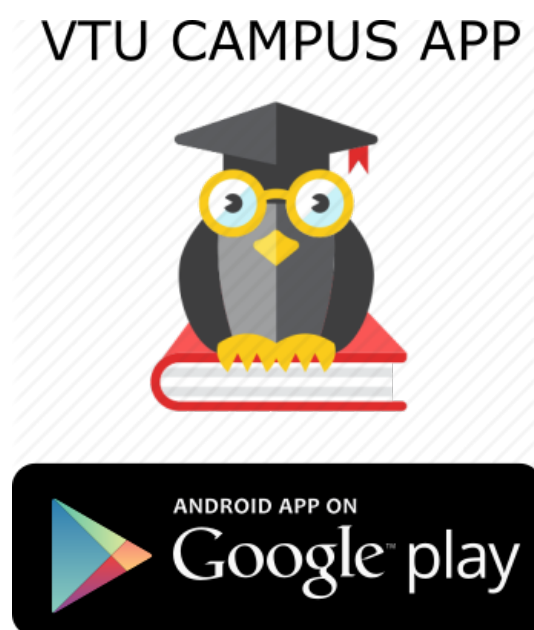


Information and Network Security VTU Question Paper Set 2017



USN

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

10CS/IS835

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

Time: 3 hrs.

Max. Marks:100

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

PART – A

- 1 a. Explain the relationship between policies, standards and practices with a diagram. (06 Marks)
b. Explain EISP and its components. (08 Marks)
c. Explain the components of contingency planning. (06 Marks)
- 2 a. Discuss five major processing – mode categories of firewalls. (10 Marks)
b. Define VPN and explain briefly the different modes to implement VPN. (10 Marks)
- 3 a. Explain different types of IDP system. (10 Marks)
b. Define Honey pot. List its advantages and disadvantages. (10 Marks)
- 4 a. Explain any 3 types of cryptographic tools. (12 Marks)
b. Explain transposition cipher method with an example. (08 Marks)

PART – B

- 5 a. Explain the model for network security. (06 Marks)
b. Describe the security services defined in X.800. (08 Marks)
c. Differentiate between Kerberos version 4 and 5. (06 Marks)
- 6 a. Explain the different types of PGP services. (05 Marks)
b. With a neat diagram, explain the general format of PGP message. (07 Marks)
c. Explain functions and cryptographic algorithms used in S/MIME functionality. (08 Marks)
- 7 a. Give the general structure of IPsec authentication header. Describe how anti – replay service is supported. (10 Marks)
b. What is security association? Discuss various parameters used to describe a security association database. (10 Marks)
- 8 a. Explain SSL protocol stack and discuss session and connection state parameters. (10 Marks)
b. Explain the requirements and features of secure electronic transaction. (10 Marks)

* * * * *

2. Any revealing of identification, appeal to evaluator and/or equations written eg. 42+8 = 50, will be treated as malpractice.



USN

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

10CS/IS835

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

Information and Network Security

Time: 3 hrs.

Max. Marks: 100

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

PART – A

- 1
 - a. Briefly explain the components of issue specific security policy. (08 Marks)
 - b. Discuss various stages in a Incident response planning strategy. (08 Marks)
 - c. Write and define different levels of controls in a security Architecture. (04 Marks)
- 2
 - a. Explain different categories of Firewalls according to their processing mode. (10 Marks)
 - b. Define any six design rules of Firewall. (06 Marks)
 - c. Discuss content filter technology in a security. (04 Marks)
- 3
 - a. Explain Host based intrusion detection system. Write its advantages and disadvantages. (08 Marks)
 - b. Discuss port scanning and Vulnerability scanning tools. (08 Marks)
 - c. Define the following terms with respect to intrusion detection system:
 - i) Alert ii) False positive iii) False negative iv) Confidence value. (04 Marks)
- 4
 - a. Describe any four attacks on a cryptosystem. (08 Marks)
 - b. Explain substitution cipher technique. Discuss its weakness. (08 Marks)
 - c. Define the following terms with respect to cryptography:
 - i) Encryption ii) Cipher iii) Keyspace iv) Strganography. (04 Marks)

PART – B

- 5
 - a. Write and explain the general format of a X.509 public key certificate. (08 Marks)
 - b. List the difference between Kerberos version 4 and version 5. (06 Marks)
 - c. Explain any Three Active security attacks. (06 Marks)
- 6
 - a. Explain the PGP message generation and message reception technique. (10 Marks)
 - b. Briefly explain the header fields of MIME protocol. (05 Marks)
 - c. What is S/MIME? What are the functions of S/SMIME? (05 Marks)
- 7
 - a. Describe the SA parameters and SA selectors of a IPSec. (10 Marks)
 - b. Draw and explain the header format of ESP protocol. (06 Marks)
 - c. Mention the applications of IPSec. (04 Marks)
- 8
 - a. Explain different phases in a SSL Handshake protocol. (10 Marks)
 - b. Define the key features of SET protocol. (04 Marks)
 - c. Discuss the need and construction of a Dual-signature in a SET protocol. (06 Marks)

* * * * *

USN

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

10CS/IS835

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

Information and Network Security

Time: 3 hrs.

Max. Marks: 100

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

PART – A

- 1 a. Explain the characteristics of viable security policies. (10 Marks)
b. Discuss the components of sample issue specific policy. (10 Marks)
- 2 a. Explain the dual homed host firewall. (10 Marks)
b. Define firewall and explain all the firewall rules. (10 Marks)
- 3 a. Explain the different types of IDP systems. (10 Marks)
b. Discuss measuring effectiveness of IDPs. (10 Marks)
- 4 a. With an example, explain vernam cipher technique for encrypting the plaintext. (10 Marks)
b. Explain the different attacks on crypto system. (10 Marks)

PART – B

- 5 a. Discuss the different active attacks. (10 Marks)
b. Explain the environmental shortcomings of Kerberos V4. (05 Marks)
c. With a diagram, explain the X-509 certificate format. (05 Marks)
- 6 a. Using figure, explain how authentication is performed in PGP. (10 Marks)
b. Explain the S/MIME functionality. (05 Marks)
c. Explain the MIME content types. (05 Marks)
- 7 a. With a diagram, explain basic combination of security associations. (10 Marks)
b. Explain the ISAKMP message exchange types. (10 Marks)
- 8 a. Explain the handshake protocol action in SSL. (10 Marks)
b. Explain the key features of SET. (05 Marks)
c. With a figure, discuss the dual signature construction. (05 Marks)

* * * * *

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.



USN

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

10CS/IS835

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

Information and Network Security

Time: 3 hrs.

Max. Marks: 100

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

PART – A

- 1 a. Describe an EISP and its components. (10 Marks)
b. With a neat diagram, explain briefly the major steps in contingency planning. (10 Marks)
- 2 a. Discuss the different generations of firewalls. (06 Marks)
b. Explain the important points for selecting the right firewall. (04 Marks)
c. Explain the implementation of Virtual Private Networks (VPN) in different method. (10 Marks)
- 3 a. Explain the advantages and disadvantages of NIDPS. (10 Marks)
b. Describe the different IDPS detection methods. (10 Marks)
- 4 a. Explain Vernam Ciphre with an example. (10 Marks)
b. Discuss the tools that are used in cryptography. (10 Marks)

PART – B

- 5 a. Explain briefly OSI security architecture. (12 Marks)
b. Discuss the difference between Kerberos version 4 and Kerberos version 5. (08 Marks)
- 6 a. With a neat diagram, explain the overview of Kerberos. (10 Marks)
b. Explain the procedure along with diagram to implement confidentiality in PGP. (10 Marks)
- 7 a. Explain the architecture of the IPSec, also discuss the role of security associations. (10 Marks)
b. Describe how Authentication Header is implemented in Transport and Tunnel modes with a neat diagram. (10 Marks)
- 8 a. Explain session state parameters and connection state parameters in detail. (10 Marks)
b. Discuss the components of a SET with diagram. (10 Marks)

* * * * *

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.