جامعة الأميرة سمية للتكنولوجيا

PSUT

Princess Sumaya University for Technology

Computer Science Department
Information Systems Security (11464)
First Exam, Fall 2016/2017

November 2, 2017

Time Allowed: 60 minutes

Instructor Name: ....

Section Time: ______________________

Student Name: ________________________

Student Number:

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

Part I: Multiple Choices questions (10 x .5 = 5 Marks)

Answer all the following questions by choosing the most correct statement

1. **Which is the principle of the encryption using a key?**
   a) The key indicates which function is used for encryption. Thereby it is more difficult to decrypt an intercepted message as the function is unknown.
   b) The key contains the secret function for encryption including parameters. Only a password can activate the key.
   c) All functions are public, only the key is secret. It contains the parameters used for the encryption resp. decryption.
   d) The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption.
   e) None of the above

2. **One way to decouple from the linguistic patterns of the plaintext is to encrypt with a cipher that uses a succession of different keys. An example of this is**
   a) Caesar cipher
   b) Kirshoff cipher
   c) Monoalphabetic cipher
   d) Vigenère cipher
   e) All of the above

3. **Secure computer system must not allow information to be disclosed to anyone who is not authorized to access it means:**
   a) Confidentiality
   b) Integrity
   c) Non-repudiation
   d) Availability
   e) None of the above

4. **_________ attack involves an adversary repeating a previously captured user response.**
   a) Client
   b) Replay
   c) Trojan horse
   d) Eavesdropping
   e) None of the above

5. **One of the aspect of computer security that's mean, the system Hardware and software keeps working efficiently and is able to recover?**
   a) Integrity.
   b) Availability.
   c) Confidentiality.
   d) Non-repudiation
   e) All of the above.

6. **__________ is any action that compromises the security of information owned by an organization.**
   a) Security mechanism
   b) Security attack
   c) Security policy
   d) Security service
   e) None of the above

7. **An example of __________ is an attempt by an unauthorized user to gain access to a system by posing as an authorized user.**
   a) Masquerade
   b) Interception
   c) Repudiation
   d) Inference
   e) None of the above

8. **________ assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.**
   a) System Integrity
   b) Data Integrity
   c) Availability
   d) Confidentiality
   e) None of the above

9. **Which is the largest disadvantage of the symmetric Encryption?**
   a) More complex and therefore more time-consuming calculations.
   b) Problem of the secure transmission of the Secret Key.
   c) Less secure encryption function.
   d) Isn't used any more
   e) None of the above

10. **Message authentication codes (MAC) and digital signatures both serve to authenticate the content of a message. Which of the following best describes how they differ?**
   a) A MAC can be verified based only on the message, but a digital signature can only be verified with the secret key used to sign the message.
   b) A MAC can be verified based only on the message, but a digital signature can only be verified with the public key of the party that signed the message.
   c) A MAC can only be verified with the secret key used to generate it, but a digital signature can be verified based only on the message.
   d) A MAC can only be verified with the secret key used to generate it, but a digital signature can be verified with the public key of the party that signed the message.

Part 2: Essay questions (6x6 = 36 Marks)

Answer ONLY three of the following seven questions

Question 2:

a) Explain in detail about main security mechanisms of Public Key Algorithms? Give some of applications of public key algorithm (2 Marks).

Solution *(0.5 mark for each point)*

1) Key Establishment:
   - There are protocols for establishing secret keys over an insecure channel. Examples for such protocols include the Diffie-Hellman key exchange (DHKE) or RSA key transport protocols.
2) Nonrepudiation
   - Providing nonrepudiation and message integrity can be realized with digital signature algorithms, e.g., RSA, DSA or ECDSA.
3) Identification
   - We can identify entities using challenge-and-response protocols together with digital signatures, e.g., in applications such as smart cards for banking or for mobile phones.
4) Encryption
   - We can encrypt messages using algorithms such as RSA or Elgamal.

b) Explain how asymmetric system is used for key exchange (2 Marks):

Solution:

1) One of the parties, for instance, Alice generates the session key
2) Alice uses the second party's public key, for instance, Bob's public key is to encrypt the session key
3) Alice sends the encrypted session key to Bob
4) Bob decrypts the encrypted session key using his own private key
5) Both parties (Alice and Bob) share the same symmetric session key
6) The session key is used for encrypting their messages.

(0.3 mark for each point)

Question 3: (6 Marks)

a) In this problem, we will compare the security services that are provided by digital signatures (DS) and message authentication codes (MAC). We assume that Oscar is able to observe all messages sent from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how (i) DS and (ii) MAC protect against each attack. The value auth(x) is computed with a DS or a MAC algorithm, respectively (4 Marks).

i) Which one provide non-repudiation? If yes, explain. If no, explain why not?

Solution:
MAC: No. because the shared key, whereas the DS provide non-repudiation

ii) Which one provide authentication? If yes, explain how. If no, explain why not?

Solution: Both provide authentication.

iii) (Message integrity) Alice sends a message x = “Transfer $1000 to Mark” in the clear and also sends auth(x) to Bob. Oscar intercepts the message and replaces “Mark” with “Oscar.” Will Bob detect this?

Solution: Will be detected with both (i) DS and (ii) MAC.

iv) (Replay) Alice sends a message x = “Transfer $1000 to Oscar” in the clear and also sends auth(x) to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this? If the answer no write the solution for this problem.

Solution:

Won’t be detected by either (Remark: use timestamps).

b) In the context of encryption, what is a session Key? What are advantages and drawbacks of a session key? (2 Marks)

Solution:
A session key is a short symmetric key used by both parties to encrypt their secret messages. **(0.5 marks)**

Advantages of a Session Key:

- A session key is short.
- A session key imposes a much lower processing overhead than public key systems. **(0.5 mark for each point)**

Drawbacks of a session key:

- Low resistance to attack
- Session keys usually stay in service for a relatively short time (sometimes only a single transaction) before being discarded.

(0.5 mark for each point)

Part3: Problems Solving (10 Marks)

Note: You should show all the required steps and rules to solve these problems.

Question 4: Assuming you have computer can perform 5 decryptions/seconds. Compute the time required for brute-force attack for key size. **(3 Points)**

a) 8 bits
b) 6 character (permutations)

Assume that on average ¾ of all possible key must be tried to achieves success brute-force attack.

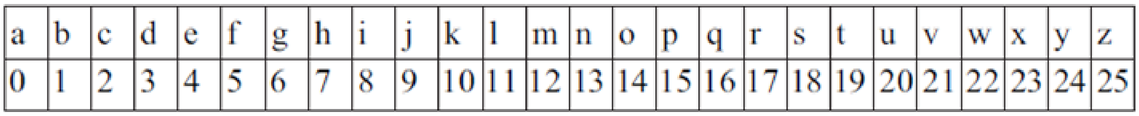
Solution:

a) Answer part (a):
   1. Number of alternative keys are: 2^8 = 256 keys
   2. To obtain the correct key we must try ¾ from possible alternative keys
   3. Number of Tries = 256*(3/4) = 192 keys
   4. Speed for your computer = 5 decryption/seconds
   5. Time required for brute force attack = 192/5 = 38.4 Seconds

b) Answer part (b):
   1. Number of alternative keys are: 6! = 6*5*4*3*2*1 = 720 keys
   2. To obtain the correct key we must try ¾ from possible alternative keys
   3. Number of Tries = 720*(3/4) = 540 keys
   4. Speed for your computer = 5 decryption/seconds
   5. Time required for brute force attack = 540/5 = 108 Seconds

Question 5: ***Caesar Cipher – Answer only one question from two questions***

Use the following table to help you find the code of letters:



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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

a) A manager of the Y-Bank received the following message "**EQZPYQYAZQK**" by his employee, they agreed to use Caesar Cipher for encryption and decryption, help the manager to decrypt the message if you know that the employee used the key of 2600000000012 for encryption, write the answer as readable sentence. Show your work in details (as table). (**4 marks**)

Answer:

K = 2600000000012 = 12

Decryption key = 26 – 12 = 14 *(1 mark)*

$p \equiv C + 14 \mod 26$ *(1 mark)*

Ciphertext	E	Q	Z	P	Y	Q	Y	A	Z	Q	K
code	4	16	25	15	24	16	24	0	25	16	10
C + 14 Mode 26	18	4	13	3	12	4	12	14	13	4	24
P	s	e	n	d	m	e	m	o	n	e	Y

(3 marks for each correct row)

The message is "send me money" *(1 mark)*

b) On a Caesar cipher text captured by an intruder, cryptanalysis showed that the highest frequency of the ciphertext letter is the letter "**Q**". If the captured message contains the word "**EQZPYQYAZQK**" then decrypt it. (**4 marks**)

Answer:

Guess: **Q** is the highest occurrence in the ciphertext = **E** is the highest occurrence in the ciphertext in the language => *16 = 4 + k (mod 26)* => *(16 -4)* => *k = 12.*

Decryption key = 26 – 12 = 14 *(1 mark)*

$p \equiv C + 14 \mod 26$ *(1 mark)*

Ciphertext	E	Q	Z	P	Y	Q	Y	A	Z	Q	K
code	4	16	25	15	24	16	24	0	25	16	10
C + 14 Mode 26	18	4	13	3	12	4	12	14	13	4	24
P	s	e	n	d	m	e	m	o	n	e	Y

(3 marks for each correct row)

The message is "send me money" *(1 mark)*

Question 6:

Decrypt the “**MITYESUSARAVYUNI**” by using **Row Transposition Ciphers**, if the key is “**361524**”. **(3 Points)**

3	6	1	5	2	4
S	U	M	A	Y	A
U	N	I	V	E	R
S	I	T	Y		

- Read plain text row by row Cipher text: **sumaya university**