

**Computer and Network Security
Fall Semester 2002**

Quiz No. 3

September 3, 2002

Time Allowed: 20 Minutes

Name: SOLUTION

Total: 20 Points

Question 1:

Work out the output of the Expansion Permutation if the input is 0xA3C5EF01. Expansion Permutation is given below: (5 points)

<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr><td>32</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr> <tr><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td></tr> <tr><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td></tr> <tr><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td></tr> <tr><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td></tr> <tr><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr> <tr><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td></tr> <tr><td>28</td><td>29</td><td>30</td><td>31</td><td>32</td><td>1</td></tr> </table>	32	1	2	3	4	5	4	5	6	7	8	9	8	9	10	11	12	13	12	13	14	15	16	17	16	17	18	19	20	21	20	21	22	23	24	25	24	25	26	27	28	29	28	29	30	31	32	1	<table style="width: 100%; border-collapse: collapse;"> <tr><td>A</td><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>D0</td></tr> <tr><td>3</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>7</td></tr> <tr><td>C</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>E0</td></tr> <tr><td>5</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td><td>B</td></tr> <tr><td>E</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>1</td><td>F5</td></tr> <tr><td>F</td><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>E</td></tr> <tr><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>80</td></tr> <tr><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>3</td></tr> </table> <p style="border: 1px solid black; padding: 5px; margin-top: 5px;">$E(0xA3C5EF01) = 0xD07E0BF5E803$</p>	A	1	1	0	1	0	0	D0	3	0	0	0	1	1	1	7	C	1	1	1	0	0	0	E0	5	0	0	1	0	1	1	B	E	1	1	1	1	0	1	F5	F	0	1	1	1	1	0	E	0	1	0	0	0	0	0	80	1	0	0	0	0	1	1	3
32	1	2	3	4	5																																																																																																												
4	5	6	7	8	9																																																																																																												
8	9	10	11	12	13																																																																																																												
12	13	14	15	16	17																																																																																																												
16	17	18	19	20	21																																																																																																												
20	21	22	23	24	25																																																																																																												
24	25	26	27	28	29																																																																																																												
28	29	30	31	32	1																																																																																																												
A	1	1	0	1	0	0	D0																																																																																																										
3	0	0	0	1	1	1	7																																																																																																										
C	1	1	1	0	0	0	E0																																																																																																										
5	0	0	1	0	1	1	B																																																																																																										
E	1	1	1	1	0	1	F5																																																																																																										
F	0	1	1	1	1	0	E																																																																																																										
0	1	0	0	0	0	0	80																																																																																																										
1	0	0	0	0	1	1	3																																																																																																										

Question 2:

What would the output be for the S2 box for each one of the following five binary inputs (1) 000101 (2) 101101 (3) 010101 (4) 111010 (5) 100111. The S2 box is given in the figure below. (5 points)

<p align="center">Table 3.6 Primitive S-Box Functions</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td colspan="15" style="text-align: center;">S_1</td></tr> <tr><td>14</td><td>4</td><td>13</td><td>1</td><td>2</td><td>15</td><td>11</td><td>8</td><td>3</td><td>10</td><td>6</td><td>12</td><td>5</td><td>9</td><td>0</td><td>7</td></tr> <tr><td>0</td><td>15</td><td>7</td><td>4</td><td>14</td><td>2</td><td>13</td><td>1</td><td>10</td><td>6</td><td>12</td><td>11</td><td>9</td><td>5</td><td>3</td><td>8</td></tr> <tr><td>4</td><td>1</td><td>14</td><td>8</td><td>13</td><td>6</td><td>2</td><td>11</td><td>15</td><td>12</td><td>9</td><td>7</td><td>3</td><td>10</td><td>5</td><td>0</td></tr> <tr><td>15</td><td>12</td><td>8</td><td>2</td><td>4</td><td>9</td><td>1</td><td>7</td><td>5</td><td>11</td><td>3</td><td>14</td><td>10</td><td>0</td><td>6</td><td>13</td></tr> <tr><td colspan="15" style="text-align: center;">S_2</td></tr> <tr><td>15</td><td>1</td><td>8</td><td>14</td><td>6</td><td>11</td><td>3</td><td>4</td><td>9</td><td>7</td><td>2</td><td>13</td><td>12</td><td>0</td><td>5</td><td>10</td></tr> <tr><td>3</td><td>13</td><td>4</td><td>7</td><td>15</td><td>2</td><td>8</td><td>14</td><td>12</td><td>0</td><td>1</td><td>10</td><td>6</td><td>9</td><td>11</td><td>5</td></tr> <tr><td>0</td><td>14</td><td>7</td><td>11</td><td>10</td><td>4</td><td>13</td><td>1</td><td>5</td><td>8</td><td>12</td><td>6</td><td>9</td><td>3</td><td>2</td><td>15</td></tr> <tr><td>13</td><td>8</td><td>10</td><td>1</td><td>3</td><td>15</td><td>4</td><td>2</td><td>11</td><td>6</td><td>7</td><td>12</td><td>0</td><td>5</td><td>14</td><td>9</td></tr> <tr><td colspan="15" style="text-align: center;">S_3</td></tr> <tr><td>10</td><td>0</td><td>9</td><td>14</td><td>6</td><td>3</td><td>15</td><td>5</td><td>1</td><td>13</td><td>12</td><td>7</td><td>11</td><td>4</td><td>2</td><td>8</td></tr> <tr><td>13</td><td>7</td><td>0</td><td>9</td><td>3</td><td>4</td><td>6</td><td>10</td><td>2</td><td>8</td><td>5</td><td>14</td><td>12</td><td>11</td><td>15</td><td>1</td></tr> <tr><td>13</td><td>6</td><td>4</td><td>9</td><td>8</td><td>15</td><td>3</td><td>0</td><td>11</td><td>1</td><td>2</td><td>12</td><td>5</td><td>10</td><td>14</td><td>7</td></tr> <tr><td>1</td><td>10</td><td>13</td><td>0</td><td>6</td><td>9</td><td>8</td><td>7</td><td>4</td><td>15</td><td>14</td><td>3</td><td>11</td><td>5</td><td>2</td><td>12</td></tr> </table>	S_1															14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	S_2															15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	S_3															10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	<p>(1) $S_2^{01}(0010) = 4 = 0100$</p> <p>(2) $S_2^{11}(0110) = 4 = 0100$</p> <p>(3) $S_2^{01}(1010) = 8 = 1000$</p> <p>(4) $S_2^{10}(1101) = 3 = 0011$</p> <p>(5) $S_2^{11}(0011) = 1 = 0001$</p>
S_1																																																																																																																																																																																																																																														
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7																																																																																																																																																																																																																															
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8																																																																																																																																																																																																																															
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0																																																																																																																																																																																																																															
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13																																																																																																																																																																																																																															
S_2																																																																																																																																																																																																																																														
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10																																																																																																																																																																																																																															
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5																																																																																																																																																																																																																															
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15																																																																																																																																																																																																																															
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9																																																																																																																																																																																																																															
S_3																																																																																																																																																																																																																																														
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8																																																																																																																																																																																																																															
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1																																																																																																																																																																																																																															
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7																																																																																																																																																																																																																															
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12																																																																																																																																																																																																																															

Question 3:

Work out the output of the Permutation Function (P) if the input is 0xA3C5EF01.

Permutation Function (P) is given below:

(5 points)

<table style="width: 100%; border-collapse: collapse;"> <tr><td style="border-top: 1px solid black; border-bottom: 1px solid black;">16</td><td style="border-top: 1px solid black; border-bottom: 1px solid black;">7</td><td style="border-top: 1px solid black; border-bottom: 1px solid black;">20</td><td style="border-top: 1px solid black; border-bottom: 1px solid black;">21</td></tr> <tr><td>9</td><td>12</td><td>28</td><td>17</td></tr> <tr><td>1</td><td>15</td><td>23</td><td>26</td></tr> <tr><td>5</td><td>18</td><td>31</td><td>10</td></tr> <tr><td>2</td><td>8</td><td>24</td><td>14</td></tr> <tr><td>32</td><td>27</td><td>3</td><td>9</td></tr> <tr><td>19</td><td>13</td><td>30</td><td>6</td></tr> <tr><td style="border-bottom: 1px solid black;">22</td><td style="border-bottom: 1px solid black;">11</td><td style="border-bottom: 1px solid black;">4</td><td style="border-bottom: 1px solid black;">25</td></tr> </table>	16	7	20	21	9	12	28	17	1	15	23	26	5	18	31	10	2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25	<table style="width: 100%; border-collapse: collapse;"> <tr><td>A</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>1</td><td>D</td></tr> <tr><td>3</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>9</td></tr> <tr><td>C</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>A</td></tr> <tr><td>5</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>5</td></tr> <tr><td>E</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>7</td></tr> <tr><td>F</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>1</td><td>1</td><td>B</td></tr> <tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>8</td></tr> <tr><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>8</td></tr> </table>	A	1	0	1	0	1	1	0	1	D	3	0	0	1	1	1	0	0	1	9	C	1	1	0	0	1	0	1	0	A	5	0	1	0	1	0	1	0	1	5	E	1	1	1	0	0	1	1	1	7	F	1	1	1	1	1	0	1	1	B	0	0	0	0	0	1	0	0	0	8	1	0	0	0	1	1	0	0	0	8
16	7	20	21																																																																																																														
9	12	28	17																																																																																																														
1	15	23	26																																																																																																														
5	18	31	10																																																																																																														
2	8	24	14																																																																																																														
32	27	3	9																																																																																																														
19	13	30	6																																																																																																														
22	11	4	25																																																																																																														
A	1	0	1	0	1	1	0	1	D																																																																																																								
3	0	0	1	1	1	0	0	1	9																																																																																																								
C	1	1	0	0	1	0	1	0	A																																																																																																								
5	0	1	0	1	0	1	0	1	5																																																																																																								
E	1	1	1	0	0	1	1	1	7																																																																																																								
F	1	1	1	1	1	0	1	1	B																																																																																																								
0	0	0	0	0	1	0	0	0	8																																																																																																								
1	0	0	0	1	1	0	0	0	8																																																																																																								
	$P(0xA3C5EF01) = 0xD9A57B88$																																																																																																																

Question 4: Circle the Correct Choice (5 points – 0.5 point each)

1. Data Encryption Standard uses a key length and block size of respectively

- a. 64 and 56 bits **b. 56 and 64 bits** c. 56 and 56 bits d. 64 and 64 bits

2. According to the shift schedule for the encipherment key the number of left shifts for the key in round 11 in DES is

- a. 2** b. 3

3. A mode of use that can be employed to prevent subversion of DES when used as a block cipher is:

- a. ECB **b. CBC** c. OFB d. RC5

4. Which of the following is not a mode of use of DES

- a. OFB b. CFB c. ECB **d. RC5**

5. When using DES in Cipher Block Chaining mode, the repetitions in message can be reflected in cipher-text.

- a. True **b. False**

6. With a 128 bit key length for a block cipher, the number of possible keys is:

- a. 10^{128} b. 3.40×10^{128} c. 2×10^{38} **d. 3.40×10^{38}**

7. Data Encryption Standard when used in electronic codebook mode is a mono-alphabetic block substitution cipher.

- a. False **b. True**

8. Diffusion is achieved through permutations.

- a. True** b. False

9. Diffusion is achieved through substitutions.

- a. True **b. False**

10. In which stream mode does an error during data transmission propagate to future bytes?

- a. ECB b. CBC **c. CFB** d. OFB