Question Paper

Exam Date & Time: 19-Apr-2018 (10:00 AM - 01:00 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

SCHOOL OF INFORMATION SCIENCES (SOIS)
SECOND SEMESTER Master of Engineering - ME (Embedded & Wireless Technology)
DEGREE EXAMINATION - APRIL 2018
Thursday, 19 April 2018
Time : 10:00 am to 1:00 pm
Cryptography and Network Security [EWT 616]

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

Answer all the questions.

1) Explain the four categories of security threats with neat diagram (10)
a. Interruption b. Interception
c. Modification d. Fabrication

2) What is the difference between polyalphabetic cipher and Monoalphabetic cipher with an example? (10)

3) Recognize the following modes of encryption for block ciphers based on their mathematical expressions and explain the mode of operation with neat block diagram. (10)

a. Ci = Ek(Ci-1 _ Pi)
b. Ci = Ek(i) _ Pi

Notation:
Pi is the i-th block of plaintext
Ci of ciphertext,
Ek() is the block cipher encryption function
and _ denotes the XOR function

4) Compare block cipher and stream cipher with the following criteria (10)
* Basic principles
* Speed
* Error
* Pros and cons of each method

5) Explain linear random number generator with an example. (10)

	Compare true and random number no generator.[10 Marks]	
6)	Alice and Bob will use Diffie-Hellman to compute a shared secret. They select p=57 and g=2. Alice picks a kAlice of 11 and Bob picks kbob of 7. a. Show the computations performed by Alice and Bob to calculate a shared secret. b. What values are hidden? c. What values can be sent over an insecure channel.	(10)
7)	Define the term a. Trap door b. Avalanche effect c. Integrity d. Diffusion	(10)
8)	Explain how Asymmetric key encryption and hashing is used for message authentication with relevant diagrams.	(10)
9)	What is Hashing? Explain the properties of Hashing. Differentiate between strong collision and weak collision.	(10)
10)	Explain DoS and DDos attack.	(10)

-----End-----