Name:_____ **ID:**_____

CSE 4057 Information System Security

Fall 2017 Final Exam

Duration: 90 minutes

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	SUM
/12	/16	/12	/12	/12	/12	/12	/21	/12	/100

Q-1. (12 pts) Consider that you have already developed an instant messaging mobile application MyApp with end-to-end encryption. You also want to develop a web application MyApp-Web that allows the application users to perform instant messaging on a web browser. Describe a method to implement end-to-end encryption for the messages sent and received using MyApp-Web. You may assume that a user can only use MyApp-Web if his/her mobile phone is also connected to the Internet and running MyApp with his/her credentials.

Q-2. (16 pts) (a – 9 pts) Suppose that Ayşe encrypts a secret image in her PC with AES using key K_S. She wants to store this encrypted image in a public database, and she does not want anybody, except Burak and Ceren, to decrypt this image. Describe a method to achieve this.

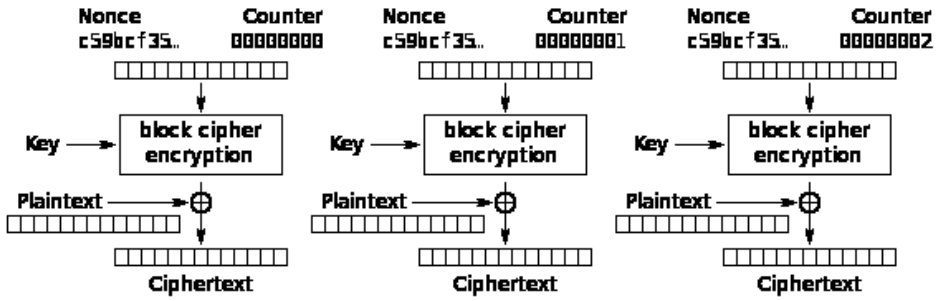
Notes:
- All public keys are securely stored in the database (they are signed by the trusted database owner).
- Public database allows any type of data to be stored.
- Ayşe, Burak and Ceren may not always connected to Internet.

(b – 7 pts) Suppose that Burak and Ceren wants to be sure that the sender of this encryped image is really Ayşe. Describe a method to provide this.

Name:_____ ID:_____

Q-3. (12 pts) What is the most important difference between SHA-1 and SHA-2? Which one would you prefer? Why? Give an example usage of these algorithms.

Q-4. (12 pts) Following figure shows counter (CTR) mode block cipher encryption:



Counter (CTR) mode encryption

Give the name of widely used protocol that uses CTR mode encyption. Briefly discuss a possible reason of chosing this encryption technique (What is an important advantage of CTR mode compared to Cipher Block Chaining (CBC), Cipher Feedback Mode (CFB) or Output Feedback Mode (OFB)?)

Q-5. (12 pts) (a – 4pts) Which encryption algorithm is used by WEP and WPA?

(b – 8 pts) WPA uses same encyption algorithm as WEP (while WPA2 uses a different algorithm). What could be the reason?

Name:_____ ID:_____

Q-6. (12 pts) Consider a stateless firewall protecting a subnet with address 196.222.111/24. This firewall only allows outside users to access internal web server (working at host 196.222.111.12). Other internal hosts are not allowed to perform any communication with the outside world. Fill in the entries of the following filter table.

(Note: HTTP port is 80, client portsa re typically >1023, flag bits are ACK, any or all.)

Action	Source Address	Dest Address	Protocol	Source Port	Dest Port	Flag Bit
Allow						
Allow						
Deny	All	All	All	All	All	All

Q-7. (12 pts) Briefly describe how TOR provides anonymity.

Q-8. (21 pts) (a – 7 pts) Step-by-step describe an example for SQL-Injection attack.

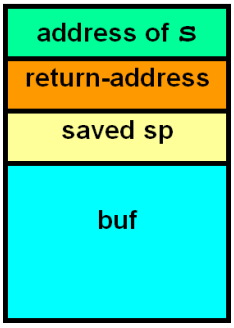
Name:_____ ID:_____

(a – 7 pts) Step-by-step describe an example persistent (stored) XSS attack.

(b – 7 pts) Step-by-step describe an example CSRF attack.

Q-9. (12 pts) Following illustrates a simple function and C stack space when this function is called.

```
void foo(char *s) {
      char buf[100];
      strcpy(buf,s);
      …
```



Briefly describe how buffer overflow attack can be performed to run a malicious small program.