


National University of Computer and Emerging Sciences, Lahore Campus

	Course Name:	Network Security	Course Code:	CS411
	Program:	BS (Computer Science)	Semester:	Spring 2018
	Duration:	180 Minutes	Total Marks:	88
	Paper Date:	21-May-2018	Weight	45
	Section:	-	Page(s):	8
	Exam Type:	Final		

Student : Name: _____ **Roll No.** _____
Section: _____

Instruction/Notes:

- 1. PLEASE DO NOT WRITE LONG STORIES. BE SPECIFIC!**
- 2. Attempt all questions on the question paper**
- 3. You are not allowed to take any part of the question paper with you**
- 4. You may use rough sheets but you don't need to attach them**
- 5. It is highly recommended to write answers in BULLETS.**

Q.No	Answer
1.6	C
1.7	C
1.8	D
1.9	E
1.10	A

Q.No	Answer
1.1	D
1.2	C
1.3	C
1.4	D

1.5	C

Q 01: Select the correct option and write them in the table above.

(20)

1. The key pair in PKI is created by
 - a. Registration Authority
 - b. Certification Authority
 - c. User
 - d. Both a & c is possible
2. The following is NOT a type of vulnerability
 - a. Technological
 - b. Configurational
 - c. Mechanisms selection
 - d. Policy
3. Adding security on the application layer adds the additional security feature of
 - a. Integrity
 - b. Authenticity
 - c. Non-repudiation
 - d. Authorization
4. One of the few failures of Microsoft is
 - a. GRE
 - b. ASL
 - c. SSH
 - d. PCT
5. For authentication in IPSec the following layers need to modify
 - a. Network layer only
 - b. Operating systems layer
 - c. Application & network layer
 - d. Transport & network layer
6. The two types of parasitic viruses are
 - a. Companion and Appending
 - b. Cavity and Prepending
 - c. Overwriting & Appending
 - d. Overwriting & Companion

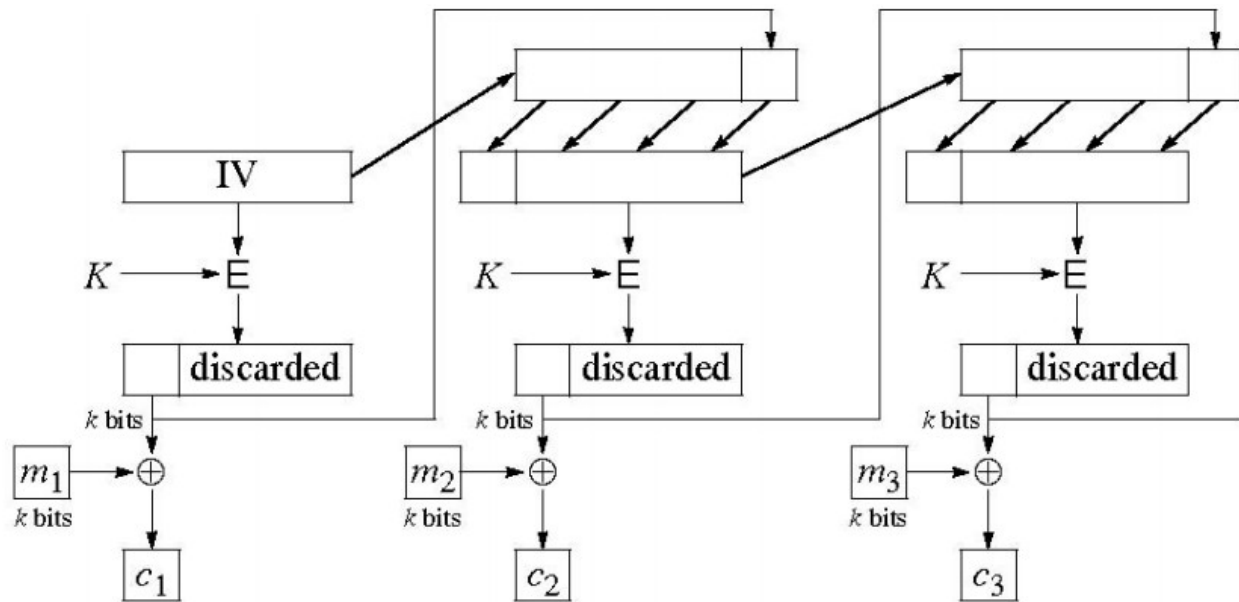
7. Three main ideas of cryptography are
 - a. Confidentiality, Integrity and availability
 - b. Confusion, Diffusion & Permutation
 - c. Kerchoff's law, Permutation & Substitution
 - d. Substitution, Confusion & Diffusion
8. Synchronization is NOT a problem with
 - a. RSA SecurID
 - b. One time token based Passwords
 - c. SoftID
 - d. CryptoCard
9. The following is NOT a problem with biometric authentication
 - a. Intrusive technology
 - b. False acceptance & rejection rate
 - c. High development costs
 - d. Lack of standard API
 - e. None of the above
10. The purpose of the KDC is to
 - a. Create a secure cryptosystem for reducing key exchanging risks
 - b. Enhance integrity measures
 - c. Improve Integrity and availability
 - d. Reinforce centralized authentication systems because they are a better solution

Q 02: Fill the table given below with appropriate values (8 points)

Algorithm	Input bits	Output bits	Key size	Stream/block
E.g. lorem ipsum	168	256	128	Block
IDEA	64	64	128	Block
RC2	64	64	8-1024	Block

RC4	stream	stream	variable	Stream
AES-256	128	128	256	Block

Q 03: With the mode of operation given below, answer the question with reasons in not more than 2 lines each.(15 points)



1. What is the name of this mode of operation?

OFB (output feedback)

2. Identify if it is synchronous / self-synchronous / stream / block cipher & importantly why?

Synchronous stream cipher: key-stream (one-time pad) depends on the IV and the key

3. What does one bit error in transmission results in? Explain your answer.

1-bit error in transmission affects only one bit of plain text

4. Is random access possible? If yes/no, how/why?

Yes, because if you get the OTP, you can decrypt any group of messages

5. If the communicating parties use implicit IV which is generated using a complex proprietary method, what is the effect of a known-plaintext attack?

In this case, only the first group of message will be decrypted since the attacker knows the first IV. For the second group, the IV will change, therefore the attacker will not be able to decrypt the message.

Q 04: a) What are the two main methods of malware analysis? Explain in one line each.(5 points)

1. Static: Code is analyzed without execution
2. Dynamic: Code is executed and its behavior is observed.

b) Three typical use cases:

1. Computer Security incident management
2. Malware research
3. Indicator of compromise extraction

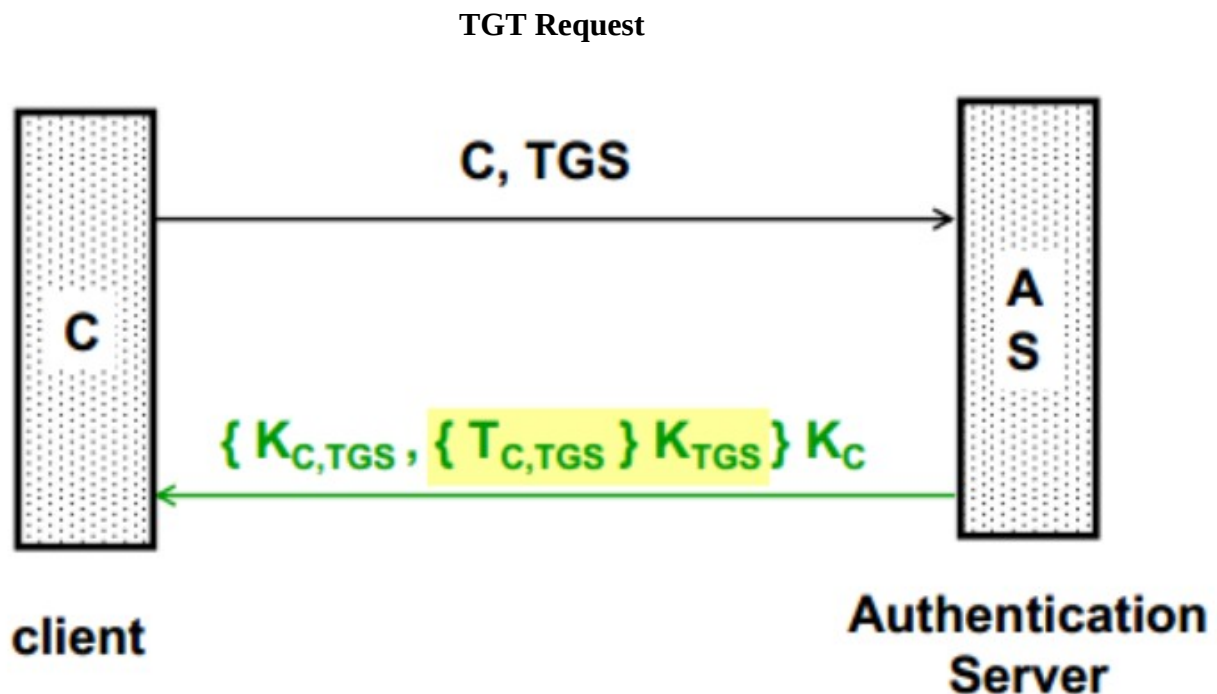
Q 05: With the help of a diagram, show the difference between the tunnel modes of Authentication Header & Encapsulating Security Payload. (8 points)



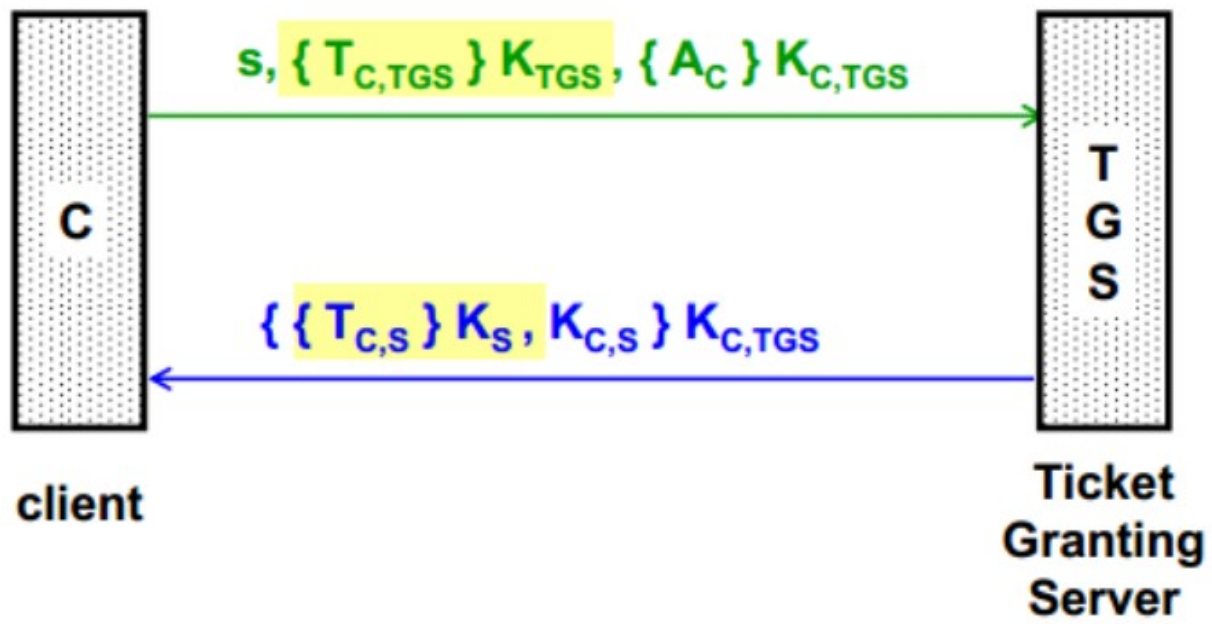
Q 06: During a heated discussion, you got very angry with your friend. Now you want to hack him and take your revenge. Luckily, you are sharing the Black Panther movie with him via bit-torrent. What is an ideal way to infect him with a malware? (6 points)

Using contagion worm, since I have already established a connection with him, I can infect him with malware. Also, I can add malware to the files I am sharing with him.

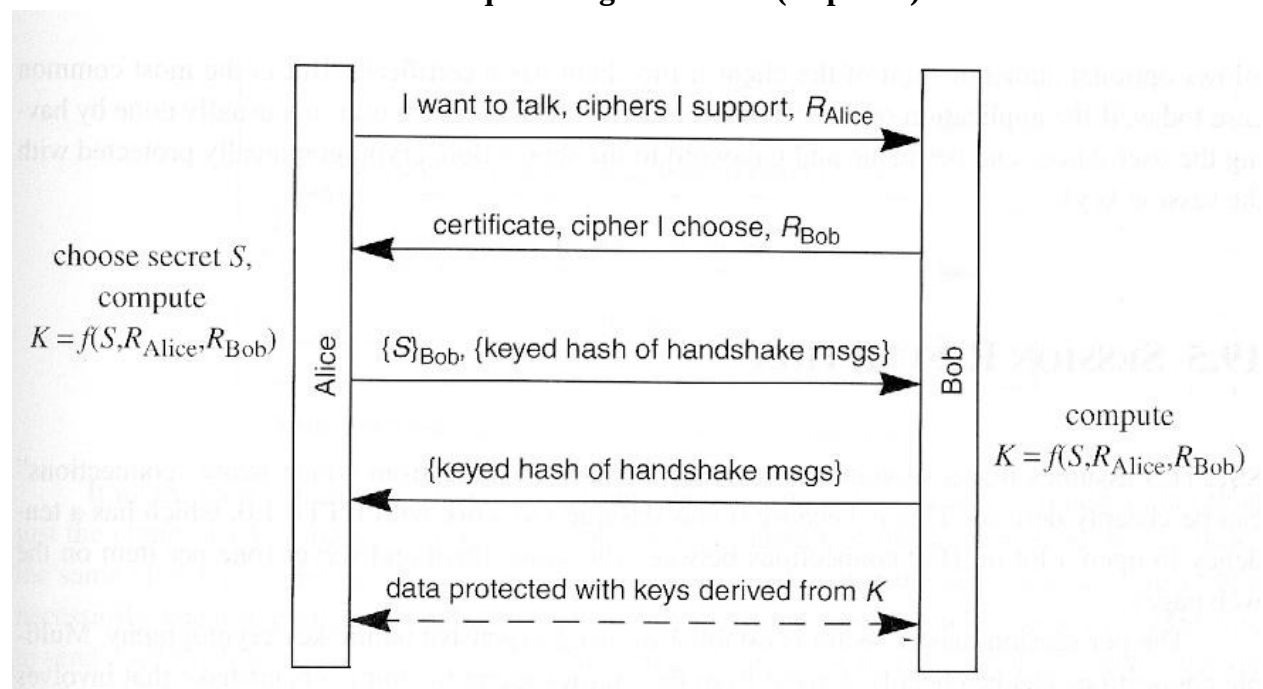
Q 07: Complete the pictorial sketch below by adding appropriate communication messages. (10 points)



Ticket Request



Q 08: The communication given below depicts how Alice and Bob would establish a secure SSL connection. Then answer the question given below. (16 points)



1. How is Bob authenticating Alice? Explain with valid reason(s).

Bob isn't authenticating Alice at all. It's a one way authentication.

- 2. How is Alice & Bob computing the Keyed hash? Using the master key or pre-master key? Any ideas why use a specific one?**

Using the master key. Because master key size is larger and its fixed. It is a standard secure key over which both parties agree after it is derived from pre-master key, random numbers of Alice and Bob.

- 3. What protocol was used in SSL to encapsulate packets from the application layer. Write its four types.**

Record protocol.

- 1. Application data**
 - 2. Change cipher spec protocol**
 - 3. Alert protocol**
 - 4. Handshake protocol**
- 4. Write down the number of keys generated in SSL v2. And v3. How are they created? What are they used for in v2 & v3?**

2 keys in SSL v2. One in each direction. One for integrity one of encryption.

6 keys in v3. One for integrity, as IV, and one for encryption from each side.

In both versions its derived from master keys.