Code : 051718

B.Tech 7th Semester Special Exam., 2020

CRYPTOGRAPHY

Time : 3 hours *Full Marks* : 70

Instructions :

(i) *The marks are indicated in the right-hand margin.*

(ii) *There are* ***NINE*** *questions in this paper.*

(iii) *Attempt* ***FIVE*** *questions in all.*

(iv) *Question No.* **1** *is compulsory.*

1. Choose the correct option of the following (any *seven*) : 2×7=14

(a) DES follows

(i) hash algorithm

(ii) Caesar cipher

(iii) Feistel cipher structure

(iv) SP-network

(b) Find the solution of $x^2 \equiv 16 \bmod 23$.

(i) $x = 6$ and 17

[✓ *(ii)* $x = 4$ and 19]

(iii) $x = 11$ and 12

(iv) $x = 7$ and 16

(c) In SHA-512, the message is divided into blocks of size ____ bits for the hash computation.

(i) 1024

(ii) 512

(iii) 256

(iv) 1248

(d) When a hash function is used to provide message authentication, the hash function value is referred to as

(i) message field

[✓ *(ii)* message digest]

(iii) message score

(iv) message leap

(e) Which one of the following is not a public-key distribution means?

(i) Public-key certificates

(ii) Hashing certificates

(iii) Publicly available directories

(iv) Public-key authorities

(f) The Data Encryption Standard (DES) was designed by

(i) Microsoft

(ii) Apple

[✓ (iii) IBM]

(iv) None of the above

(g) Which of the following encryption keys is used to encrypt and decrypt the data?

(i) Public key

[✓ (ii) Private key]

(iii) Symmetric key

(iv) Asymmetric key

(h) In asymmetric key cryptography, the private key is kept by

[✓ (i) sender]

(ii) receiver

(iii) both sender and receiver

(iv) all the connected devices to the network

(i) Network layer firewall has two sub-categories as

(i) statefull firewall and stateless firewall

(ii) bit-oriented firewall and byte-oriented firewall

(iii) frame firewall and packet firewall

(iv) None of the above

2. (a) What is the OSI security architecture? List and briefly define the three key objectives of computer security. 7

(b) List and briefly define the categories of passive and active security attacks. List and briefly define the categories of security services. 7

3. Encrypt the message "meet me at the usual place at ten rather than eight O'clock" using the Hill cipher with the key $\begin{pmatrix}7 & 3\\ 2 & 5\end{pmatrix}$.

Show your calculations and the result. Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext. 14

4. *(a)* What is the difference between diffusion and confusion? What are the critical aspects of Feistel cipher design? 7

(b) What is the output of the first round of the DES algorithm when the plaintext and the key both are all zeros? 7

5. *(a)* Describe SubBytes, Shift Rows, MixColumns and AddRoundKey of AES. 7

(b) Find all irreducible polynomials of degree 3 over GF(2). 7

6. One of the most attractive applications of public-key algorithms is the establishment of a secure session key for a private-key algorithm such as AES over an insecure channel. Assume Bob has a pair of public/private keys for the RSA cryptosystem. Develop a simple protocol

using RSA which allows the two parties Alice and Bob to agree on a shared secret key. Who determines the key in this protocol, Alice, Bob or both?

Do the questions mentioned below on RSA : 7×2=14

(a) In the RSA public-key encryption scheme, each user has a public key, *e*, and a private key, *d*. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?

(b) In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M?

7. Briefly explain Diffie-Hellman key exchange. Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $q = 157$ and a primitive root $a = 5$.

(a) If Alice has a private key $XA = 15$, find her public key YA. 7

(b) If Bob has a private key $XB = 27$, find his public key YB. 7

8. *(a)* What problem was Kerberos designed to address? What entities constitute a full service Kerberos environment? What are the threats associated with user authentication over a network or an Internet? 7

(b) Explain X.509 certificate. 7

9. Write short notes on the following : 14

(a) S/MIME

(b) HMAC

(c) Digital signature

(d) Denial of service attack

★ ★ ★