SEAT NO. _____

NED UNIVERSITY OF ENGINEERING & TECHNOLOGY

FINAL YEAR(BACHELOR OF SCIENCE IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY)
FALL SEMESTER EXAMINATIONS 2022
BATCH 2019

Time: 3 Hours **Dated:10-02-2023**
Max.Marks:60

Network & Information Security - CT-460

Instructions: Attempt all questions. Each question carries equal marks.

Q.1(a) Explain the broad level steps involved in the Data Encryption Standard (DES). Discuss expansion permutation and S-Box substitution process with respect to DES. Apply the given S-BOX 4 on a given 6-bit number (100110) and find out the corresponding 4-bit number. [C3] **(06)**

	0	1	2	3
0	7	13	14	3
1	13	8	11	5
2	10	6	9	0
	3	15	0	6

0	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S-Box 4

(b) A firewall is usually a combination of packet filters and application (or circuit) gateways, define both the types of firewall. Also discuss the following configuration of firewall: [C1] **(06)**

[i] Single-Homed Bastion
[ii] Dual-Homed Bastion
[iii] Screened Subnet Firewall

Q.2(a) Shaheer is reading a mystery book involving cryptography. In one part of the book the author gives a cipher text "CIW" and two paragraphs later the author tells the reader that this is a shift cipher and the plain text is "yes". In the next chapter, the hero found a tablet in a cave with "XVIEWYVI" engraved on it. Find the secret message. [C1] **(06)**

(b) Write down all the steps involved in generating the MD5 fingerprint and also show the number of padding bits and number of blocks generated if the length of the input message is 4000 bits. [C1] **(06)**

Q.3(a) Encrypt the plaintext: "Common sense is not so common!" by applying the affine cipher with Key (5,22). Given that the finite set of alphabet is" ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789". [C3] **(06)**

(b) Develop a scenario and implement Man in the Middle (MIMT) attack in the Diffie-Hellman key exchange method. Suppose (g=7, n=23, x=3 and y=5) and find out the values of the following by using the Diffie-Hellman algorithm. [C3] **(06)**

[i] What is the value of Symmetric Key?
[ii] What are the values of 'A' and 'B'?

Q.4(a) Why do we use Digital Certificates and what are the significance of the digital signature? How Digital certificate be verified? Explain each step with the help of block diagram. How the Registration Authority (RA) would verify the Proof of Possession (POP) of key pair. [C1] **(06)**

(b) Why are the chaining algorithms being used? Explain the following chaining algorithms. [C1] **(06)**

[i] Cipher Block Chaining (CBC)
[ii] Cipher Feed Back (CFB)
[iii] Output Feed Back (OFB)
[iv] Electronic Code Book (ECB)

Q.5(a) Write down all the steps involved in RSA Algorithm to generate the Public and Private Key pair. Consider a plain text alphabet "H". Using the RSA algorithm and the values as E=3, D=11 and N=15, solve and verify the generated cipher text. [C3] **(06)**

(b) How many tuples are used in Cryptosystems? Discuss each tuple with the help of an example. Two people ALICE and BOB want to communicate over an insecure channel like telephone line or computer network in such a way that OSCAR (Hacker) cannot understand what is being said. Discuss principles of security with respect to the above mentioned scenario. [C1] **(06)**

********** * **********