NED UNIVERSITY OF ENGINEERING & TECHNOLOGY

FINAL YEAR FALL SEMESTER (SOFTWARE ENGINEERING)
EXAMINATIONS 2017-18
BATCH 2014-2015

Time: 3 Hours

Dated:16-03-2018
Max.Marks:60

Network & Information Security - CT-460

Note: Attempt any five questions. All questions carry equal marks.

Question: 1

a) Encrypt using the Auto Key Cipher scheme. [4]
Key = HUAWEI Plaintext = STOP MOVING EVERYONE

b) Encrypt and decrypt the message 'OVER' using the Hill cipher with the key $\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$. Show your calculations with result. [4]

c) Explain the following: [4]
(1) Confidentiality (2) Avalanche Effect (3) Confusion and Diffusion (4) Integrity

Question: 2

a) Explain the encryption and decryption processes of Feistel Cipher. [4]

b) Demonstrate the three-bit Ideal Block Cipher scheme. Discuss the security strength and key space problem in general Ideal Block Cipher scheme. [4]

c) Explain the significance of Reversible and Irreversible mapping in cryptography. [4]

Question: 3

a) Explain the stream cipher implementation of Cipher Feedback (CFB). [4]

b) Describe the Meet in the Middle attack on 3DES scheme. [4]

c) What will be the net effect on decryption process of a block cipher scheme implemented in PCBC-Mode, if two adjacent blocks of cipher-text are interchanged during transmission? [4]

Question: 4

a) Find the RSA Public / Private Keys with $n=87$? Show complete calculation method of your answer. [4]

b) What is digital certificate and what problem does it solve? [4]

c) Explain the Diffie-Hellman Key exchange process. [4]

Question: 5

a) Explain the difference between Unconditional Security and Computational Security [4]

b) What are the main properties of a Cryptographic Hash Function? [4]

c) Suppose RC4 secret internal state is set in the reverse order from S[0] = 255, S[1] = 254, S[2] = 253 up to S[255] = 0. Find the key byte if i = 253 and j = 252. [4]

Question: 6

a) Describe IPSec protocol? Briefly explain two different modes of IPSec with their advantages and disadvantages. [4]

b) Explain why it is not recommended to use same key twice in One Time Pad encryption. [4]

c) Explain the certificate issuance process in Public Key Infrastructure (PKI). [4]

ECB

The End

n=87