CS6701 – CRYPTOGRAPHY AND NETWORK SECURITY

ANNA UNIVERSITY QUESTION PAPERS

NOV\DEC 2007
MAY/JUNE 2007
APRIL/MAY 2008
MAY/JUNE 2009
NOV/DEC 2009
NOV/DEC 2010
APRIL/MAY 2011
NOV/DEC 2011
NOV/DEC 2011
APR/MAY 2012
NOV/DEC 2012
MAY/JUN 2013
NOV/DEC 2013
MAY/JUN 2014
NOV/DEC 2014
APRIL/MAY 2015

B.E/B.Tech DEGREE EXAMINATION NOV\DEC2007

CRYPTOGRAPHY & NETWORK SECURITY

PART A — (10*2 = 20 MARKS)

1. What is avalanche effect?
2. What are types of attacks on encrypted message?
3. Find get (56, 86) using Euclid's algorithm.
4. Why Elliptic Curve Cryptography is considered to be better than RSA?
5. What is masquerading?
6. Define weak collision property of a hash function?
7. What is x.509 standard?
8. Give IPSEC ESP format
9. What are honey pots?
10. List down the four phases of virus?

PART B (5 x 16 = 80)

11. (a) Discuss in detail encryption and decryption process of AES. (16)

(OR)

(b) (i) Briefly explain design principles of block cipher. (8)

(ii) Discuss in detail block cipher modes of operation (8)

12. (a) (i) Discuss in detail RSA algorithm, highlighting its computational aspect and security. (10)

(ii) Perform decryption and encryption using RSA algorithm with p = 3; q = 11; e = 7 and N = 5. (6)

(OR)

(b) (b) Briefly explain Deffie Hellman key exchange with an example. (16)

13. (a) (i) Explain authentication functions in detail. (10)

(ii) Explain the process of creating a window based calculator with your own UI. (8)

(ii) What is meant by message digest? Give an example. (6)

(OR)

(b) (i) Briefly explain Digital signature algorithm. (8)

(ii) Discuss clearly Secure Hash Algorithm (8)

(OR)

B.E/B.TECH DEGREE EXAMINATION NOV/DEC 2009
CRYPTOGRAPHY & NETWORK SECURITY
PART A — (10*2 = 20 MARKS)

1. Whatis cryptanalysis and cryptography?
2. Define threat and attack.
3. What is the role of session key in public key schemes?
4. What is a zero point of an elliptic curve?
5. What are the functions used to produce an authenticator?
6. List the properties a digital signature should possess?
7. Mention the scenario where kerberos scheme is preferred.
8. What are the technical deficiencies in the kerberos version 4 protocol?
9. List the classes of intruders.
10. Give the types of viruses.

PART B — (5 * 16 = 80 MARKS)

11. (a). Explain the OSI security architecture along with the services available. [16]

(Or)

11. (b).(i).Given 10 bit key K=1010000010. Determine K1, k2 where
P10=3 5 2 7 4 10 1 9 8 6
P8= 6 3 7 4 8 5 10 9 by using SDES key generation method. [16]

12.(a).(i).Perform Encryption/Decryption using RSA algorithm for the following:
p=3, q=11, e=7, m=5 [8]
(ii).What attacks are possible on RSA algorithm? [8]

(Or)

12.(b).(i).Given the key 'MONARCHY' apply play fair to plain text "FACTIONALISM" to ensure confidentiality at the destination, decrypt the ciphertext and establish Authenticity [8]

(ii).Apply public key encryption to establish confidentiality in the message from A to B. You are given m=67, KU={7,187}, KR={23,187} [8]

B.E/B.Tech DEGREE EXMINATION, MAY/JUNE 2014

CRYPTOGRAPHY & NETWORK SECURITY

PART A — (10*2 = 20 MARKS)

1. Define confidentiality.
2. What you mean by passive attacks
3. Define stream and block cipher
4. What are the disadvantages of double DES
5. State cryptography
6. Define elliptic cryptosystem
7. Write out hash function.
8. Mention the services provided by the pretty good privacy
9. How is security handled in .NET?
10. Define –DoS

PART B-(5X16=80 marks)

11. (a) Explain in detail about the security services classifications and security mechanism 16

OR

(b) Compare and contract symmetric crypto primitives and asymmetric crypto primitives with suitable examples 16

12. (a) Explain briefly –substitution ciphers and transposition ciphers. 16

OR

(b) Explain in detail about the DES algorithm. 16

13. (a) Discuss in detail about the Rabin cryptosystem

OR

(b) State and explain RSA cryptosystem 16

14. (a) Write out key management concept and Diffie-hallman key exchange concept. 16

OR

(b) How is security provided at transport layer, network layer and in application layer? Discuss 16

15. (a) explain in detail about the WAP Security and GSM security. 16

OR

(b) Write a detailed technical note single sign on (SSO) 16

14. Describe the different types of firewalls and its configuration in detail

UNIT – V

PART-A

1. What is dual signature? What it is purpose?

2. What are the services provided by PGP?

3. Define S/MIME.

4. Draw the header format for an ISAKMP message.

5. What are the protocols used to provide IP security?

6. Give the applications of IP Security.

7. What is meant by SET? What are the features of SET?

8. Why is R64 conversion useful for email generation?

9. What are the steps involved in SET Transactions?

10. Why email compatibility function in PGP needed

11. What is tunnel mode in IP security?

12. What are the elements of MIME?

13. Why does PGP generate a signature before Apply compression?

14. What services are provided by IPSec?

15. Expand and define SPI.

16. How can the signed data entity of S/MIME be prepared? Write the steps