Question Paper

Exam Date & Time: 29-Nov-2023 (10:00 AM - 01:00 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

Manipal School of Information Sciences (MSIS), Manipal
First Semester Master of Engineering - ME (Cyber Security) Degree Examination - November / December 2023

Cryptology [CYS 5101]

Marks: 100 **Duration: 180 mins.**

Wednesday, November 29, 2023

Answer all the questions.

1) Classify the different categories of Cryptographic Attacks. (CO1)(BL3) (10 Marks) (10)

2) (10)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Explain the working of affine cipher. (CO2)(BL5) (5 Marks)

Consider the expression for affine cipher:
*-e(x) = ax + b mod 26*with *a* and *b* unknown,
You perform a chosen plaintext attack using *'hahaha'*. The ciphertext is *'LOLOLO'*.
Determine the encryption function. (CO2)(BL5) (5 Marks)

3) Explain the working of Playfair Cipher and apply encryption to any plaintext using PLAYFAIR as keyword. (CO2)(BL3) (10 Marks) (10)

4) Briefly explain the working of VIGENERE Cipher with an example. (CO2) (BL4) (10 Marks) (10)

5) Explain the use and application of RC4 Cipher with a use case example (CO2)(BL4) (5 Marks) (5)

6) Illustrate the steps involved in RSA algorithm with an example. (CO3)(BL3) (10 Marks) (10)

7) Briefly explain the AES transformation functions. (CO2)(BL2) (15 Marks) (15)

8) What is MD5 algorithm? Discuss its application, benefits and drawbacks in Cyber Security. (CO3)(BL2) (10 Marks) (10)

9) What is Post Quantum Cryptography? Differentiate between Quantum and Post Quantum Cryptography. (CO5)(BL4) (2+8 Marks) (10)

10) Illustrate why asymmetric key cryptography is called as public key cryptography. (CO4)(BL3) (10 Marks) (10)

-----End-----