4. Explain basic combination of security association. How many type of key management the IPSec architecture have? Explain format, Payload types and exchange type of ISAKMP in detail.

5. Explain the term PGP in detail. Draw the general format of PGP with explanation. What services are provided by PGP? How does PGP used in the concept of truth for public key and information?

6. (a) What are the antivirus approaches with its generation?
   (b) What is Firewall? Define its types in detail. Explain its characteristics? Discuss firewall configuration system in detail. How firewall is Network Configuration Management (NCM)?

❑❑

BCA

(SEM. VI) EXAMINATION, MAY, 2018

BCA - 601 (N) : COMPUTER NETWORK SECURITY

Time : Three Hours *Maximum Marks : 75*

Note : Attempt questions from ***all*** Sections as directed.

Inst. : The candidates are required to answer only in serial order. If there are many parts of a question, answer them in continuation.

SECTION – A

Note : *All* questions are compulsory.

1. Define the following terms :
   (i) Kerberos
   (ii) Model for Internetwork Security
   (iii) Transport Layer Security.
   (iv) PGP.

SECTION – B

Note : Attempt *any seven* questions. Each question carries 8 marks.

2. Using a diagram explain all components of a symmetric encryption scheme.
3. What is Mono-alphabetic Cipher? How is it different from Caesar Cipher?
4. Distinguish between Symmetric and Asymmetric key cryptography.
5. Explain, why is SHA more secure than MD5.
6. What do you understand by a Virus? What are the various intrusion detection approaches?
7. Discuss firewall configuration system in detail. Mention the limitations of firewalls.
8. Explain briefly about the SNMPv3.
9. What do you understand by Web Security Threats? What is the secure socket layer?
10. What do you understand by IP Security Architecture?

SECTION – C

Note : Attempt *any one* question. Each question carries 11 marks.

11. Explain the purpose of Owner Trust field, Key Legitimacy field and Signature Trust field maintained in the Public Key ring of PGP. Explain why owners Trust field is not enough to permit PGP to use corresponding public key?
12. What is the purpose of MIME? Discuss functionality of MIME. Also explain delta revocation.

❑❑

BCA

(SEM. VI) EXAMINATION, MAY, 2019

BCA - 601 (N) : COMPUTER NETWORK SECURITY

Time : Three Hours *Maximum Marks : 75*

Note : Attempt questions from ***all*** Sections as directed.

Inst. : The candidates are required to answer only in serial order. If there are many parts of a question, answer them in continuation.

SECTION – A 2 each

Note : *All* questions are compulsory.

1. What are four categories of active attacks? Just name them.
2. What are different types of data confidentiality?
3. What do you understand by Non-repudiation?
4. What do you understand by Cipher? What is block cipher?

SECTION – B 8 each

Note : Attempt *any seven* questions from this Section.

5. What are technical deficiencies of Kerberos ver. 4?
6. Compare various threats on the web, their consequences and countermeasures against them.
7. What services Pretty Good Privacy (PGP) provides? Elaborate them.
8. What is Intrusion? How is it detected?
9. What is secure hash function? What properties should it possess?
10. What are the various types of attacks on encrypted message? Explain in details.
11. Explain Diffie-Hellman Key Exchange.
12. Explain triple DES (3DES).
13. What are different types of Firewalls? Explain all in short.

SECTION – C 11 each

Note : Attempt *any one* question from this Section.

14. What do you understand by IPSecurity (IPSec.)? What are its applications and benefits?
15. Explain in detail the handshake protocol. What key exchange methods are supported?

□□

BCA

(SEM. VI) EXAMINATION, MAY, 2017

BCA – 601 (N) : COMPUTER NETWORK SECURITY

Time : Three Hours *Maximum Marks :75*

Note : Attempt questions from all Sections as directed.

Inst. : The candidates are required to answer only in serial order. If there are many parts of a question, answer them in continuation.

SECTION – A
(Short Answer Type Questions)

Note : *All* questions are compulsory. Each question carries 5 marks.

1. (A) (a) Define the three security goals.
   (b) List and briefly define types of cryptanalytic attacks based on what is known to the attacker.

   (B) Differentiate substitution and transposition techniques for encryption. Discuss PLAYFAIR cipher by suitable example.

   (C) (a) What are three broad categories of application of public key cryptosystem?
   (b) What are the properties a digital signature should have?

   (D) How can you differentiate intruders and viruses? Specify at least five virus with short description. Define basic principle for use of firewall.

   (E) What services defined in RFC 4301 for IPSec? Describe the modes of use IPSec by AH and ESP. Compare those modes with respect of IPSec protocols.

   (F) Define Public Key Infrastructure created by IETF on X.509 with its duties in detail.

   (G) Define protocol for e-Mail security with use of suitable example on the basis of e-Mail architecture. In S/MIME explain how two entities / persons exchange key for encrypting message.

   (H) (a) What is the difference between an unconditionally secure cipher and a computationally secure cipher?
   (b) What problem was kerberos designed to address?

   (I) Explain the versions of SNMP. With proper comparison between them define which one is best.

SECTION – B
(Long Answer Type Questions)

Note : Attempt *any two* questions. Each question carries 15 marks.

2. (a) Explain transport layer security.
   (b) Give an overview of SET. What are the components of SET? Define in detail. What are the SET transaction types?

3. Give a detailed description of SNMP architecture. What are the components of SNMP? Define in detail. What are the applications of SNMP – V3? Define community of facility with respect of SNMP- VI.

BCA

(SEM. VI) EXAMINATION, MAY/JUNE, 2016
BCA – 601 (N) : COMPUTER NETWORK SECURITY

Time : 3 Hours *Total Marks :75*

Note : Section 'A' is compulsory. Attempt *seven* questions from Section 'B' and *one* question from Section 'C'.

Inst. : The candidates are required to answer only in serial order. If there are many parts of a question, answer them in continuation.

SECTION – A

1. (a) Define the following terms : (4)
   (i) Data confidentiality
   (ii) Authentication
   (b) Write in short about two general approaches to attacking a conventional encryption scheme. (4)

SECTION – B

2. Using a diagram explain all components of a symmetric encryption scheme. (8)
3. Explain any one of the multiletter encryption cipher. Mention name of such cipher you are explaining. (8)
4. Write in short about Block cipher modes of operation. (8)
5. Find gcd of 1970 and 1066 using Euclid's Algorithm. (8)
6. (a) Mention various key distribution techniques. (4)
   (b) Define session key and master key. (4)
7. Draw and write about each part of general format of a X.509 certificate. (8)
8. Write about the five principal services provided by PGP. (8)
9. Mention and write about the security association parameters used in IPSEC. (8)
10. What do you understand by Digital Signature? Explain Digital Signature Algorithm. (8)

SECTION – C

11. Define the term Intrusion. What are the various intrusion detection approaches? Explain. (11)
12. Write in short about each of the following : (11)
    (i) SNMP
    (ii) Firewall type
    (iii) SSL

❑❑