Network Security VTU Question Paper Set 2017

USN □□□□□□□□□□ **10EC832**

Eighth Semester B.E. Degree Examination, Dec.2016/Jan.2017
Network Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer any FIVE full questions, selecting atleast TWO questions from each part.***

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

PART – A

1 a. What are the different types of active and passive attacks? **(05 Marks)**

b. Draw the model for network security and specify the four major tasks performed by it. **(04 Marks)**

c. For the cipher text "IMWNIAUP" find the plain text using the key "MINIMUM" using playfair cipher. **(05 Marks)**

d. In an S – DES encryption system the 10 bit key is given as 1001000110. P_{10} is given as $P_{10} = 2\ 7\ 1\ 6\ 3\ 5\ 4\ 9\ 10\ 8$. P_8 is given as $P_8 = 3\ 5\ 6\ 7\ 10\ 2\ 4\ 9$. Deduce sub keys K_1 and K_2. **(06 Marks)**

2 a. Explain with neat block diagrams a single round of DES encryption. **(10 Marks)**

b. Given the cipher text "E M Q Y". Find the plain text using the key $\begin{pmatrix}1 & 1\\ 3 & 2\end{pmatrix}$ in Hill cipher. **(07 Marks)**

c. Write three differences between conventional cryptosystems and public key crypto systems. **(03 Marks)**

3 a. Write the RSA algorithm. **(05 Marks)**

b. In a public key system using RSA intercept the cipher text is 10, sent to a user where public key is 5 and n = 35. Deduce the plain text. **(05 Marks)**

c. What are message Authentication codes? Give the block diagrams to show how MAC is obtained for i) Authentication ii) Confidentiality and authentication tied to plain text and iii) confidentiality and authentication tied to cipher text. **(10 Marks)**

4 a. Draw a block diagram to show any one use of hash functions. **(02 Marks)**

b. Explain the arbitrated digital signature approach of the digital signature function. **(10 Marks)**

c. Explain with diagrams the signing and verifying of digital signature algorithm. **(08 Marks)**

PART – B

5 a. Show the SSL record protocol operation and the details of SSL record format with diagram and explain. **(06 Marks)**

b. Who are the participants of SET? Give the sequence of events required for SET. Explain with appropriate diagram. **(10 Marks)**

c. What are the requirements for digital signature? **(04 Marks)**

6 a. Explain why we need web security. **(02 Marks)**

b. Explain with diagrams how a new password is loaded and how a password is verified. **(10 Marks)**

c. Explain with diagram the distributed intrusion detection. **(08 Marks)**

7 a. Explain how the compression virus propagates. **(08 Marks)**

b. Explain the digital immune system. **(10 Marks)**

c. What are the limitations of fire walls? **(02 Marks)**

8 a. What are the characteristics of a bastion host? **(10 Marks)**

b. Explain with a diagram the application level gateway. **(10 Marks)**

* * * * *

USN □□□□□□□□□□ **10EC832**

Eighth Semester B.E. Degree Examination, June/July 2016
Network Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer FIVE full questions, selecting at least TWO questions from each part.***

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

PART – A

1 a. With a neat diagram, explain network access security model with gate keeper function. **(05 Marks)**

b. Classify and explain different type of attacks. **(08 Marks)**

c. Using the keyword "ENCRYPT" create playfair matrix and obtain ciphertext for the message "MATCHFIXED". Also write the rules used. **(07 Marks)**

2 a. Explain single round of DES along with the key generation. **(10 Marks)**

b. Explain the working of counter mode of block cipher operation. **(04 Marks)**

c. Discuss the final evaluation criteria of AES. **(06 Marks)**

3 a. Justify how both confidentiality and authentication are obtained in publickey cryprosystems. **(05 Marks)**

b. Write RSA algorithm. **(04 Marks)**

c. In Diffie Hellman key exchange q = 71, its primitive root $\alpha = 7$ A's private key is 5 B's private key is 12. Find: i) A's public key; ii) B's public key, iii) Shared secret key. **(05 Marks)**

d. Explain the distribution of secret key using the public key cryprography with confidentiality and authentication. **(06 Marks)**

4 a. List out the requirements and explain the arbitrated digital signature technique. **(10 Marks)**

b. Compare RSA and DSS approach. **(06 Marks)**

c. Illustrate replay attack with examples. **(04 Marks)**

PART – B

5 a. Explain the key requirements and features of SET. **(10 Marks)**

b. Discuss SSL record in terms of fragment compression and encryption. **(10 Marks)**

6 a. Explain password selection strategies. **(08 Marks)**

b. Describe statistical anomaly detection. **(06 Marks)**

c. Discuss the different categories of intruders. **(06 Marks)**

7 a. Give the taxonomy of malicious programs. Briefly explain all the software threats. **(10 Marks)**

b. Describe digital immune system with diagram. **(06 Marks)**

c. Brief on four generations of Antivirus software. **(04 Marks)**

8 a. What is firewall? Explain the various firewall configurations with relevant diagram. **(10 Marks)**

b. Write short notes on:
i) Data Access Control
ii) Concept of Trusted system **(10 Marks)**

* * * * *

USN □□□□□□□□□□ **10EC832**

Eighth Semester B.E. Degree Examination, Dec.2015/Jan.2016

Network Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer any FIVE full questions, selecting atleast TWO questions from each part.***

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

PART – A

1 a. With a neat block diagram, discuss the functioning of network security model. List four basic tasks of designing security model. **(10 Marks)**

b. Encrypt the message "ELECTRONICS" using playfair cipher with a key "INDIA". Also, give the rules for encryption. **(10 Marks)**

2 a. Encrypt the plain text "HAND" using hill cipher with the key

$$\text{key} = \begin{vmatrix} 5 & 8 \\ 17 & 3 \end{vmatrix}$$

Also decrypt it and verify the encryption and decryption text. **(10 Marks)**

b. In S – DES, 10 – bit key is "1010000010". Find the sub keys k_1 and k_2. If

$$\begin{array}{llllllllllll} P_{10} & = & 3 & 5 & 2 & 7 & 4 & 10 & 1 & 9 & 8 & 6 \\ P_8 & = & 6 & 3 & 7 & 4 & 8 & 5 & 10 & 9 \end{array}$$

(10 Marks)

3 a. In a RSA algorithm system, the cipher text received is C = 10 with a public key $P_U = \{5, 35\}$, deduce the plain text. Verify the answer by encryption process. **(10 Marks)**

b. Explain Diffie – Hellman key exchange algorithm. Also calculate the Y_A, Y_B and secret key (k) for $q = 23$, $\alpha = 07$, $X_A = 3$ and $X_B = 6$. **(10 Marks)**

4 a. Write a short note on Hash function. **(05 Marks)**

b. Mention the requirements for a digital signature. **(05 Marks)**

c. Explain the signing and verifying functions of digital signature algorithm (DSA). **(10 Marks)**

PART – B

5 a. Explain the SSL architecture. **(10 Marks)**

b. Highlight the key features of SET. **(05 Marks)**

c. Explain in detail, the payment capture transaction supported by SET. **(05 Marks)**

6 a. Explain the architecture of a distributed intrusion detection system. Give the major issues in the design. **(10 Marks)**

b. Briefly explain the password selection strategies. **(10 Marks)**

7 a. Give the taxonomy of malicious programs and explain in brief. **(10 Marks)**

b. With a schematic, explain the typical step in digital immune system. **(10 Marks)**

8 a. With a neat diagram, explain the concept of trusted systems. **(10 Marks)**

b. What is firewall? Mention the capabilities and limitations of firewalls. **(10 Marks)**

* * * * *

USN □□□□□□□□□□

10EC832

Eighth Semester B.E. Degree Examination, June/July 2015
Network Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer any FIVE full questions, selecting atleast TWO questions from each part.***

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

PART – A

1 a. Explain X·800 security mechanisms, in detail. **(10 Marks)**

b. Differentiate between active and passive attacks. **(04 Marks)**

c. In S –DES, 10 bit key is 1011010011 find the sub keys k_1 and k_2 if :
P_{10} = 35274101986 ; P_8 = 637485109. **(06 Marks)**

2 a. Decrypt the cipher text "CQSUBJNR" using Hill cipher technique with the key : $\begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$. Find the plain text [Hint : a = 0, b = 1, - - - - - z = 25]. **(10 Marks)**

b. How are the disadvantages of ECB mode of operation overcome in the CBC mode of operation? **(10 Marks)**

3 a. Perform encryption and decryption using RSA if p = 7, q = 11, e = 13 and M = 5. **(08 Marks)**

b. Explain the public key distribution of secret key with confidentiality and authentication. **(04 Marks)**

c. With neat schematics, explain message authentication code. **(08 Marks)**

4 a. What is a digital signature? List the properties and requirements of digital signature. **(10 Marks)**

b. Discuss the various approaches of one – way authentication protocol. **(10 Marks)**

PART – B

5 a. What are the services provided by SSL record protocol for SSL connections? Explain overall operation of SSL record protocol. **(10 Marks)**

b. List and explain the SET participants with neat diagram. **(10 Marks)**

6 a. Explain the techniques used for intrusion. **(06 Marks)**

b. Write short notes on honey pots. **(04 Marks)**

c. Explain password selection strategies in detail. **(10 Marks)**

7 a. Write short notes on Trojan horses. **(05 Marks)**

b. Explain the various phases that a virus undergoes during its life time. **(05 Marks)**

c. Discuss the two most important advanced antivirus techniques. **(10 Marks)**

8 a. List and explain the different attacks on packet filtering routers along with appropriate counter measures. **(10 Marks)**

b. Explain briefly the concept of trusted systems. **(10 Marks)**

* * * * *

USN □□□□□□□□□□ **10EC832**

Eighth Semester B.E. Degree Examination, June / July 2014
Network Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer FIVE full questions, selecting at least TWO questions from each part.***

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

PART – A

1 a. Distinguish between passive and active attacks. **(04 Marks)**

b. Explain the different categories of security services. **(06 Marks)**

c. Draw the block diagram of network security model and explain it. Mention basic tasks in designing a particular security service. **(10 Marks)**

2 a. Encrypt the plain text "PAY MORE MONEY" using Hill Cipher with the key.

$$\text{Key} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

Show the calculations and cipher text. **(10 Marks)**

b. Draw the single round DES algorithm and explain the process in detail. **(10 Marks)**

3 a. In a RSA algorithm system it is given that p = 3, q = 11, e = 7 and M = 5. Find the cipher text 'C' and decrypt 'C' to get plaintext M. **(06 Marks)**

b. Explain Diffie-Hellman key exchange algorithm with example. **(06 Marks)**

c. What is key management? Explain distribution of secret key using public key cryptography. **(08 Marks)**

4 a. Explain arbitrated digital signatures technique. **(08 Marks)**

b. With neat diagram, explain digital signature algorithm. **(08 Marks)**

c. Illustrate replay attacks. **(04 Marks)**

PART – B

5 a. Draw the block diagram of handshake protocol action and explain it. **(08 Marks)**

b. Explain in detail: i) Purchase request ii) Payment authorization transaction supported by Secure Electronic Transaction (SET). **(08 Marks)**

c. List the features of secure socket layer. **(04 Marks)**

6 a. What are the different types of intrusion detection system and explain it? **(10 Marks)**

b. Mention the advantages and disadvantages of signature-based detection. **(04 Marks)**

c. Explain the password selection strategies. **(06 Marks)**

7 a. Briefly describe the types of viruses. **(08 Marks)**

b. With a neat diagram, explain digitial immune system. **(08 Marks)**

c. Difference between worm and virus. **(04 Marks)**

8 a. What are the different types of firewall and explain packet filtering router in detail? **(10 Marks)**

b. What are the different firewall configurations and explain it? **(10 Marks)**

* * * * *