Q. P. Code: 24641

DEC - 17

(Time: 3hrs) **(Marks 80)**

1. Question No 1 is compulsory.
2. Attempt any three out of the remaining five questions.

Q1. (a) Encrypt the message "Cryptography is fun" with a multiplicative cipher with key = 15. Decrypt to get back original plaintext. **05**

(b) With the help of suitable examples compare and contrast monoalphabetic ciphers and polyalphabetic ciphers? **05**

(c) What are the properties of hash functions? What is the role of a hash function in security? **05**

(d) What are the different protocols in SSL? How do the client and server establish an SSL connection **05**

Q2. (a) What is a digital certificate? How does it help to validate the authenticity of a user? Explain the X.509 certificate format. **10**

(b) With reference to DES comment on the following: **10**

i) Block size and key size
ii) Need for expansion permutation
iii) Avalanche and completeness effects
iv) Weak keys and semi-weak keys
v) Role of S-box.

Q3. (a) What are the different types of viruses and worms? How do they propagate? **10**

(b) What are the various ways for memory and address protection in Operating System? **10**

Q4. (a) Explain briefly with examples, how the following attacks occur: **10**

i) Phishing attack
ii) Denial of Service attack
iii) SQL injection attack
iv) Cross-site scripting attack

(b) How is security achieved in the transport and tunnel modes of IPSec? What are security associations? **10**

Q5. (a) What are the different threats to emails? Give an algorithm to secure emails being sent from user A to user B. **10**

(b) A and B wish to use RSA to communicate securely. A chooses public key as (7,119) and B chooses public key as (13,221). Calculate their private keys. A wishes to send message m=10 to B. What will be the ciphertext? With what key will A encrypt the message "***m***" if A needs to authenticate itself to B. **10**

Q6. (a) Compare and contrast (any two): 10

i) Block and stream ciphers

ii) MD-5 versus SHA

iii) Key generation in IDEA and Blowfish

(b) What are the different components of an Intrusion Detection System? 10
Compare the working of signature based IDS with anomaly based IDS.

.....

691A54CAB1BACD4A7A3F52499EBD9AA4

DEC - 18

Time: 3 Hours Marks: 80

N.B: Q.1 Compulsory. Solve any 4.

Q. 1 **Summaries and find Plain text by decrypting cipher text "XVWG" using Hill Cipher Substitution technique .**

KEY matrix →

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$$

10

Q. 1 b) **Consider a scenario where an intruder wants to access some valuable information from an ongoing communication. What security services should be implemented in system and which mechanism can be used to achieve those security services?**

Q. 2 a) Encrypt " **academic committee will meet today** " using Playfair Cipher with Keyword "**ROYAL ENFIELD**" 10

Q. 2 b) Discuss CBC and OFB Block cipher Modes with examples. 10

Q. 3 a) If generator g=2 and n or p =11, using diffie Hellman algorithm, solve the following: 10

i) Show that 2 is primitive root of 11
ii) If A has public key 9, What is A's Private Key
iii) If B has public key 3, What is B's Private Key
iv) Calculate shared secret Key

Q. 3 b) **Elaborate International Data Encryption Algorithm (IDEA) and its key generation?** 10

Q. 4 a) Explain Digital Signature and Digital Certificate used for authentication 10

Q. 4 b) Calculate Cipher Text using RSA Algorithm for following data: Prime Numbers P=7, Q= 17. Plain Text Message M=10. Find pair of keys and Cipher text (D,C and P).

Q. 5 a) Explain Hash Based Message Authentication Code. Give Example also. 10

Q. 5 b) Describe various types of Intrusion Detection System (IDS). What are Active and Passive IDS?

1685EEF251B9899113CE47ECACEA3234

Q. 6 a) Convert given PT = $(CA)_{16}$ with Key (1011001101) using S-DES Algorithm.

Given- P10 (3,5,2,7,4,10,1,9,8,6) P4 (2,4,3,1)

P8 (6,3,7,4,8,5,10,9) IP (2,6,3,1,4,8,5,7)

E/P (4,1,2,3,2,3,4,1) IP^{-1} (4,1,3,5,7,2,8,6)

S0=

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

S1=

0	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3

Q. 6 b) Explain concept of key management along with its distribution system.

1685EEF251B9899113CE47ECACEA3234

diffmail

Mailbox of exam_kgce2010

Subject: Correction in QP Code: 57241

From: University of Mumbai<support@muapps.in> on Tue, 27 Nov 2018 11:45:16

To: <exam_kgce2010@rediffmail.com>

University of Mumbai

Correction in 1T00717 - B.E.(COMPUTER)(Sem VII) (R-2012) (CBSGS) / 42102 - Cryptography and System Security **QP Code: 57241**

Instruction : Question 1 Compulsory, Solve Any Three Instead of Four

Q. 3 a) ii) If A has private key 9, What's A's Public Key
iii) If B has private key 3, what's B's Public Key

q.5 b) .... Marks 10
q.6 a) .... Marks 10
q.6 b) .... Marks 10

University of Mumbai
https://muapps.in
support@muapps.in
022-26534263 / 022-26534266
Mon-Fri, 10am - 5pm

DEC - 19

(3 hours) **Marks:[80]**

N.B

1. Question No. 1 is compulsory.
2. Attempt any 3 out of remaining 5.

Q.1	a) Explain the different software flaws with example.	**05**
	b) Define goals of security and mechanism to achieve them.	**05**
	c) Define the properties and applications of Hash function.	**05**
	d) Explain handshake protocol in SSL.	**05**
Q.2	a) How is security achieved in Transport and Tunnel modes of IPSEC? Explain the role of AH and ESP.	**10**
	b) How does PGP achieve confidentiality and authentication in emails?	**10**
Q.3	a) Why are digital certificates and signatures required? What is role of digital signature in digital certificates? Explain any one digital signature algorithm.	**10**
	b) What are the different components of Intrusion Detection System? Compare signature based IDS to anomaly based IDS.	**10**
Q.4	a) Discuss DES with reference to following points • Block size and key size • need of expansion permutation • role of S-box • weak keys and semi weak keys • possible attacks on DES	**10**
	b) Explain Diffie Hellman key exchange algorithm. What types of attacks are possible on it explain with example.	**10**
Q.5	a) Explain briefly the following attacks with example (I) Session hijacking (II) Salami Attack (III) SQL injection (IV) Buffer overflow	**10**
	b) What is Denial of Service attack? What are the different ways in which an attacker can mount a DOS attack on a system?	**10**
Q.6	a) Explain the working of Kerberos.	**10**
	b) Elaborate the steps of key generation using RSA algorithm. In RSA system the public key (E, N) of user A is defined as (7,187). Calculate Φ(N) and private key 'D'. What is the cipher text for M=10 using the public key.	**10**

MAY - 17

3 hrs. 80 marks

Note :
1. **Question 1 is compulsory.**
2. **Attempt any 3 questions out of the rest.**
3. **Make suitable assumptions whenever necessary and justify them**
4. **Each question carries equal marks.**

Q1.

a) Use the Play fair cipher with the keyword : "MEDICINE" to encipher the message "The greatest wealth is health". (5)

b) Explain key rings in PGP. (5)

c) Briefly define idea behind RSA and also explain (10)

1) What is the one way function in this system?
2) What is the trap door in this?
3) Give Public key and Private Key.
4) Describe security in this system.

Q2)a) Explain DES, detailing the Feistel structure and S-block design (10)

b) Consider a Voter data management system in E-voting system with sensitive and non-sensitive attributes. (10)

1) Show with sample queries how attacks (Direct, Inference) are possible on such data sets
2) Suggest 2 different ways to mitigate the problem.

Q 3)

a) Explain Diffie-Hellman Key exchange algorithm with suitable example. Also explain the problem of MIM attack in it (10)

b) What are Denial of Service attacks? Explain any three types of DOS attacks in detail (10)

Q 4)

a) IPSec offers security at n/w layer. What is the need of SSL? Explain the services of SSL protocol? (10)

b) What are the types of firewalls? How are firewalls different from IDS (10)

Q 5)a) What are the various ways in which public key distribution is implemented. Explain the working of public key certificates clearly detailing the role of certificate authority. (10)

b) Why are Digital Signatures & Digital certificates required? What is the significance of Dual Signature. (10)

Q6 Attempt any 4 (20)

a) SHA-1
b) Timing and Storage Covert Channel
c) Session Hijacking and Spoofing
d) Blowfish
f) S/MIME

MAY - 18

Q. P. Code: 24643

(3 Hours) [Total Marks:80]

1. Question No. 1 is compulsory.
2. Attempt any three out of the remaining five questions.
3. Assume suitable data if necessary
4. Figures to right indicate full marks.

Q.1	(a)	What is the purpose of S-boxes in DES? Explain the avalanche effect?	[05]
	(b)	Give examples of replay attacks. List three general approaches for dealing with replay attacks.	[05]
	(c)	Why is the segmentation and reassembly function in PGP(Pretty Good Privacy) needed?	[05]
	(d)	List and explain various types of attacks on encrypted message.	[05]
Q.2	(a)	What is the need for message authentication? List various techniques used for message authentication. Explain any one.	[10]
	(b)	Explain Kerberos protocol that supports authentication in distributed system.	[10]
Q.3	(a)	What characteristics are needed in secure hash function? Explain the operation of secure hash algorithm on 512 bit block.	[10]
	(b)	What is a nonce in key distribution scenario? Explain the key distribution scenario if A wishes to establish logical connection with B. A and B both have a master key which they share with itself and key distribution center.	[10]
Q.4	(a)	Why E-commerce transactions need security? Which tasks are performed by payment gateway in E-commerce transaction? Explain the SET (Secure Electronic Transaction) protocol.	[10]
	(b)	In RSA system the public key of a given user e=7 & n=187.	[10]

2F4A7267688055B483146CAF0560042A

1) What is the private key of this user?
2) If the intercepted CT=11 and sent to a user whose public key e=7 & n=187. What is the PT?
3) Elaborate various kinds of attacks on RSA algorithm?

Q.5 **(a)** How can we achieve web security? Explain with example. **[10]**

(b) Use Hill cipher to encrypt the text "short". The key to be used is "hill". **[10]**

Q.6 **(a)** Explain IPSec protocol in detail. Also write applications and advantages of IPSec. **[10]**

(b) Differentiate between i) MD-5 and SHA ii) Firewall and IDS. **[10]**

****

2F4A7267688055B483146CAF0560042A

MAY - 19

[3 Hours] **[Total Marks 80]**

N. B: 1. Question No. 1 is Compulsory.
2. Solve any THREE from Question No. 2 to 6.
3. Draw neat well labeled diagram wherever necessary.

Q.1	a)	Enlist security goals. Discuss their significance.	(05)
	b)	Compare AES and DES. Which one is bit oriented? Which one is byte oriented?	(05)
	c)	What is authentication header(AH)? How does it protect against replay attacks?	(05)
	d)	List various Software Vulnerabilities. How vulnerabilities are exploited to launch an attack.	(05)
Q.2	a)	Encrypt the plaintext message "SECURITY" using affine cipher with the key pair (3, 7). Decrypt to get back original plaintext.	(10)
	b)	Explain different types of Denial of Service attacks.	(10)
Q.3	a)	Users A and B use the Diffie-Hellman key exchange technique with a common prime 71 and primitive root 7. Show that 7 is primitive root of 71. If user A has private key x=5, what is A's Public Key R_1? If user B has private key y=12, what is B's public key R_2? What is the shared secret key?	(10)
	b)	What are traditional ciphers? Discuss any one substitution and transposition cipher with example. List their merits and demerits.	(10)
Q.4	a)	Alice chooses public key as (7, 33) and B chooses public key as (13, 221). Calculate their private keys. A wishes to send message m=5 to B. Show the message signing and verification using RSA digital signature.	(10)
	b)	Discuss in detail block cipher modes of operation.	(10)
Q.5	a)	What is the need of SSL? Explain all phases of SSL Handshake protocol in detail.	(10)
	b)	What are the requirements of the cryptographic hash functions? Compare MD5 and SHA Hash functions. State real world applications of hash functions.	(10)
Q. 6		Write short notes on any FOUR: a. Kerberos b. Buffer Overflow c. 3DES d. X.509 e. IDS	(20)

------x-----

NOV-DEC - 19

(3 hours) **Marks:[80]**

N.B

1. Question No. 1 is compulsory.
2. Attempt any 3 out of remaining 5.

Q.1 a) Explain the different software flaws with example. **05**

b) Define goals of security and mechanism to achieve them. **05**

c) Define the properties and applications of Hash function. **05**

d) Explain handshake protocol in SSL. **05**

Q.2 a) How is security achieved in Transport and Tunnel modes of IPSEC? Explain the role of AH and ESP. **10**

b) How does PGP achieve confidentiality and authentication in emails? **10**

Q.3 a) Why are digital certificates and signatures required? What is role of digital signature in digital certificates? Explain any one digital signature algorithm. **10**

b) What are the different components of Intrusion Detection System? Compare signature based IDS to anomaly based IDS. **10**

Q.4 a) Discuss DES with reference to following points **10**

- Block size and key size
- need of expansion permutation
- role of S-box
- weak keys and semi weak keys
- possible attacks on DES

b) Explain Diffie Hellman key exchange algorithm. What types of attacks are possible on it explain with example. **10**

Q.5 a) Explain briefly the following attacks with example **10**

(I) Session hijacking (II) Salami Attack

(III) SQL injection (IV) Buffer overflow

b) What is Denial of Service attack? What are the different ways in which an attacker can mount a DOS attack on a system? **10**

Q.6 a) Explain the working of Kerberos. **10**

b) Elaborate the steps of key generation using RSA algorithm. In RSA system the public key (E, N) of user A is defined as (7,187). Calculate Φ(N) and private key 'D'. What is the cipher text for M=10 using the public key. **10**