Suggested Solutions to Homework Assignment #1B

(prepared by Willy Chang)

1. Exercise problems from [Stallings 6E, intl.]:

5.2 (Modified)

a. $\{02\}^{-1}=\{8D\}$

b. We need to show that the transformation defined by Equation 5.2, when applied to $\{02\}^{-1}$, produces the correct entry in the S-box. We have

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

The result is $\{77\}$, which is the same as the value for $\{02\}$ in the S-box (Table 5.2a).

5.4 **a**.

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

b.

01	05	09	0D
00	04	08	0C
03	07	0B	0F
02	06	0A	0E

c.

7C	6B	01	D7
63	F2	30	FE
7B	C5	2B	76
77	6F	67	AB

d.

7C	6B	01	D7
F2	30	FE	63
2B	76	7B	C5
AB	77	6F	67

e.

75	87	0F	B2
55	E6	04	22
3E	2E	B8	8C
10	15	58	0A

5.6 **a.** AddRoundKey

b. The MixColumn step, because this is where the different bytes interact with each other.

c. The ByteSub step, because it contributes nonlinearity to AES.

d. The ShiftRow step, because it permutes the bytes.

e. There is no wholesale swapping of rows or columns. AES does not require this step because: The MixColumn step causes every byte in a column to alter every other byte in the column, so there is not need to swap rows; The ShiftRow step moves bytes from one column to another, so there is no need to swap columns.

6.4 **a.** No. For example, suppose C_1 is corrupted. The output block P_3 depends only on the input blocks C_2 and C_3.

b. An error in P_1 affects C_1. But since C_1 is input to the calculation of C_2, C_2 is affected. This effect carries through indefinitely, so that all ciphertext blocks are affected. However, at the receiving end, the decryption algorithm restores the correct plaintext for blocks except the one in error. You can show this by writing out the equations for the decryption. Therefore, the error only effects the corresponding decrypted plaintext block.

6.8 (Modified) As CFB mode has a step of shift register, if there's a bit error occurs in a segment of ciphertext, in the decryption phase, not only will that problematic ciphertext segment itself fail to be decrypted correctly, it will also be put into the shift register for the follow-up segments' decryption, causing the decryption of other segments to be incorrect as well.

The length the error propagates depends on how long the time that problematic ciphertext segment stays in the shift register. In our context here, with $b = 128, s = 8$, the error segment will stay in the shift register for the next 16 rounds of decryption, thus 16 segments the propagation will be. Counting the error segment itself, totally are there 17 segments being affected.

6.12 **a**. Assume that the last block (P_N) has j bits.
After encrypting the last full block (P_{N-1}), encrypt the ciphertext (C_{N-1}) again, select the leftmost j bits of the encrypted ciphertext, and XOR that with the short block to generate the output ciphertext.

b. While an attacker cannot recover the last plaintext block, he can change it systematically by changing individual bits in the ciphertext. If the last few bits of the plaintext contain essential information, this is a weakness.

7.1 We give the result for $a = 3$:
1, 3, 9, 27, 19, 26, 16, 17, 20, 29, 25, 13, 8, 24, 10, 30, 28, 22, 4, 12, 5, 15, 14, 11, 2, 6, 18, 23, 7, 21, 1

7.2 **a**. Maximum period is $2^{4-2} = 4$
b. a must be 3, 5, 11, or 13
c. The seed must be odd

2. Consider pseudorandom number generation based on block ciphers and assume AES-128 is used as the encryption algorithm. What is the expected period of the bit stream with the OFB mode of operation? Please justify your answer. (10 points)

Solution.

To compute the expected period of the bit stream, we shall first compute the expected number of rounds the encryption algorithm should go to generate a repeated block. And, multiplying the expected value with the block length, we derive the expected period of the bit stream.

In the following table, the first column is the number of rounds that the encryption algorithm has been applied. The second column shows the relationship between seeds. The third column shows the probability that the generated bit stream repeats exactly at the corresponding round. Assume that the initial seed value is V_0.

Let us look at the probability of repeat to happen at round 3, for example. The first part $\frac{1}{2^{128}-2}$ is the probability for $V_0 = V_3$, i.e., a repeat first occurs given that $V_0 \neq V_1$, $V_0 \neq V_2$. The fraction is reasoned as follows:

The AES encryption algorithm is invertible, a one-to-one mapping. There is no way that a newly block (here, it is V_3) equals to any previous generated block (V_1, V_2) as they have been mapped onto once. So the number of possibilities of this generated block (the denominator part of the fraction) should be $2^{128} - 2$ (without V_1 and V_2). And, the numerator part being one is trivial, for the only way that a repeat can occur we need V_3 to equal V_0.

The rest of the line represents the probability of having $V_0 \neq V_1$, $V_0 \neq V_2$ (with $V_1 \neq V_2$ for sure).

rounds	seed values transition	probability that the generated bit stream repeat
1	$V_0 \to V_1$	$\frac{1}{2^{128}}$
2	$V_0 \to V_1 \to V_2$	$\frac{1}{2^{128}-1} \times \frac{2^{128}-1}{2^{128}} = \frac{1}{2^{128}}$
3	$V_0 \to V_1 \to V_2 \to V_3$	$\frac{1}{2^{128}-2} \times \frac{2^{128}-1}{2^{128}} \times \frac{2^{128}-2}{2^{128}-1} = \frac{1}{2^{128}}$
$\vdots$	$\vdots$	$\vdots$
2^{128}	$V_0 \to V_1 \to \cdots \to V_{2^{128}}$	$\frac{1}{2^{128}}$

So, with the generalization up to round 2^{128}, the expected number of rounds to get a repeated bit stream is:

$1 \times \frac{1}{2^{128}} + 2 \times \frac{1}{2^{128}} + \cdots + 2^{128} \times \frac{1}{2^{128}}$
$= (1 + 2 + \cdots + 2^{128}) \times \frac{1}{2^{128}}$
$= \frac{(2^{128}+1)\times 2^{128}}{2} \times \frac{1}{2^{128}}$
$= \frac{(2^{128}+1)}{2}$
As a result, the expected period of the bit stream is $128 \times \frac{(2^{128}+1)}{2} = 64 \times (2^{128} + 1)$.

□