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.

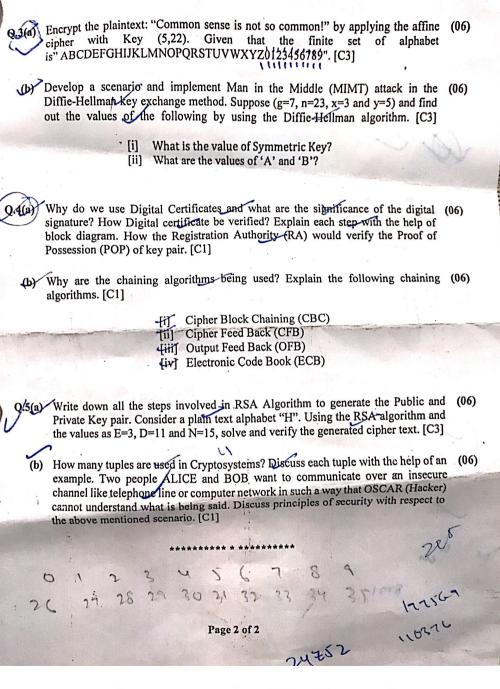
Explain the broad level steps involved in the Data Encryption Standard (DES). (06)Discuss expansion permutation and S-Box substitution process with respect to DES. Apply the given S-BOX 4 on a given 6-bit number (100110) and find out the corresponding 4-bit number, [C3]

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

S-Box 4

- A firewall is usually a combination of packet filters and application (or circuit) (06) gateways, define both the types of firewall. Also discuss the following configuration of firewall: [C1]
 - Single-Homed Bastion
 - **Dual-Homed Bastion**
 - Screened Subnet Firewall [iii]
- 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]
 - 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]

Scanned with CamScanner



Scanned with CamScanner