Code : 051718

B.Tech.7th Semester Special Examination, 2016

Cryptography

Time : 3 hours *Full Marks : 70*

Instructions :

*(i) There are **Nine** questions in this paper.*

*(ii) Attempt **Five** questions in all.*

*(iii) **Questions No.1 is Compulsory.***

(iv) The marks are indicated in the right hand margin.

---

1. Multiple choice Questions (MCQs) :

(a) By encryption of a text we mean

(i) compressing it

(ii) scrambling it to preserve its security

(iii) expanding it

(iv) hashing it

(b) In public key encryption if A wants to send and encrypted message

(i) A encrypts message using his private key

(ii) A encrypts message using B's private key

(iii) A encrypts message using B's public key

(iv) A encrypts message using his public key

(c) A digital signature is

(i) a bit string giving identity of a correspondent

(ii) a unique identification of a sender

(iii) an encrypted signature of a

(iv) sender an authentication of an electronic record by tying it uniquely to a key only a sender knows.

(d) The Secure Electronic Transaction protocol is used for

(i) credit card payment

(ii) cheque payment

(iii) electronic cash payments

(iv) payment of small amounts internet services

(e) Which of the following security properties does an S-Box provide ?

(i) Diffusion (ii) Integrity

(iii) Malleability (iv) Confusion

(f) Disclosure is a threat against which security goal?

(i) Confidentiality (ii) Integrity

(iii) Assurance (iv) Availability

(g) Which of the following encryption modes suffer from malleability attacks?

(i) Counter CBC-MAC (CCM)

(ii) Cipher Block Chaining (CBC)

(iii) Offset Code Book (OCB)

(iv) Electronic Code Book(ECB)

(h) A way of verifying both the sender of information and the integrity of a message is through the use of

(i) Private key encryption

(ii) digital signatures

(iii) Public key encryption

(iv) digital certificates

(i) A(n) ..... is a key less substitution cipher with N inputs and M outputs that uses a formula to define the relationship between the input stream and output stream.

(i) S-Box (ii) P-Box

(iii) T-Box (iv) None of these

(j) SSL provides only ..... .

(i) integrity (ii) confidentiality

(iii) authentication (iv) durability

2. (a) Given a protocol in which the sender's party performs the following operation:

Protocol; $y = e_{k1}\left(x \| H\left(k2 \| x\right)\right)$,

Where x is the message, H is a hash function such as SHA-1, e is a symmetric key encryption algorithm '$\|$' denotes simple concatenation, and k1, k2 are secret keys which are only known to the sender and the receiver.

Provide a step-by-step description what the receiver does upon reception of y.

(b) An affine cipher with modulus 26 encrypts 4 as 2 and 7 as 17. Determine the key.

3. (a) Use RSA system, where primes p-23 and q=17 and public encryption key is e=3. Compute the decryption key d. show your computations.

(b) Describe in detail how the cipher text C= 165 is decrypted. You must show that you understand how the algorithm for efficient modular exponentiation works.

4. (a) Explain briefly the concepts: one-way function, one-way hash function, trapdoor one-way function.

   (b) The cipher text ATMCCDCTWCWG was obtained using the Vigenere cipher with the keyword CAT. Find the corresponding plaintext.

5. (a) A Feistel cipher is used in the DES algorithm. Describe the operation of a Feistel cipher.

   (b) Use Chinese Remainder Theorem, to find the number which is repeatedly divided by 3 gives remainder as 2; when divided by 5, the remainder is 3; and divided by 7 the remainder is 2. What is the number ?

6. (a) Differentiate between Kerboros V4 and Kerboros V5.

   (b) What are the important services offered by PGP?

7. (a) Explain HMAC in detail with a diagram.

   (b) Alice wants to send a message M with a digital signature Sig (M) to Bob. Alice and Bob have an authentic copy of each other's public keys, and have agreed on using a specific hash function h. Outline the steps that Alice must follow when signing M, and the steps that recipient Bob must follow for validating the signature Sig (M).

8. (a) List all components of AES. Describe Substitute Bytes and Shift Rows Transformation in detail.

   (b) Consider the following key: $\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}$. Encrypt the plaintext, MATH.

9. (a) Why 2-DES is weak in comparison with 3-DES?

   (b) Eve has stumbled upon the square key that Alice and Bob are using to exchange messages via Playfair encryption. That key is:

R	P	M	L	D
S	A	X	I/J	C
H	K	Q	U	Y
E	W	O	Z	G
B	F	T	V	N

Eve now has to decode the message she has intercepted, which starts out: BQZRX SQWTW VSGSV XLUNQ.

***