A

جامعــة الأمــيرة ســمية للتكـنولـوجـيا

PSUT

Princess Sumaya University for Technology

Information Systems Security (11464)
Second Exam, Fall 2017/2018

Jan 13, 2018

Time Allowed: 60 minutes

Instructor Name: ....

Section Time: ______________________

Student Name: ________________________

Student Number: |__|__|__|__|__|__|__|__|

Question	Points	Score
1	5	
2	4	
3	6	
4	6	
5	4	
Total	25	

Note that try to show your calculations for needed questions

Question (1): Circle the correct answer:**(5 Marks)**

1. **What is data encryption standard (DES)?**

   a) Block cipher b) Stream cipher c) Bit cipher

   d) Both a and b e) None of the above

2. **There are ________________ smaller numbers that are coprime with 101.**

   a) 95 b) 100 c) 102

   d) 101 e) None of the above

3. **One of the following methods make password guessing is hard to crack?**

   a) Limited time period b) Minimum length c) Last Login message

   d) Limited attempts e) All of the above

4. **Using a modulus of n=676, one of the following is not a valid key for modular multiplication encryption**

   a) 2 b) 13 c) 8

   d) 16 e) All of the above

5. **In DES algorithm, the key size is:**

   a) 64 b) 56 c) 128

   d) 16 e) None of the above

6. **One of the authentications does not need additional authentication devices?**

   a) Some thing you know b) Something you have c) Static biometric (physiological)

   d) Dynamic biometric (behavioral) e) All of the above

7. **The __________ strategy is when users are told the importance of using hard to guess passwords and provided with guidelines for selecting strong passwords.**

   a) proactive password checking b) user education c) reactive password checking

   d) computer-generated password e) None of the above

8. **A __________ is a password guessing program.**

   a) Password Cracker b) password hash c) password salt

   d) password biometric e) None of the above

9. **Recognition by fingerprint, retina, and face are examples of __________.**

   a) face recognition b) static biometrics c) token authentication

   d) dynamic biometrics e) None of the above

10. **Each individual who is to be included in the database of authorized users must first be __________ in the system.**

    a) verified b) authenticated c) identified

    d) enrolled e) None of the above

Question (2): (4 Marks)

a) **Describe the general concept of a challenge-response protocol. (2 Points)**

b) **What are the aims of using the Salt in password system? (2 Points)**

Answer:

Question (3): (6 Marks)

a) Assume the following is the input for **DES s-boxes**
100010 001000 100110 010011 000000 011101 000000 000111

What is the output from **DES S-boxes for S2 and S5**? Write the results in hexdecimal. **(2 Points)**

b) Show the first six words (**W0, W1, W2, W3, W4, W5**) of the key expansion for a **128-bit key of all ones in AES**. **(4 points)**

Rule 1: K[n] : W[i] = K[n-1]: W[i] XOR K[n]: w[i-1]
Rule 2: K[n]: W0 = K[n-1]: W0 xor SubByte (K[n-1] : W3 >>8) XOR Rcon[n]

Question 4: (6 Marks)

a) Perform the following **RSA** key generation steps. Each step must satisfy the requirements of RSA. Suppose **p= 7** and **q=11**, show how you can deal with large number if you have a need for that**.**

1. Compute the **Modula (n)** and **φ(n)** **(1 Point)**

2. If **d= 43 choose the suitable public key from the list (3, 67, 7).** Show your calculations. **(1 Point)**

3. Determine the public and private keys. **(1 Point)**

4. If Bob uses the same *n* for his key pair, and his public key is 13, what is his private key? **choose the suitable private key from the list (6, 97, 37).** Show your calculations. **(1 Point)**

5. If the message **(M)= "2"**, **Encrypt this message** by using the **values for e and d** according to question **5**. **(1 Point)**

Question 5: Answer of the following and show your calculations **(4 Marks)**

1. -25 mod 19 =

2. State which if any of the following pairs are congruent modulo 10:
   1. 17, 6
   2. 25, 5

3. Using Fermat's theorem compute 13^{17} mod 17 =

4. Calculate the Euler Totient Function Ø(n), where n= 20.

Appendix:

The English alphabitcal order: a b c d e f g h i j k l m n o p q r s t u v w x y z

S-DES

IP							
2	6	3	1	4	8	5	7

IP^{-1}							
4	1	3	5	7	2	8	6

P10									
3	5	2	7	4	10	1	9	8	6

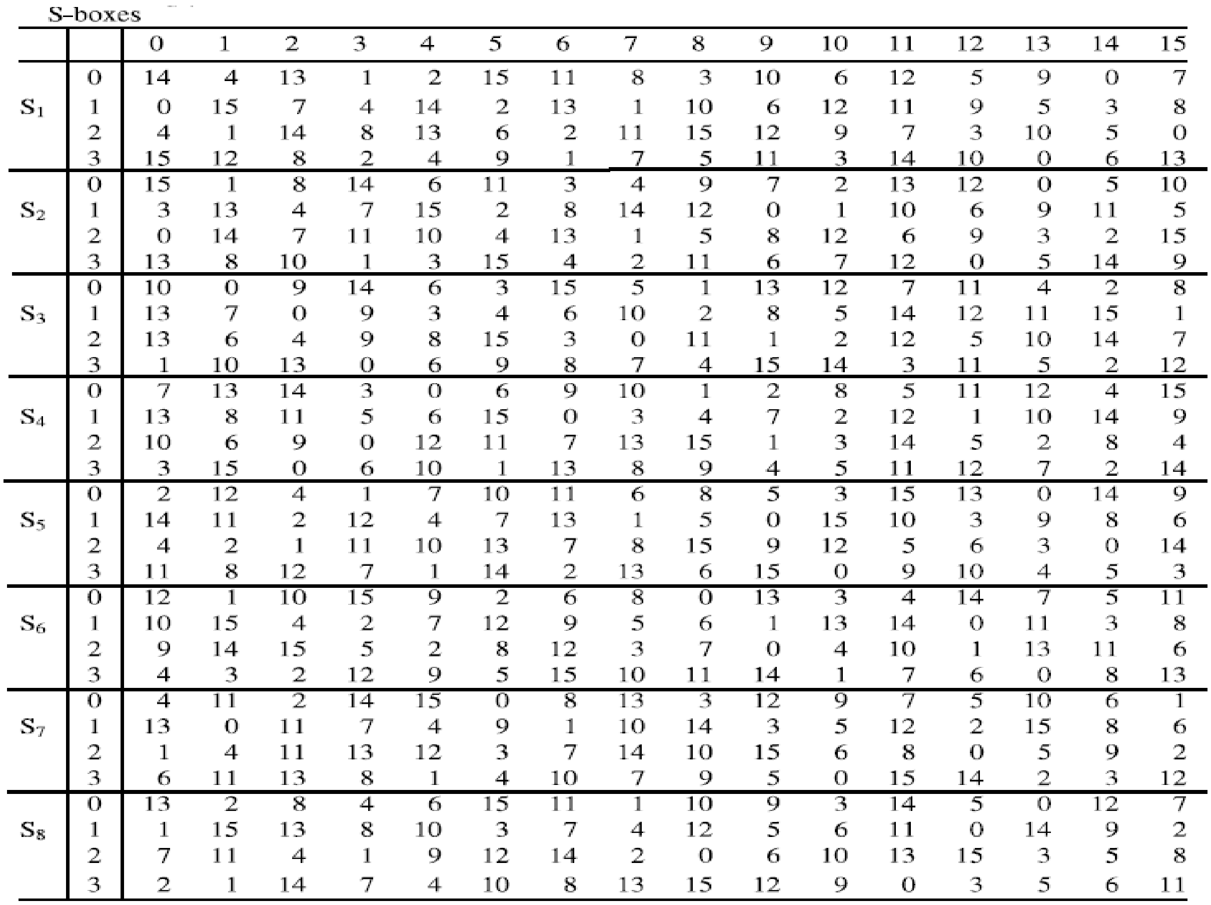
P8							
6	3	7	4	8	5	10	9

E/P							
4	1	2	3	2	3	4	1

P4			
2	4	3	1

$$S0 = \begin{array}{c|cccc|} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & \mathbf{3} & 2 \\ \hline \end{array} \qquad S1 = \begin{array}{c|cccc|} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & \mathbf{2} & 1 & 0 & 3 \\ \hline \end{array}$$

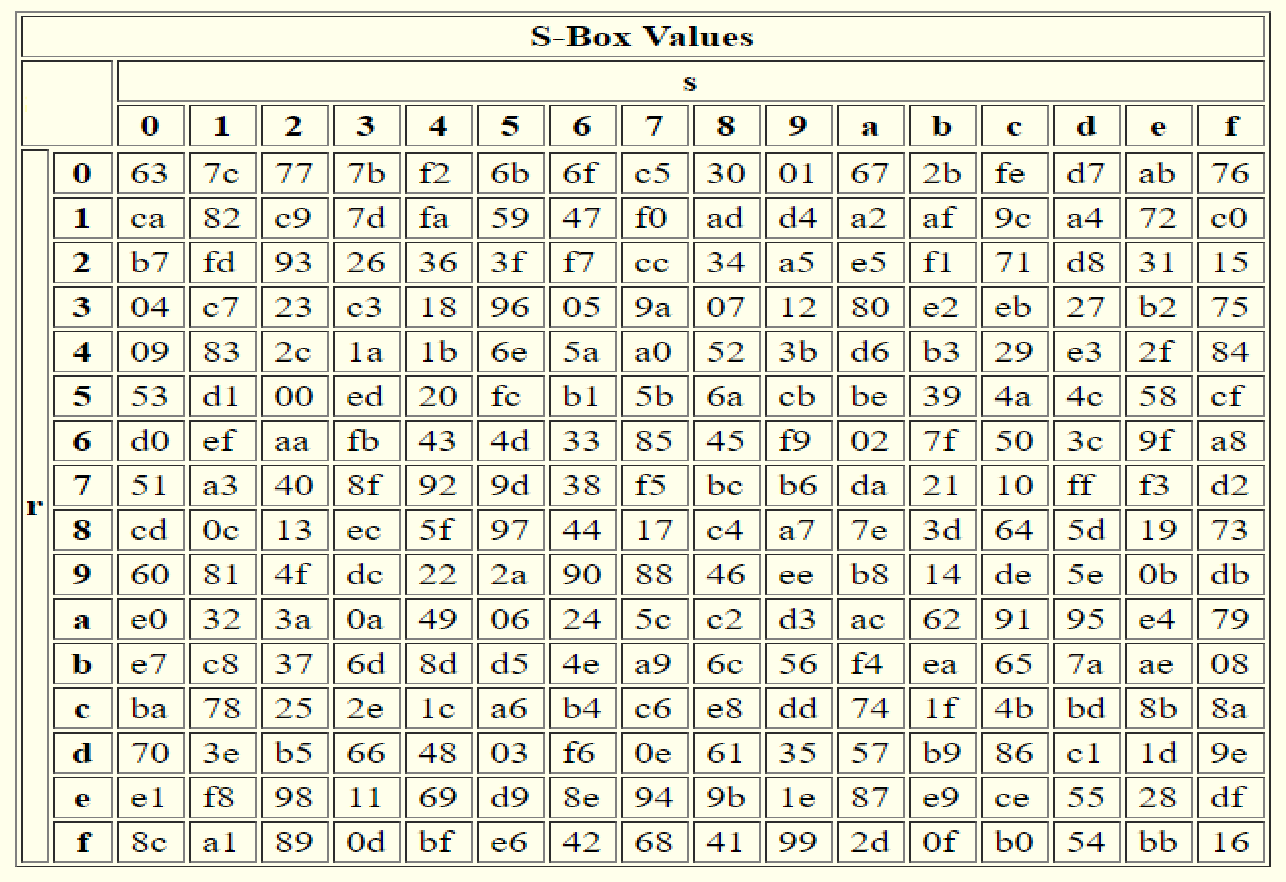
DES



S–boxes

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
S_1	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
S_2	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
S_3	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
S_4	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
S_5	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
S_6	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
S_7	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
S_8	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

AES: SubByte Table



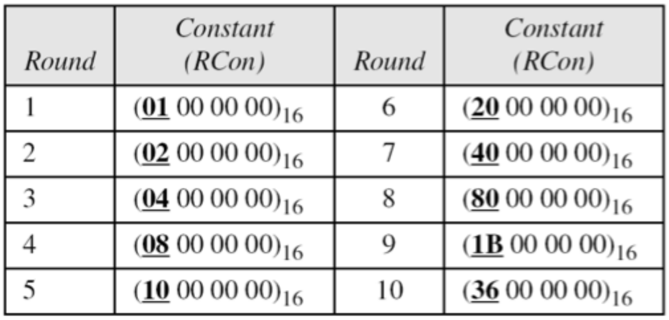
S-Box Values

		s															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**
r	**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

Constant multiplication matrix

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}.$$

Round Constant (RCon)



Round	*Constant (RCon)*	*Round*	*Constant (RCon)*
1	$(\underline{\mathbf{01}}\ 00\ 00\ 00)_{16}$	6	$(\underline{\mathbf{20}}\ 00\ 00\ 00)_{16}$
2	$(\underline{\mathbf{02}}\ 00\ 00\ 00)_{16}$	7	$(\underline{\mathbf{40}}\ 00\ 00\ 00)_{16}$
3	$(\underline{\mathbf{04}}\ 00\ 00\ 00)_{16}$	8	$(\underline{\mathbf{80}}\ 00\ 00\ 00)_{16}$
4	$(\underline{\mathbf{08}}\ 00\ 00\ 00)_{16}$	9	$(\underline{\mathbf{1B}}\ 00\ 00\ 00)_{16}$
5	$(\underline{\mathbf{10}}\ 00\ 00\ 00)_{16}$	10	$(\underline{\mathbf{36}}\ 00\ 00\ 00)_{16}$