SET B

SRM University, Kattankulathur
Faculty of Engineering and Technology, Department of Information Technology
15IT327E- CRYPTOGRAPHY
Cycle Test -2

Specialisation: IT/CSE/SWE
Date:25/10/2017
Max. Marks: 100

Degree : B.Tech
Year/Sem : III/5TH SEM
Duration : 3hrs

										Register Number

Instructional Objective covered in this test:
IO3. Understand various block cipher and stream cipher models.
IO4. Describe the principles of public key cryptosystems, hash functions and digital signature.
IO5. Gain a first-hand experience on encryption algorithms, encryption modes.

Student outcome covered in this test:
1.An ability to use and apply current technical concepts and practices in the core information technologies.

j1.An ability to use and apply current technical concepts in the core information technologies

j2. An ability to use and apply current practices in the core information technologies

2.An ability to use current techniques, skills, and tools necessary for computing practice.

i1.An ability to understand current techniques and Skills.

Mark Allotment

Question No	Instructional Objectives	Course Outcome	Sub Outcome	Marks		Outcome Met/Not Met	Mark Scored (/100)
				Max Marks	Obtained Marks		
1	IO3	j	j1				
2	IO3	j	j1				
3	IO3	j	j1				
4	IO3	j	j1				
5	IO3	j	j1				
6	IO3	j	j1				
7	IO3	j	j1				
8	IO4	j	j2				
9	IO4	j	j2				
10	IO4	j	j2				
11	IO4	j	j2				
12	IO4	j	j2				
13	IO4	j	j2				
14	IO4	j	j2				
15	IO4	j	j2				
16	IO4	j	j2				
17	IO4	j	j1				
18	IO4	j	j1				
19	IO5	i	i1				
20	IO5	i	i1				

Part A (Answer all the Questions) **(20*1=20 Marks)**

1. The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key
   a) 12 b) 18 c) 9 d) 16
2. DES follows
   a) Hash Algorithm b) Caesars Cipher c) Feistel Cipher Structure d) SP Networks
3. _____mode operates on the full block of plaintext and ciphertext
   a) Electronic Codebook Book (ECB) b) Cipher Block Chaining (CBC)
   c) Cipher FeedBack (CFB) d) Output FeedBack (OFB)
4. The 4×4 byte matrices in the AES algorithm are called
   a) States b) Words c) Transitions d) Permutations
5. Which of the following slows the cryptographic algorithm
   1) Increase in Number of rounds
   2) Decrease in Block size
   3) Decrease in Key Size
   4) Increase in Sub key Generation
   a) 1 and 3 b) 2 and 3 c) 3 and 4 d) 2 and 4
6. For the AES-128 algorithm there are _____ similar rounds and _____ round is different.
   a) 2 pair of 5 similar rounds ; every alternate
   b) 9 ; the last
   c) 8 ; the first and last
   d) 10 ; no
7. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____
   a) Scaling of the existing bits b) Duplication of the existing bits
   c) Addition of zeros d) Addition of ones
8. How many keys does the Triple DES algorithm use?
   a) 2 b) 3 c) 2 or 3 d) 3 or 4
9. Blowfish encrypts blocks of plaintext which have size
   a) 256 bits b) 64 bits c) 72 bits d) 128 bits
10. AES have 3 different configuration with respect to number of rounds and
    a) Data size b) Round size c) Key size d) Encryption size

11. Elliptic curve cryptography uses curves whose variables & coefficients are finite

a) Finite elliptic curve b)Prime curves c) Binary curves d) Base curves

12. Calculate the number of subkeys required in RC5 for 18 rounds of computation.

a) 40 b) 38 c) 36 d) 34

13. _____ substitution is the process that accepts 48 bits from XOR operation

a) S-box
b) P-box
c) Expansion permutations
d) Key transformation

14. The input to the encryption and decryption algorithm of AES is a single _____block.

a) 32 b) 128 c) 64 d) 16

15. The _____must be a data block that is unique to each execution of the encryption operation.

a) key b) IV c) nonce d) CBC

16. ElGamal encryption system is

a) symmetric key encryption algorithm
b) asymmetric key encryption algorithm
c) not an encryption algorithm
d) none of the mentioned

17. The DSS signature uses which hash algorithm?

a) MD5 b) SHA-2 c) SHA-1 d) Does not use hash algorithm

18. MD5 produces __ bits hash data ?

a) 128 b) 150 c) 160 d) 112

19. Message authentication code is also known as

a) key code b) keyed hash function
c) hash code d) message key hash function

20. A hash function guarantees integrity of a message. It guarantees that message has not be

a) Replaced b) Over view c) Changed d) Violated

SET A

Faculty of Engineering and Technology, Department of Information Technology

SRM UNIVERSITY

15IT327E- CRYPTOGRAPHY

Cycle Test – 2

Degree : B.Tech
Year/Sem : III/5TH SEM
Duration : 3 hours

Specialization: IT/CSE/SWE
Date: 25/10/2017
Max. Marks: 100

Part B [Answer any five questions] (5 X 4 =20 Marks)

21. Diagrammatically represent public key cryptosystem used for authentication
22. State the strength and weakness of DES
23. What are the characteristics of blowfish.
24. What is man-in-the-middle attack?
25. Write short note on elliptic curve cryptography?
26. Why SHA is more secure than MD5?
27. Explain signing and verifying in DSS

Part C [Answer all the Questions] (5 X 12 =60 Marks)

28a. Explain the Feistel Cipher Structure in detail?

[OR]

28b. Explain the working principles of RC5.

29a. Discuss about techniques used for distribution of public keys.

[OR]

29b. Explain in detail about of DES with neat diagram

30a. Explain in detail about MAC and Hash Function with neat diagrams.

[OR]

30b.Explain in detail about RSA algorithm. Given p=17, q=11, e=7, generate public and private keys, also encrypt and decrypt message 88.

31a. Explain in detail about Diffie Hellman Key Exchange protocol with example.

[OR]

31b. Explain the working of elliptic curve cryptography, brief out how it is applied in cryptography.

32a.Explain the working principles of SHA Algorithm.

[OR]

32b.Explain the working principles of MD5 Algorithm

****** ALL THE BEST ******