

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

VASAVI COLLEGE OF ENGINEERING (Autonomous), HYDERABAD
B.E. (CBCS) IV-Semester Main Examinations, May-2019

Basics of Cryptology
 (Open Elective-II)

Time: 2 hours

Max. Marks: 40

Note: Answer ALL questions in Part-A and any FIVE from Part-B

Q.No.	Stem of the question	M	L	CO	PO
Part-A (5 × 2 = 10 Marks)					
1.	Define i) Cryptography ii) Cryptanalysis	2	1	1	1
2.	Write the formula to find the multiplicative inverse of a modulo m and hence find the inverse of 7 under mod 31.	2	3	1	1
3.	Define Polyalphabetic Substitution Ciphers.	2	1	2	1
4.	Write the steps involved in Enciphering the plain text using Permutation Cipher.	2	1	2	1
5.	Define i) Enciphering and ii) Deciphering.	2	1	1	1
Part-B (5 × 6 = 30 Marks)					
6. a)	Define i) Cipher ii) Cipher text.	2	1	1	1
b)	Using the Caesar (Additive) transformation $C = P + 3 \pmod{26}$, encipher the message "THIS MESSAGE IS TOP SECRET" with key as 9.	4	3	1	1
7. a)	Let $C(x) = ax + b \pmod{26}$ is an affine transformation. Derive the inverse relationship of the given transformation.	2	2	1	1
b)	Encipher the Plain text RIGHT CHOICE using the Affine transformation $C = 15P + 14$.	4	3	1	1
8. a)	What is meant by Monoalphabetic Substitution Cipher?	2	1	1	1
b)	Encipher the Plaint text SEND THE OTP , using the Multiplicative Cipher with key as 5.	4	3	1	1
9. a)	Distinguish between Hill Digraph Cipher and Hill Trigraph Cipher.	2	1	2	1
b)	Decipher the Cipher text XOIK , which was Enciphered with the key matrix $A = \begin{bmatrix} 9 & 5 \\ 2 & 11 \end{bmatrix}$, using Hill Digraph Cipher.	4	3	2	1
10. a)	Explain Exponentiation Cipher	2	1	2	1
b)	Encipher the Plain text THIS IS AN EXAMPLE using Exponentiation Cipher with $p=2633$ and $e = 29$.	4	3	2	1

11. a) Explain Vigenère Cipher with an example.	2	1	2	1
b) Encipher the plain text DO NOT CLICK THIS LINK, using the Vigenere Cipher with the key as KEYWORD.	4	3	2	1
12. a) If a message is enciphered by Affine cipher then what are the number of possibilities to decipher?	2	1	1	1
b) Write about Public key Cryptography.	4	2	2	1

M: Marks; L: Bloom's Taxonomy Level; CO: Course Outcome; PO: Programme Outcome

S. No.	Criteria for questions	Percentage
1	Fundamental knowledge (Level-1 & 2)	50
2	Knowledge on application and analysis (Level-3 & 4)	50
3	*Critical thinking and ability to design (Level-5 & 6) (*wherever applicable)	00

~~~~~