Code : 061705

B.Tech 7th Semester Exam., 2020

INFORMATION SECURITY

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. Answer any *seven* of the following as directed : 2×7=14

(a) What is Digital Certificate?

(b) List three protocols that are used in web services.

(c) Microsoft Internet Information Server and Apache HTTP Server are examples of web server software packages.

(Write True or False)

(d) What do you mean by Data Encryption Standard?

(e) What do you understand by Digital Currencies?

(f) What is trusted operating system?

(g) List common software-based attacks.

(h) What is biometric authentication?

(i) What are the components of PGP?

(j) What are the disadvantages of symmetric key encryption?

2. *(a)* We use Diffie-Hellman key exchange with two users *A* and *B* where prime number, $p = 29$. Answer the following questions : 7

(i) Calculate the smallest primitive element for the given prime number, i.e., $p = 29$. Show each step.

(ii) User *A* chooses a secret key $X_A = 5$ and user *B* chooses a secret key $X_B = 3$. Calculate the common secret key between user *A* and user *B*.

(b) What is the role of cryptography in E-commerce? How does authentication scheme help to secure e-commerce? 7

3. *(a)* Compare the various generation of firewall. Comment on the security achieved and the ease of implementation of the various generations of firewalls. 7

(b) Differentiate between SPAM and Virus. How do you avoid each of the two in your system? 7

4. *(a)* "The double DES (data encryption standard) encryption algorithm takes 112 bit key irrespective of 56 bit key in single DES as a one input for encryption. But the security level in double DES not enhances as proportion to the increased key size compared to single DES." Justify the statement with your comments. 7

(b) What are the threats associated with a direct digital signature scheme? 7

5. *(a)* Suppose $H(m)$ is a collision resistant hash function that maps a message of arbitrary bit length into a n-bit hash value. Is it true that, for all messages x, x' with $x \neq x'$, we have $H(x) \neq H(x')$? Explain your answer. 7

(b) Encrypt the message "meet me at the usual place at ten rather than eight o'clock" using the Hill cipher with the key. Show your calculations and the result.

$$key = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$$ 7

6. *(a)* Suppose that user A has obtained a certificate from certification authority (CA) X1 and user B has obtained a certificate from CA X2. Assume if user A does not securely know the public key of X2, then user A can only read user B's certificate, but A cannot verify the signature. Write the procedure through which user A can verify the signature. 7

(b) RFID tags are extremely small devices capable of broadcasting a number over the air that can be read by a nearby sensor. RFID tags are used for tracking inventory, and they have many other potential uses. For example, RFID tags are used in passports and it has been suggested that they should be put into paper money to prevent counterfeiting. In the future, a person might be

surrounded by a cloud of RFID numbers that would provide a great deal of information about the person.

(i) Discuss some privacy concerns related to the widespread use of RFID tags.

(ii) Discuss security issues, other than privacy, that might arise due to the widespread use of RFID tags. 7

7. (a) Suppose that Alice and Bob decide to always use the same IV instead of choosing IVs at random.

(i) Discuss a security problem this creates if CBC mode is used.

(ii) Discuss a security problem this creates if CTR mode is used.

(iii) If the same IV is always used, which is more secure, CBC or CTR mode? 7

(b) How are operating systems provide security to applications and data? Explain in detail. 7

8. Recall that with the RSA public key system it is possible to choose the same encryption exponent, e, for all users. For the sake of efficiency, sometimes a common value of $e = 3$ is used. Assume this is the case.

(a) What is the cube root attack on RSA and when does it succeed?

(b) Give two different ways of preventing the cube root attack. Both of your proposed fixes must still provide improved efficiency over the case where a common encryption exponent $e = 3$ is not used. 14

9. (a) Consider the knapsack cryptosystem. Suppose the public key consists of (18, 30, 7, 26) and $n = 47$.

(i) Find the private key, assuming $m = 6$.

(ii) Encrypt the message $M = 1101$ (given in binary). Give your result in decimal. 7

(b) We want to design a secure mutual authentication protocol based on a shared symmetric key. We also want to establish a session key, and we want perfect forward secrecy.

(i) Design such a protocol that uses three messages.

(ii) Design such a protocol that uses two messages. 7

★ ★ ★