TT#01 Course: Computer, Data & Network Security (**SWE 337**)

Marks: 20 Time: **40 mins**

1. What are the differences between Access Control Metrics and Access Control Lists of Access Control Models? **04**
2. What is Digital Signature? Briefly state the steps in producing digital signatures. **03**
3. Calculate the GCD(2260, 812) using the Euclidean Algorithm. **04**
4. Suppose you are given the following text "dog" and a random matrix K. Now find the cipher text using Hill Cipher. **05**

$$K = \begin{bmatrix} 1 & 2 & 5 \\ 3 & 3 & 4 \\ 2 & 1 & 3 \end{bmatrix}$$

5. Find the unicity distance of the Caesar cipher where the number of keys = 25 and the language is English. **04**

75-52 = 23

176 352 528 704 (636 - 528 = 108)

812 1624 2436

2260 - 1624 = 636

812 - 636 = 176

TT#02 Course: Computer, Data & Network Security (**SWE 337**)

Marks: 20 Time: **40 mins**

1. Suppose a group of people agreed upon a key, K = "PUZZLE". Now find the ciphertext of the plaintext, M = "LITTLE" using Playfair cipher. **- 05**
2. Write a short note on Diffie-Hellman key exchange protocol. **- 03**
3. Why is ECB mode bad with images? Explain in brief. **- 02**

Shahjalal University of Science and Technology
Institute of Information and Communication Technology (IICT)
Software Engineering
3rd Year 2nd Semester Final Examination' Dec 2022 (Session: 2018-19)
Course Code: SWE 337 Credits: 2 Course Title: Computer, Data & Network Security
Time: 2 hrs Total Marks: 50

Group A

[Answer all the questions]

1. Answer any FIVE **5x1=5**

a) What do you understand by the term "Integrity" in the context of Computer Security?

b) Eavesdropping is an active attack? True or False? If false, why?

c) What is Message Authentication Code?

d) What is "Non-Repudiation"?

e) What is digital signature?

f) What is the one time pad?

g) What is the Open Design Principle?

2. Answer any FOUR **4x2.5=10**

a) Differentiate between Authentication and Authorization?

b) Briefly explain the A.A.A concepts in modern computer security.

c) What is Digital Signature? Briefly state the steps in producing digital signatures.

d) Calculate the GCD(226, 12) using the Euclidean Algorithm.

e) Suppose the number of keys for substitution Cipher is 26!. If we partition the plaintext into bigram, what will be the number of keys in the keyspace?

f) Write the disadvantages of substitution cipher.

3. Answer any TWO **2x5=10**

a) What is block cipher? Briefly explain the ECB and CFB mode of block cipher.

b) Suppose you are given the following text "Tom" and a random matrix K. Now find the cipher text using Hill Cipher.

$$K = \begin{bmatrix} 1 & 2 & 5 \\ 3 & 3 & 4 \\ 2 & 1 & 3 \end{bmatrix}$$

c) Suppose Bob wants to send a message, M = 13 to Alice, Both Alice's public key and private key are (33, 3) and (33, 7). Now calculate the ciphertext C and then decrypt it to retrieve the message, M.

10 K
12 L
13 M
14 N
15 O
16 P
17 Q
18 R
19 S
20 T
21 U

Group B

[Answer all the questions]

4. Answer any FIVE **5x1=5**

a) What do you understand by the term "Security by obscurity"?

b) What is Kerckhoffs's Principle for open design?

c) What is "Dictionary attack"?

d) What is SSH?

e) What is Social Engineering attack?

f) What is pretexting?

g) What is the least privilege principle?

5. Answer any FOUR **4x2.5=10**

a) Calculate 5^{31} mod 13 using repeated squaring.

b) Briefly describe some benefits of IPsec.

c) Suppose the number of keys for substitution Cipher is 26!. If we partition the plaintext into trigram, what will be the number of keys in the keyspace?

d) What are the advantages and disadvantages of asymmetric cryptography?

e) How can Man-In-The-Middle attack be mitigated?

f) Briefly state how Digital Certificate works.

6. Answer any TWO **2x5=10**

a) Dexter wants to set up his own public and private keys. He chooses p = 23 and q = 19 with e = 283. Find d so that ed has a remainder of 1 when divided by (p − 1)(q − 1). **5**

b) Suppose Nazia chose a prime number, p = 7 and a generator g = 3. She will use Elgamal Cryptosystem for encryption and decryption.

i) Find the public key and private key for Nazia. **2**

ii) If Munif wants to send a message, M = 7, to Nazia, what will be the ciphertext of Munif? **3**

c) Suppose Alice chose a prime number, p = 7 and a generator g = 3. She will use Elgamal Cryptosystem for encryption and decryption.

i) Find the public key and private key for Alice. **2**

ii) If Bob wants to send a message, M = 13, to Alice, what will be the ciphertext of Bob? **3**

© K = "ASGARD" plaintext, M = "GROOT" playfair cipher

Shahjalal University of Science and Technology
Institute of Information and Communication Technology
Software Engineering
Term Test 1

Course Code: SWE 337 Credits: 2 Course Title: Computer, Data and Network Security
Time: 1 hr Total Marks: 20

a)	What do you understand by Data Confidentiality? What are the necessary steps to take to make your data confidential?	5
b)	Suppose Sara wants to send a message to Henderson only. Write the steps so that Henderson can be sure of the fact that the message came from Sara and nobody else. What is this technology called?	5
c)	Suppose we are using 8-bit ascii encoding. Now each English alphabet is estimated to carry 1.25 bits of information. Calculate the probability that a randomly selected sequence of 32 bits is a meaningful text message.	7
d)	A computer can test a password in every nanosecond. How much time will it take for an attacker to crack the password of length 8. (The password may consist of any of the 128 ascii characters)	3

Shahjalal University of Science and Technology
Institute of Information and Communication Technology
Software Engineering
Term Test 2

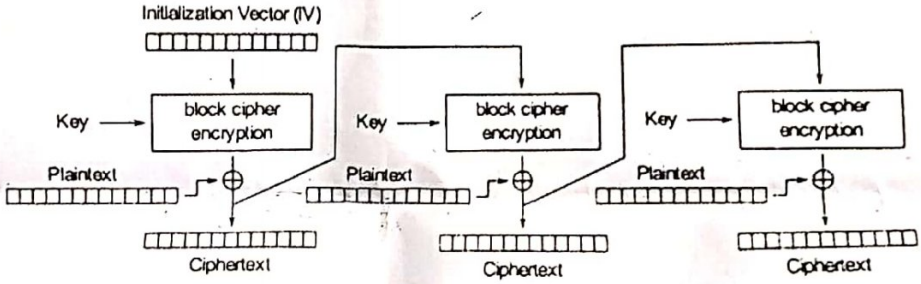
Course Code: SWE 337 **Credits: 2** **Course Title: Computer, Data and Network Security**
Time: 45 Minutes Total Marks: 20

1. Encrypt the text "CAB BCC ACC B" using Block Cipher with padding where
   m = 3;
   $k = \begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix}$;

   For the first block $\vec{x} = \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}$

   And for the last block $\vec{x} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$

   Hints: The last block will become B22 after padding. And you may assume that there are at most 4 characters in the entire character set. **Marks: 10**
2. Can you identify any problem with the above mechanism? How can you improve the above mechanism? (Not more than 3 lines/points) **Marks: 2**
3. Write the problems with ECB mode of Block Cipher. (Not more than 3 lines/points) **Marks: 2**
4. What would be the problem of the following Block Cipher architecture and why? Write within 6 lines/points. **Marks: 6**



Cipher Feedback (CFB) mode encryption

5 mod 25

25)5(

44
25
19

Shahjalal University of Science and Technology
Institute of Information and Communication Technology

B.Sc. (Engg.) in Software Engineering
3rd Year 2nd Semester Final Examination, 2019
Session: 2016-17

Course No.: SWE 337 **Course Title: Computer, Data and Network Security**
Credits: 2 **Time: 2 hrs** **Total Marks: 50**

Group A
[Answer all the questions]

1. Answer any FIVE. **5x1=5**

a) What is the role of a Certificate Authority?
b) Write the full form of AES.
c) Why are public keys used?
d) Why is padding used in encryption?
e) Write the four modes of block cipher.
f) Vigenère cipher uses a key that is as long as the plain text. Is it True or False?

2. Answer any FOUR. **4x2.5=10**

a) What is Fail Safe Default? Give a practical example of a popular system that violates this principle.
b) A computer can test a password in every nanosecond. How much time will it take for an attacker to crack the password of length 10 (the password may consist of any of the 128 ASCII characters)?
c) Describe how a Brute Force attack happens.
d) What is the difference between an Encryption Algorithm and a Hashing Algorithm?
e) What is a Social Engineering Attack?

3. Answer any TWO. **2x5=10**

a) What do you understand by Data Confidentiality? Describe the steps to achieve Data Confidentiality.
b) Between CFB and OFB which one has a better encryption architecture? Why?
c) Suppose we have a network of 2300 users. They want to communicate in a secretive manner.
   i. How many keys are required if we use a Symmetric Key Cryptosystem?
   ii. How many key pairs are required if we use an Asymmetric Key Cryptosystem?

[Answer all the questions]

4. **Answer any FIVE.** 5x1=5

a) In CBC mode we can take advantage of pre computed IV. Is it True or False? If false give correct answer.

b) What is a "Quid pro quo" attack?

c) Write 3 components of a Crypto System.

d) "Brute-force decryption is likely to succeed for messages in natural language that are not too short". Is it True or false? If false give correct answer.

e) Why are RAIDs used?

f) What is cryptanalysis?

5. **Answer any FOUR.** 4x2.5=10

a) How can you fulfill availability triad of a security system? Can you give an example?

b) Describe Man In The Middle attack.

c) The AA Corporation has a new refrigerator, the Fridge, which has a camera that takes a picture of the contents of the refrigerator and uploads it to the AA Corporation's web site. The Fridge's owner can then access this web site to see what is inside their refrigerator without opening the door. For security reasons, the AA Corporation encrypts this picture and gives a 4-digit PIN to decrypt this picture to the Fridge's owner, so he or she can get access to the pictures of their Fridge's interior. Suppose you have been hired as a security expert to find holes in the system. How will you test the system?

d) Suppose we are using ASCII encoding. Now each English alphabet is estimated to carry 1.25 bits of information. Calculate the probability that a randomly selected sequence of 32 bits is a meaningful text message.

e) What are the problems of security questions in password reset systems? Can you give a real life example of a hacking that was performed based on this?

6. **Answer any TWO.** 2x5=10

a) How can Message Authentication Codes be used to ensure Data Integrity? Describe.

b) Encrypt the text "CBB BAC ABC B" using Block Cipher with padding where m = 3;

$$k = \begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix};$$

For the first block $\vec{x} = \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}$

And for the last block $\vec{x} = \begin{bmatrix} 1 \\ 3 \\ 3 \end{bmatrix}$ B22

Hints: The last block will become ~~B22~~ 33 after padding and you may assume that there are at most 4 characters in the entire character set.

c) Suppose Rupa wants to send a secret message to Emma. There is possibility of eavesdropping. Now propose a mechanism that will ensure both Confidentiality and Integrity of the data. What is this technology called? There needs to be way so that Emma can be assuring of the fact that the message came from ~~Kamal~~ Rupa only and nobody else.