Name:_____ ID:_____

CSE 4057 Information System Security

Fall 2017 Midterm Exam

Duration: 90 minutes

Q1	Q2	Q3	Q4	Q5	SUM
/20	/25	/22	/20	/15	/100

Q-1. (20 pts) Assume there is a Certificate Authority (CA) with a well-known public key. Further assume every user is issued a certificate for his/her public key. Answer the following questions.

(a) (7 pts) Suppose Alice wants to send a very large message M to Bob. Alice does not care about confidentiality, but needs to send M in authenticated way. Describe an efficient method for this using public key cryptography. Please show your work by drawing a diagram.

(b) (5 pts) Assume Bob receives the message sent by Alice. Describe how Bob should process the message.

(c) (8 pts) Suppose Alice wants to send many large messages to Bob and she would not want to sign digital signatures for all the messages. Describe a protocol between Alice and Bob, so that all the messages can be sent in authenticated way. Describe the intiution behind your protocol, and show your idea by drawing a diagram

Name:_____ ID:_____

Q-2. (25 pts) Suppose that we want to implement a simple end-to-end encryption mechanism for our peer-to-peer messaging application MyApp. We have a MyApp server that tracks the users. Each user has a public, private key pair. Private keys are only known by the users and public key is known by the server and any user can obtain these keys when necessary. Answer the following questions:

(a) (6 pts) Describe why a key exchange mechanism is needed for encrypting/decrypting messages between two peers. (Why don't we use just the public keys we obtain from the server?)

(b) (5 pts) Briefly describe a key exchange mechanism by using RSA. (We don't ask RSA encryption details, but +3pts bonus if you describe.)

(c) (5 pts) Briefly describe a key exchange mechanism by using Diffie-Helman (or you may answer for Elliptic Curve DH). (We don't ask DH or ECDH details, but +3pts bonus if you describe.)

(d) (9 pts) Describe how man-in-the middle attack would be applied for both (b) and (c). Show your work by drawing a diagram for each.

Name:_____ ID:_____

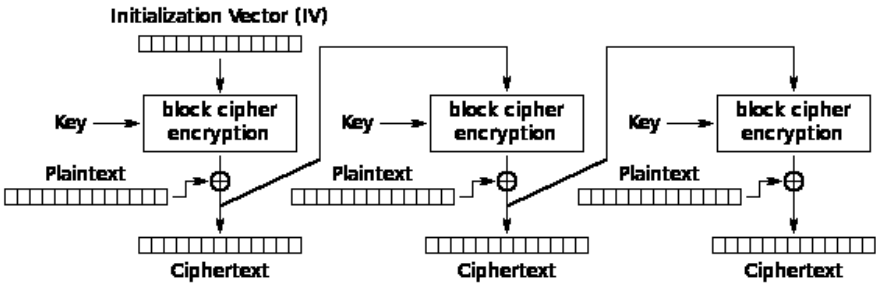
Q-3. (22 pts) Answer the following questions about block ciphers:

(a) (5 pts) DES is not secure. Why?

(b) (5 pts) AES decryption is a bit harder than AES encyption. Why?

(c) (5 pts) What is the reason of using Cipher Block Chaining (CBC) in block ciphers?

(d) (7 pts) Cipher Feedback Mode encryption is given in the following figure. Draw the diagram for decryption.



Cipher Feedback (CFB) mode encryption

Name:_____ ID:_____

Q-4. (5x4=20 pts) Consider the following threats for Web Security and briefly (but concisely) describe how these are addressed in SSL.

(a) Man in the Middle attack – Attacker sends his public key to the client as if it is the public key of the server.

(b) Man in the Middle attack – Attacker intercepts the handshake messages and erase the strong algorithms from the list of algorithms sent by the client.

(c) Replay attack – Earlier SSL handshake messages are re-used.

(d) Truncation attack – Attacker forges TCP connection close segment.

Q-5. (15 pts) Consider a VPN that uses IPSec tunneling mode with Encapsulating Security Payload (ESP). Describe where and how an original datagram is converted to IPSec datagram and how it is converted back to original datagram.