COMSATS University Islamabad
Sahiwal Campus
(Department of Computer Science)

Course Title:	Information Security			**Course Code:**	CSC432	**Credit Hours:**	03
Course Instructor:	Dr. Khalid Mahmood			**Programme Name:**	CS		
Semester:	7th	**Batch:**	**Section:** A,B		**Date:**	04-12-2020	
Time Allowed:	90 Minutes			**Maximum Marks:**	20		
Student's Name:				**Reg. No.**	CUI/ /SWL		

Important Instructions / Guidelines:

Read the question paper carefully and answer the questions according to their statements.
Mobile phones are not allowed. Calculators must not have any data/equations etc. in their memory.

2nd Sessional Examination FALL-20

Q.1: The following shows the reminders of powers of 10 when divided by 13. We can prove that the pattern will be repeated for higher powers:

$10^0 \bmod 13 = 1$ $\quad$ $10^1 \bmod 13 = -3$ $\quad$ $10^2 \bmod 13 = -4$

$10^3 \bmod 13 = -1$ $\quad$ $10^4 \bmod 13 = 3$ $\quad$ $10^5 \bmod 13 = 4$

Use the above information, find the reminder of an integer when divided by 13. Test your method with 631453672.

Q.2: Alice and Bob have decided to ignore Kirchhoff's principle and hide the type of the cipher they are using:

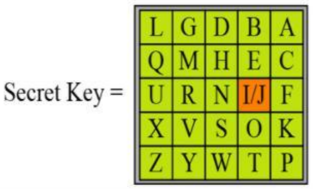
a) How can Eve decide whether a substitution or a transposition cipher was used?
b) If Eve knows that the cipher is a substitution cipher, how can she decide whether it was an additive, multiplicative, or affine cipher?
c) If Eve knows that the cipher is a transposition, how can she find the size of the section (m)?

Q.3: **(a)** The plaintext "letusmeetnow" and the corresponding ciphertext "HBCDFNOPIKLB" are given. You know that the algorithm is a Hill cipher, but you don't know the size of the key. Find the key matrix

(b) John is reading a mystery book involving cryptography. In one part of the hook, the author gives a ciphertext "CIW" and two paragraphs later the author tells the reader that this is a shift cipher and the plaintext is "yes". In the next chapter, the hero found a tablet in a cave with "XVIEWYWI" engraved on it. John immediately found the actual meaning of the ciphertext. What type of attack did John launch here? What is the plaintext"?

Q4: Encrypt the message "The house is being sold tonight" using the following ciphers. Ignore the space between words:

a) Vigenere cipher with key: dollars;
b) Autokey cipher with key =7;
c) Playfair cipher with key created in the text (see Figure 1)



Secret Key =

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

Figure 1