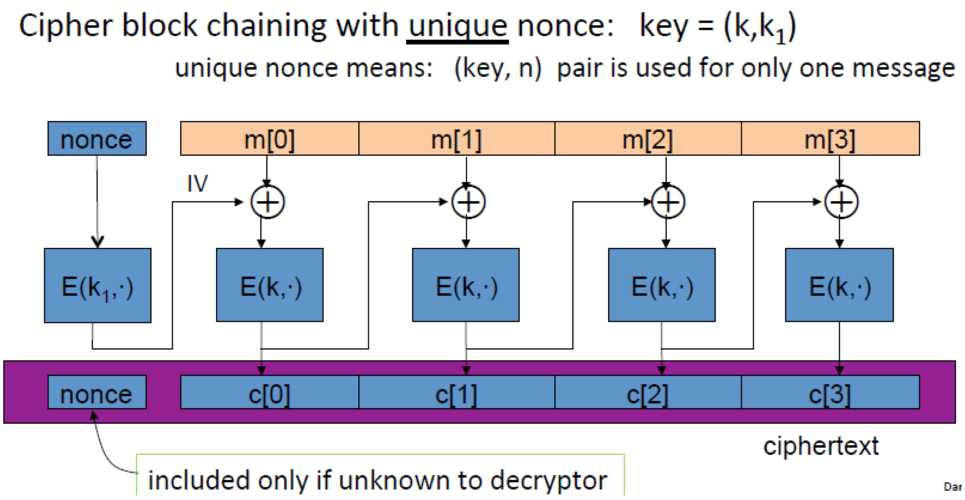

Figure 3: Nonce-based CBC

$$
\begin{aligned}
\text{Nonce} &= 0^{128} \\
m_0 &= \left(0^{128}, 0^{128}\right) \\
F\left(k, \text{nonce}\right) &= IV \\
F\left(m_0 \oplus IV\right) &= \left(c_0, c_1\right) \\
c_1 &= F\left(k, c_0\right) \\
\text{Nonce} &= c_0 \\
m_1 &= \left(c_0 \oplus c_1\right) \\
F\left(k, \text{nonce}\right) &= c_1 \qquad \textit{See line 5} \\
F\left(k, c_1 \oplus \left(c_0 \oplus c_1\right)\right) &= c_0'
\end{aligned}
$$

The association between c_0, c_1, c_0' is that $c_0 = c_0'$.

7. What is the corresponding ciphertext for the below message if CBC with random IV is used for encryption.

   Note:

   i. *Suppose that the underlying block cipher is AES.*

   ii. *The $E(k, \cdot)$ function shifts the input, 1 bit to the left.*

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

   iv. *Make sure that you append the padding block before encrypting.*

Message:

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

IV:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	3	0	1	4	1	1	1	2	1	0	0	1	3	0	0

Ciphertext:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
IV	3	0	0	0	0	0	1	0	2	0	3	2	0	3	4	1

Figure 4: Answer to question 7

8. Given the following messages with different length for encryption through CBC mode, *Identify the padding block size and content for each message. Suppose the underlying block cipher is AES.* In addition, suppose each character is one byte.

Message	Padding block size	Content of padding block
H E L L O W O R L D	6	6
A C K N O W L E D G E M E N T S	16	16
A C C O M M O D A T I V E N E S S	15	15

Figure 5: Answer to question 8