Department of Computer Science and Engineering
University of Chittagong
7^{TH} Semester BSc (Engg.) Examination 2021
CSE 717: INFORMATION SECURITY
Marks: 52.5 Time: 4 hours

[Using section-wise separate answer scripts, answer any three questions from each of the following two sections and all the parts of a question chronologically.]

SECTION A

A-1/ (a) Derive a risk equation depending on threat agent, probability of attack, and expected loss. Draw a related model. 4.75

(b) How do physical and behavioral bio-metrics fail for authentication? How would you evaluate bio-metrics authentication using standard criteria? 3

(c) Remark on the threats in wireless networks. 1

A-2/ (a) i. The one-time pad offers complete security – do you agree on this? Defend your answer. 2.75

ii. What are the fundamental difficulties of one-time pad? 2

(b) Using following Playfair matrix:

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

Encrypt the message: **See you at CSE department** 4

A-3/ (a) i. Calculating $\mathbf{3^{11} \bmod 17 = X}$ is easy, but calculating discrete logarithm $\mathbf{11 = 3^X \bmod 17}$ is very difficult. Explain above statement. 2.75

ii. Using the extended Euclidean algorithm, find the multiplicative inverse of $\mathbf{1234 \bmod 4321}$. 2

(b) i. Using **Fermat**'s theorem, find $\mathbf{3^{201} \bmod 11}$ 2

ii. Use **Euler**'s theorem to find a number x between 0 and 28 with x^{85} congruent to 6 *modulo* 35. 2

A-4/ (a) i. For DES, explain the following equation. At the end of the decryption process, we have to reverse the initial permutation:

$$IP^{-1}(R_{16}^d,\ L_{16}^d) = IP^{-1}(L_0,\ R_0) = IP^{-1}(IP(x)) = x$$

where x is the plain text that was the input to the DES encryption. 2.75

ii. Draw a block diagram of 3-DES. Also, write down a simple equation to represent subsequent DES encryption for 3- DES. 2

(b) i. What do you understand by avalanche effect? Write down two families of attacks in DES. 2

ii. Write a program that can encrypt and decrypt using the general Caesar cipher. 2

SECTION B

B-1/ (a) Draw the Advanced Encryption Standard (AES) encryption block diagram. 4.75

(b) i. Discuss the following properties for cryptographic hash function: *Pre-image resistance*, *Second pre-image resistance*, *Collision resistance*. 2

ii. How can you achieve authentication encryption? 2

B-2/ (a) Perform encryption and decryption using the RSA algorithm, for $p = 3$, $q = 11$, $e = 7$, $M = 2$. The value of n and chiper-text must be explicitly shown. 2.75

(b) Explain the six steps of Kerberos authentication scheme with appropriate diagram. 2.5

(c) Draw the generic model of digital signature process. 2

(d) State secure hash function requirements. 1.5

B-3/ (a) i. How is the blockchain related with cryptography? 2.75

ii. What do you understand about bitcoin? 2

(b) Discuss the process of input-output scripts for signature validation for bitcoin. 4

B-4/ (a) How would you differ between ransomware and social engineering? 2

(b) Discuss the application areas of IPSec. Compare session state and connection state. 2.5

(c) Explain the architecture of IPSec. 2.5

(d) Describe Backdoor, logic bomb, and Trojan horse. 1.75

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
UNIVERSITY CHITTAGONG

7TH SEMESTER BSC ENGINEERING EXAMINATION
CSE 717 (*Information Security*) MARKS: 54 TIME:

Using section-wise separate answer-scripts, answer any three of the four questions from each of the following two sections. Keep handwriting legible.

SECTION A

Question 1: 2+3+3+1 marks

(a) *Ambiguity is security's enemy* – why and how?

(b) Fill in the blanks marked A, B and C in the following with appropriate information/computer security terms, before explaining them in brief:

Consider a simple security policy for a house. No one is allowed in the house unless accompanied by a family member, and only family members are authorized to remove physical objects from the house. An unaccompanied stranger in the house is a security violation. An unlocked back door is a .....(A)..... A stranger entering through such a door, and removing a television, amounts to .....(B)..... The attack vector is entry through the unlocked door. A .....(C).....here is the existence of an individual motivated to profit by stealing an asset and selling it for cash.

(c) Write down key roles and responsibilities with the following professions in information/computer security:

- Penetration tester
- Cyber security analyst
- Data security analyst
- Network analyst
- Cyber security auditor
- Cyber security architect

(d) What is steganography?

Question 2: 3+3+3 marks

(a) What are the essential ingredients of a symmetric cipher? What is the difference between a block cipher and a stream cipher?

(b) Explain how cryptanalysis can possibly work for *Caesar cipher* and *one time pad*.

(c) What are the principal elements of a public-key cryptosystem? What are the roles of the public and the private key?

Question 3: 3+2+4 marks

(a) Outline in general terms an efficient procedure for picking a prime number. The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How can such an algorithm be used to test for primality?

(b) Calculating $3^{11} \bmod 17 = X$ is easy, but calculating discrete logarithm $11 = 3^X \bmod 17$ is very difficult — explain.

(c) Using Fermat's theorem, find $2^{202} \bmod 5$.

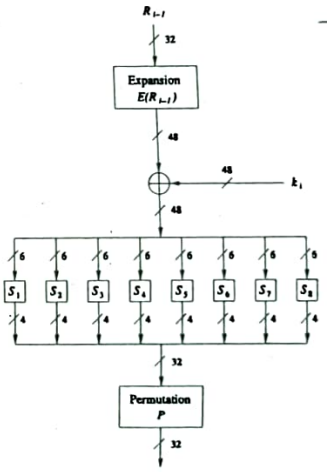
And employ Euler's theorem to find a number X, $0 \leq X \leq 9$, such that X is congruent to 5^{1000} modulo 10.

Question 4: 2+3+4 marks

(a) Why did IBM include the concept of S-box in Data Encryption Standard (DES)? What is the S_1-box representation of 37. [The value given at row 3 and col 2 at S_1 table is 08]

(b) Draw a schematic diagram for 3-DES. Derive an encryption equation for 3-DES, where input text is X and the cipher text is Y.

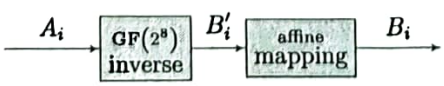
(c) Give a short description of the components of the *f-function* in DES as depicted in the following figure.



SECTION B

Question 5: 4.5+4.5 marks

(a) Describe the two Operations as shown in the following figure



within the Advanced Encryption Standard (AES) S-Box which computes the function $B_i = S(A_i)$. Assume that the S-Box input $A_i = (11000010)_2 = (C2)_{hex}$.

Multiplicative inverse table in $GF(2^8)$ for bytes xy used within the AES box S-Box is as given.

X \ Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
1	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
2	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
3	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
4	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	B9	09
5	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
6	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
7	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
8	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
9	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
A	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
B	0C	E0	1F	EF	11	75	78	71	A5	BE	76	3D	BD	BC	86	57
C	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
D	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
E	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
F	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

(b) Sketch and explain the generic model of the *digital signature process.*

Question 6: (3+2+2)+2 marks

(a) Using RSA, encrypt the message $M = 3$, assuming the two primes chosen to generate the keys are $p = 13$ and $q = 7$. You should choose a value $e < 10$. Show your calculations and assumptions.
If Alice used the RSA algorithm in sending the above message $M = 3$ to Bob so that Charlie could not read the message, then what are Alice's and Bob's public keys? Assuming a brute force attack is not possible, explain the steps that Charlie could take to break the encrypted message. (You do not need to perform the calculations, you just need to point out what Charlie needs to calculate and why).
(b) What are the properties a digital signature should have? What requirements should a digital signature scheme satisfy?

Question 7: 2+3+4 marks

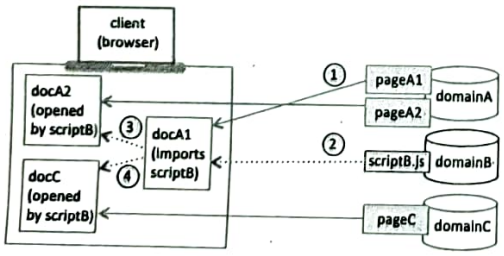
(a) In what order should the signature function and the confidentiality function be applied to a message, and why? What are some threats associated with a direct digital signature scheme?
(b) Write short notes on: SQL *injection* and *social engineering*.
(c) SWIFT is a worldwide network used by banks to send each other financial transaction information. Consumers and businesses do not connect directly to SWIFT, only financial institutions can. It has been abused in the last decade, malicious hackers tried to use it to steal US$1 billion from a central bank.
Ars Technica, a major tech magazine, wrote:

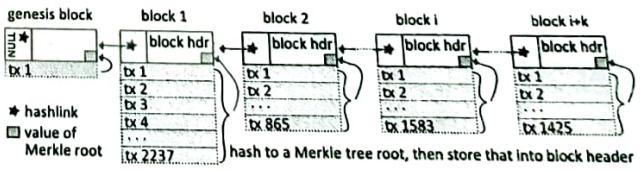
> SWIFT's security stems from two major sources. Notionally, it's a private network, and most banks set up their accounts such that only certain transactions between particular parties are permitted. The network privacy means that it should be hard for someone outside a bank to attack the network, but if a malicious hacker breaks into a bank – as was the case here – then that protection evaporates. The central bank involved has all the necessary SWIFT software and authorized access to the SWIFT network. Any malicious hacker running code within the that central bank also has access to the software and network.

i. You've been hired to do a penetration test of some bank's SWIFT gateway. What should your goal be? That is, what concrete, verifiable result would prove that you had successfully hacked your client's SWIFT gateway.
ii. You of course do not want to damage the SWIFT gateway in any way, and especially not do anything that would leave it open to other attackers. What steps would you take to ensure that there was no damage?

Question 8: 4+4+1 marks

(a) Explain the *same-origin* policy, preferably using of a full blockchain is given below.
following schematic as an illustrative example.





(b) How is data integrity checked in blockchain? A depiction

(c) How do you distinguish between Ethereum's currency *ether* (ETH) and *bitcoin*?

University of Chittagong
Department of Computer Science and Engineering
7th Semester B.Sc. (Engg.) Examination-2020
Course Code: CSE-717 Course Title: Information Security
Total marks: 52.5 Marks Time: 4.00 hours

[Answer any ***three*** questions from each of the ***Group-A*** and ***Group-B***. A separate answer script must be used for Group-A and Group-B. Figures in the right-hand margin indicate full marks.]

Group-A

1. a) Using the following Playfair matrix: 4.75

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

Encrypt this message: "*Must see you over CU playground. Coming now.*"

b) Using the Vigenère cipher, encrypt the word "*explanation*" using the key *cse*. 4

2. a) Solve the following congruences using the Chinese remainder theorem. 4.75

$$X \equiv 1 \bmod 3$$
$$X \equiv 1 \bmod 4$$
$$X \equiv 1 \bmod 5$$
$$X \equiv 1 \bmod 7$$

b) (i) Calculating $3^{11} \bmod 17 = X$ is easy, but calculating discrete logarithm $11 = 3^x \bmod 17$ is very difficult. Explain the above statement. In this aspect, what do you understand by the cyclic group? 2+2

(ii) Find out the distinct remainders for $b^x \bmod 7$.

3. a) Using the extended Euclidean algorithm, find the multiplicative inverse of 550 mod 1769. 4.75

b) (i) Using Fermat's theorem, find $3^{202} \bmod 11$. 2+2

(ii) Use Euler's theorem to find a number a between 0 and 9 such that a is congruent to 7^{1000} modulo 10.

4. a) (i) The following questions are related to data encryption standards: If initial permutation (IP) is there, why do we need IP^{-1}? What is the S_1-box representation of 37? [The value given at row 3 and col 2 at S_1 table is 08] 2+2.75

(ii) Draw the details of the F-function in DES.

b) (i) For DES, explain the following equation. 2+2

At the end of the decryption process

$$IP^{-1}(R^{d}_{16}, L^{d}_{16}) = IP^{-1}(L_0, R_0) = IP^{-1}(IP(x)) = x$$

Where x is the plain text that was the input to the DES encryption.

(ii) How the concept of the finite field are used in cryptography?

Group-B

5. a) (i) Draw a block diagram of 3-DES. Write down a simple equation to represent DES encryption for 3-DES. 2.75+2

(ii) What do understand by the avalanche effect? Write down two families of attacks in DES.

b) Draw the classical Feistel cipher structure for the symmetric block encryption algorithm. 3

c) What are the differences between a block cipher and a stream cipher? 1

6. a) Perform encryption and decryption using the RSA algorithm, for $p = 3$, $q = 11$, $e = 7$, and $M = 2$. (The value of n and cipher-text must be explicitly shown.) 4.75

b) (i) In an RSA system, the public key of a given user is $e = 31$, $n = 3599$. What is the private key of this user? 2+2

(ii) In the RSA public-key encryption scheme, each user has a public key, e, and a private key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?

7. a) Draw the generic model of the digital signature process. 4.75

b) Find out the 8-bit word related to $x^5 + x^2 + x$. 2

c) How would you test a number $n = 29$ is a prime or not using the Miller-Rabin algorithm? Show the steps clearly. 2

8. a) Determine the benefits of IPSec. What are the differences between transport mode and tunnel mode? 2.25

b) What are the general services defined by RFC4301 for IPSec? 2.25

c) Discuss the application areas of IPSec. Compare session state and connection state. 2.25

d) Explain the architecture of IPSec. 2