MS-III CBGS May 2015

KT

QP Code : 19325

(1)

Time allowed:3 hrs

Maximum marks: 80

Note

i. Q1. is compulsory
ii. Answer any four from Q2 – Q7
iii. Figures to right indicate marks
iv. Answers to the same questions should be answered together

Q 1. A) What is network security? Explain different types of attacks in network security [10]

B) Distinguish between symmetric and asymmetric cryptography [10]

Q 2. A) What is digital certificate? How is digital certificate issued and by whom? [08]

B) What is Kerberos? How is Kerberos V5 different from V4? [07]

Q 3. A) What is man in the middle attack? Explain with help of an example [08]

B) What do you mean by IDS? Explain detection mechanism [07]

Q 4. A) What is hash? Compare SH1 and MD5. [08]

B) Discuss MD4 in detail [07]

Q 5. A) Explain DES algorithm with reference to its overview and DES round [08]

B) Explain in brief the security mechanism used in electronic transaction [07]

Q 6. A) What is firewall? Explain its types with suitable diagram [08]

B) Discuss Secure Socket layer in e-commerce [07]

Q 7. **Write Short Notes( Any Three )** [15]

a) Integrity Check b) Honey Pots

c) Digital Signature d) PGP

---

DP-Con. : 9682-15.

Network Security 8/Dec./2014

2

QP Code : 17885

[3 Hours] [ Total Marks:80

N.B. :(1) Question No. 1 is **compulsory.**
(2) Attempt any **four** questions from question Nos. 2 to 7.

1. (A) What is network security? Explain different types of Attacks in network Security. 10
(B) Explain in details the DES algorithm with reference to its overview and a DES Round. 10

2. (A) What is Hash? Compare SHA1 and MD5. 7
(B) Explain KDC. How does the key distribution work with multiple KDC domains? 8

3. (A) Explain Diffle-Hellman Key distribution algorithm. What is Man-in-the-Middle attack? 7
(B) What is Digital certificate? How is Digital certificate issue and by whom. 8

4. (A) How Kerberos version 5 works? How is Kerberos vS different from v4? 8
(B) What do you mean by IDS? Explain Detection mechanism. 7

5. (A) What is firewall? Explain its type with suitable diagrams. 8
(B) Discuss SSL as an internet protocol for secure exchange of information. 7

6. (A) Explain in brief the security mechanism used in an Electronic transaction. 7
(B) What is Mutual Authentication? A version of this protocol has a security pitfall known as theReflection Attack. What is Reflection Attack? Suggest one method of fixing this. 8

7. Write short note on the following:— 15
(A) Integrity check
(B) S/MIME
(C) Cross certification
(D) Honey Pots

3113 IIIrd Sem IT (Rev) Network Security

QP Code : **17776**

(3 Hours) [ Total Marks : 100

N.B. (1) Questions No. **1** is **compulsory**.
(2) Attempt any **four** out of remaining **six** questions.
(3) **Each** question carry **equal** marks.
(4) **Figures** to the **right** indicate **marks**.

1. (a) What are key principles of security ? 5
(b) Explain digital signature. 5
(c) Distinguish between symmetric and asymmetric cryptography. 5
(d) Explain different types of firewalls. 5

2. (a) What is message digest ? Explain MD2 algorithm for generating the message digest. 10
(b) List the sequence of steps in DES algorithm ? 10

3. (a) Explain RSA algorithm with the help of numerical example. 10
(b) Explain working of KDC and multi domain KDC. 10

4. (a) Explain mutual authentication and reflection attack with the help of diagram. Suggest one method for fixing it. 10
(b) Explain the features of Kerberos v4 and v5. 10

5. (a) Distinguish between ECB and CBC modes. 10
(b) Explain man in the middle attack in Diffie-Hellman algorithm with an example. 10

6. (a) Explain one and two way public key authentication. 10
(b) Discuss Secure Electronic transaction in e-commerce. 10

7. Write short notes on any **four** of the following : 20
(a) Biometrics
(b) PGP
(c) Ticket lifetimes and revoking
(d) SSL
(e) PKCS.

MCA - III CBGS 9/5/14
Network Security

**QP Code : GJ-2394**

**Time :3hrs** **Total Marks: 80**

Note: 1) Question No. **1** is compulsory.
2) Attempt any **four** from Q No. **2** to Q No. **7**

Q.1(a) What are key principles of Network security (10)
(b) Distinguish between symmetric and asymmetric cryptography. (10)

Q2 (a) Explain in details the DES algorithm with reference to its overview and a DES Round. (08)
(b) Name the methods used for encrypting large messages. Explain output feedback mode (OFM). (07)

Q3 (a) Explain with the help of a diagram the working of Kerberos version 4. (08)
(b).How are Kerberos ticket lifetimes in V5 different from V4? (07)

Q 4 (a)What is man in middle attack? Explain with the help of an example. (08)
(b) Discuss Diffie-Hellman crypto system. (07)

Q.5(a )Compare SHA1 and MD5. (08)
(b). Discuss MD4 in detail. (07)

Q.6(a) Explain password based and address based authentication. (08)
(b) Discuss Secure Socket Layer in e-commerce. (07)

Q7. Short notes on any three of the following:- (15)
a. Email security
b. Smart Cards
c. Biometrics
d. Honey pots

MS Sem III 7/12/13 CGSGS

on. 3110-13

CE-8333

(3 Hours) [Total Marks : 80

**N.B. :** (1) Question No. **1** is **compulsory**.
(2) Answer any **four** from Question Nos. **2** to **7**.

1. (a) Explain features of Kerberos $V_4$ and $V_5$ messages. 10
   (b) Explain Diffie-Hellman key exchange algorithm in detail. 10

2. (a) What are key principles of security ? 8
   (b) Distinguish between Symmetric and Asymmetric key cryptography. 7

3. (a) Explain one DES round in detail. 8
   (b) What is message digest? Compare MD5 and SHA-1 message digest algorithms. 7

4. (a) Explain SSL Handshake protocol. 8
   (b) (i) Explain the concept of Keyrings in PGP. 4
   (ii) What is the purpose of SSL alert protocol ? 3

5. (a) What is reflection attack in mutual authentication? How it can be prevented? 8
   (b) Explain Kerberos and its working. 7

6. (a) What is KDC? How it is different from CA? 8
   (b) What is Firewall? Explain its different types? 7

7. Write short notes on any **three** :- 15
   (a) Biometrics
   (b) PEM
   (c) Intrusion Detection System
   (d) IPSec.