Suggested Solutions to Homework Assignment #1B

(prepared by Wei-Hsien Chang)

1. Exercise problems from [Stallings 2011]:

4.17 **a.** **Euclid**: gcd(2152, 764) = gcd(764, 624) = gcd(624, 140) = gcd(140, 64) = gcd(64, 12) = gcd(12, 4) = gcd(4, 0) = 4
Stein: $A_1 = 2152, B_1 = 764, C_1 = 1; A_2 = 1076, B_2 = 382, C_2 = 2; A_3 = 538, B_3 = 191, C_3 = 4; A_4 = 269, B_4 = 191, C_4 = 4; A_5 = 78, B_5 = 191, C_5 = 4; A_5 = 39, B_5 = 191, C_5 = 4; A_6 = 152, B_6 = 39, C_6 = 4; A_7 = 76, B_7 = 39, C_7 = 4; A_8 = 38, B_8 = 39, C_8 = 4; A_9 = 19, B_9 = 39, C_9 = 4; A_10 = 20, B_10 = 19, C_{10} = 4; A_{11} = 10, B_{11} = 19, C_{11} = 4; A_{12} = 5, B_{12} = 19, C_{12} = 4; A_{13} = 14, B_{13} = 5, C_{13} = 4; A_{14} = 7, B_{14} = 5, C_{14} = 4; A_{15} = 2, B_{15} = 5, C_{15} = 4; A_{16} = 1, B_{16} = 5, C_{16} = 4; A_{17} = 4, B_{17} = 1, C_{17} = 4; A_{18} = 2, B_{18} = 1, C_{18} = 4; A_{19} = 1, B_{19} = 1, C_{19} = 4;$
gcd(2152, 764) = 1×4 = 4

b. Euclid's algorithm requires a "long division" at each step whereas the Stein algorithm only requires division by 2, which is a simple operation in binary arithmetic.

5.1 We want to show that $d(x) = a(x) \times b(x) \bmod (x^4 + 1) = 1$. Substituting into Equation (5.12) in Appendix 5A, we have:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 0E \\ 09 \\ 0D \\ 0B \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

But this is the same set of equations discussed in the subsection on the MixColumn transformation:

$(\{0E\} \cdot \{02\}) \oplus \{0B\} \oplus \{0D\} \oplus (\{09\} \cdot \{03\}) = \{01\}$
$(\{09\} \cdot \{02\}) \oplus \{0E\} \oplus \{0B\} \oplus (\{0D\} \cdot \{03\}) = \{00\}$
$(\{0D\} \cdot \{02\}) \oplus \{09\} \oplus \{0E\} \oplus (\{0B\} \cdot \{03\}) = \{00\}$
$(\{0B\} \cdot \{02\}) \oplus \{0D\} \oplus \{09\} \oplus (\{0E\} \cdot \{03\}) = \{00\}$

The first equation is verified in the text. For the second equation, we have $\{09\} \cdot \{02\} = 00010010$; and $\{0D\} \cdot \{03\} = \{0D\} \oplus (\{0D\} \cdot \{02\}) = 00001101 \oplus 00011010 = 00010111$. Then

$$\begin{array}{lcl} \{09\} \cdot \{02\} & = & 00010010 \\ \{0E\} & = & 00001110 \\ \{0B\} & = & 00001011 \\ \{0D\} \cdot \{03\} & = & \underline{00010111} \\ & & 00000000 \end{array}$$

For the third equation, we have $\{0D\} \cdot \{02\} = 00011010$; and $\{0B\} \cdot \{03\} = \{0B\} \oplus (\{0B\} \cdot \{02\}) = 00001011 \oplus 00010110 = 00011101$. Then

$$\begin{array}{lcl} \{0D\} \cdot \{02\} & = & 00011010 \\ \{09\} & = & 00001001 \\ \{0E\} & = & 00001110 \\ \{0B\} \cdot \{03\} & = & \underline{00011101} \\ & & 00000000 \end{array}$$

For the fourth equation, we have $\{0B\} \cdot \{02\} = 00010110$; and $\{0E\} \cdot \{03\} = \{0E\} \oplus (\{0E\} \cdot \{02\}) = 00001110 \oplus 00011100 = 00010010$. Then

$$\begin{array}{lcl} \{0B\} \cdot \{02\} & = & 00010110 \\ \{0D\} & = & 00001101 \\ \{09\} & = & 00001001 \\ \{0E\} \cdot \{03\} & = & \underline{00010010} \\ & & 00000000 \end{array}$$

Thus, we found out $d(x) = a(x) \times b(x) \bmod (x^4 + 1) = 1$ by calculating these four equations.

5.2 **a.** $\{53\}^{-1} = \text{CA}$.

b. We need to show that the transformation defined by Equation 5.2, when applied to $\{53\}^{-1}$, produces the correct entry in the S-box. After converting {CA} to binary format (11001010), we get

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

The result is 1110 1101 = ED, which is the same as the value for {53} 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.** The question assumes that there was an error in block C_4 of the transmitted ciphertext.

ECB mode: In this mode, ciphertext block C_i is used only as input for the direct dencryption of plaintext block P_i. Therefore, a transmission error in block C_4 will only corrupt block P_4 of the decrypted plaintext.

CBC mode: In this mode, ciphertext block C_i is used as input to the XOR function when obtaining plaintext blocks P_i and P_{i+1}. Therefore, a transmission error in block C_4 will corrupt blocks P_4 and P_5 of the decrypted plaintext, but will not propagate to any of the other blocks.

CTR mode: In this mode, ciphertext block C_i, as well as the encrypted counter ti, are used only as input for the direct decryption of plaintext block P_i. Therefore, a transmission error in block C_4 will only corrupt block P_4 of the decrypted plaintext.

b. The question assumes that the ciphertext contains N blocks, and that there was a bit error in the source version of P_3.

ECB mode: In this mode, ciphertext block C_i is generated by direct encryption of plaintext block P_i, independent of the other plaintext or ciphertext blocks. Therefore, a bit error in block P_3 will only affect ciphertext block C_3 and will not propagate further. Thus, only one ciphertext block will be corrupted.

CBC mode: In this mode, ciphertext block C_i is generated by XORing plaintext block Pi with ciphertext block C_{i-1}. Therefore, a bit error in block P_3 will affect ciphertext block C_3, which in turn will affect ciphertext block C_4 and so forth, and therefore the error will propagate through all remaining ciphertext blocks. Thus, $N - 2$ ciphertext block will be corrupted.

CTR mode: In this mode, ciphertext block C_i is generated by applying the XOR function to plaintext block P_i and the encrypted counter t_i, independent of the other

plaintext or ciphertext blocks. Therefore, a bit error in block P_3 will only affect ciphertext block P_3 and will not propagate further. Thus, only one ciphertext block will be corrupted.

6.7 For this padding method, the padding bits can be removed unambiguously, provided the receiver can determine that the message is indeed padded. One way to ensure that the receiver does not mistakenly remove bits from an unpadded message is to require the sender to pad every message, including messages in which the final block is already complete. For such messages, an entire block of padding is appended.

2.

		0000 0	0001 1	0010 g	0100 g^2	1000 g^3	0011 g^4	0110 g^5
0000	0	0	0	0	0	0	0	0
0001	1	0	1	g	g^2	g^3	$g+1$	g^2+g
0010	g	0	g	g^2	g^3	$g+1$	g^2+g	g^3+g^2
0100	g^2	0	g^2	g^3	$g+1$	g^2+g	g^3+g^2	g^3+g+1
1000	g^3	0	g^3	$g+1$	g^2+g	g^3+g^2	g^3+g+1	g^2+1
0011	g^4	0	$g+1$	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g
0110	g^5	0	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1
1100	g^6	0	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g
1011	g^7	0	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1
0101	g^8	0	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1
1010	g^9	0	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1
0111	g^{10}	0	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1
1110	g^{11}	0	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g
1111	g^{12}	0	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2
1101	g^{13}	0	g^3+g^2+1	g^3+1	1	g	g^2	g^3
1001	g^{14}	0	g^3+1	1	g	g^2	g^3	$g+1$

...

1100 g^6	1011 g^7	0101 g^8	1010 g^9	0111 g^{10}	1110 g^{11}	1111 g^{12}	1101 g^{13}
0	0	0	0	0	0	0	0
g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1
g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1
g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1
g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g
g^2+g+1	g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2
g^3+g^2+g	g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2	g^3
g^3+g^2+g+1	g^3+g^2+1	g^3+1	1	g	g^2	g^3	$g+1$
g^3+g^2+1	g^3+1	1	g	g^2	g^3	$g+1$	g^2+g
g^3+1	1	g	g^2	g^3	$g+1$	g^2+g	g^3+g^2
1	g	g^2	g^3	$g+1$	g^2+g	g^3+g^2	g^3+g+1
g	g^2	g^3	$g+1$	g^2+g	g^3+g^2	g^3+g+1	g^2+1
g^2	g^3	$g+1$	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g
g^3	$g+1$	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1
$g+1$	g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g
g^2+g	g^3+g^2	g^3+g+1	g^2+1	g^3+g	g^2+g+1	g^3+g^2+g	g^3+g^2+g+1

...

1001 g^{14}
0
g^3+1
1
g
g^2
g^3
$g+1$
g^2+g
g^3+g^2
g^3+g+1
g^2+1
g^3+g
g^2+g+1
g^3+g^2+g
g^3+g^2+g+1
g^3+g^2+1

3. In the CTR mode, the seed value (V) will be incremented by 1 after each encryption. Thanks to the invertibility of the encryption algorithm, different values of V give rise to different pseudorandom bits. Only when the value of V loops back to the initial value, the whole

stream will repeat. V has 2^{128} possible values, each producing 128 pseudorandom bits. So, the period of the pseudorandom bit stream is 128×2^{128} bits long.