Code : 061505

B.Tech 5th Semester Examination, 2016

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.

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

---

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

(a) What is Trojan horse?

(b) List advantages and disadvantages of symmetric key and asymmetric key cryptosystem?

(c) Define properties of a MAC function?

(d) Define ideal block cipher?

P.T.O.

(e) In asymmetric key cryptography, the private key kept by:

(i) sender

(ii) receiver

(iii) sender and receiver

(iv) all the connected devices to the network

(f) The RSA algorithm is not secure against

(i) Man-in-the middle attack

(ii) Meet-in the middle attack

(iii) Known plaintext-cipher text pair attack

(iv) Modulus factorization attack

(g) The number of Round function in AES-128 is:

(i) 8

(ii) 10

(iii) 12

(iv) 14

(h) The time complexity of an RSA encryption and decryption process for b-bit message is:

(i) $O(b^2)$ and $O(b^3)$

(ii) $O(b)$ and $O(b^2)$

(iii) $O(nb^2)$ and $O(b^3)$

(iv) $O(b^2)$ and $O(nb^2)$

(i) Which one of the following algorithm is not used in asymmetric-key cryptography?

(i) RSA algorithm

(ii) diffie-hellman algorithm

(iii) electronic code book algorithm

(iv) none of the mentioned

(j) Which one of the following is a cryptographic protocol used to secure HTTP connection?

(i) Stream control transmission protocol (SCTP)

(ii) transport layer security (TSL)

(iii) explicit congestion notification (ECN)

(iv) resource reservation protocol

2. (a) What is the idea behind man-in-the-middle attack? Draw a neat diagram to explain the attack?

(b) Differentiate between computer security, Network security and Information security in detail with suitable example.

7+7=14

3. (a) How digital signature is different from manual signature? Explain how digital certificate are generated using any one of the scheme that your knows.

(b) Encrypt the message "hide the gold" using the play fair cipher with the key "Hello world". Ignore the spaces between the words. Show your calculations and the results.

7+7=14

4. (a) What are the information security goals? Explain why the balance among different goals is needed.

(b) Users A and B use the Diffie-Hellman key exchange technique with a common prime Q=71 and a primitive root α =7.

i. If user A has private key X_A=5, what is A's public key Y_A

ii. If user B has private key X_B = 12, what is B's public key Y_B?

iii. What is the shared secret key? 7+7=14

5. (a) Suppose that user A has obtained a certificate from certification authority CA<<X_1>> and user B has obtained a certificate from CA<<X_2>>. Assume if user A does not securely know the public key of X_2, then user A can only read user B's certificate, but A cannot verify the signature. Write the procedure through user A can verify the signature?

(b) Using the RSA algorithm find the cipher for the message 00111011 with the given p=3, q=11 and Φ(n)=20?

7+7=14

6. (a) What is trap door one way function? How cryptographic hash function are different from the non-cryptographic hash function?

(b) Define the digital signature standard (DSS) algorithm for digital signature generation and verification. 7+7=14

7. (a) What is firewall security? How does firewall management program for Implementing Default allow and Default Deny policies on proxy will work?

(b) Consider a one-way authentication technique based on asymmetric encryption:

$A \rightarrow B : ID_A$

$B \rightarrow A : E(PU_a, R_2)$

$A \rightarrow B : R_2$

(i) Explain the protocol.

(ii) What type of the attack this protocol is susceptible to? 7+7=14

8. (a) A web worm always executes on the user's browser. Yes or no? Explain.

(b) What are the design principles of trusted operating system? Define the role of trusted computing base in providing security. 7+7=14

9. (a) What is meant by saying that a particular site has a cross-site scripting vulnerability? Can you identify such sites on the Internet?

(b) Write short notes on the following:

i. Information Leakage

ii. Phishing emails

iii. Denial-of-Service Attack

7+7=14

***

Code : 061805

B.Tech. 8th Semester Exam., 2017

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) Questions No. 1 is compulsory.

1. Define any 7 out of the following 10 terms: (2×7)

(a) Public key cryptography

(b) Digital Signature

(c) Non-repudiation

(d) Authentication

(e) Firewall

(f) Virus

(g) CAPTCHA

(h) Intrusion Detection

(i) Confusion

(j) Avalanche Effect

2. (a) What is Codebook Cipher ? Explain with the help of an example how it can provide security. 7

(b) Explain Transposition Cipher Method and using the method produce the Ciphertext for the following Plaintext: "sack gaul spare no one" and the key pattern is:

$1 \rightarrow 4,\ 2 \rightarrow 8,\ 3 \rightarrow 1,\ 4 \rightarrow 5,\ 5 \rightarrow 7,\ 6 \rightarrow 2,\ 7 \rightarrow 6$ and $8 \rightarrow 3$. 7

3. (a) Write down the working of RC4 algorithm. Take an example to support your answer. 7

(b) Define AES. Enlist the key difference in the working mechanisms of AES and DES. 7

4. (a) Explain the Diffie-Hellman key exchange algorithm with the help of a suitable example. 7

(b) Using RSA algorithm find the pair of public key and private key when, p=7, q=13 and e=5. Also encrypt the message M=10.

5. (a) What do you mean by a Cryptographic Hash function? Give an example to show how it works. 7

(b) What is the importance of passwords in providing security? What are the basic things that should be kept in mind while creating a Password? 7

(a) What is Biometrics? Give a real world example of how Biometrics is used as a method of authentication. 7

(b) How does the Two-Factor authentication work? Is it secure? Justify your statement. 7

7. (a) Draw an Access Control Matrix for an Organization. Describe how it can be used to derive ACLs and C-lists. 7

(b) Encipher the plaintext "ITS COOL" using affine cipher technique when encipherment function is E(x) = (5x + 8) MOD 26. 7

8. (a) What do you mean by a Malware ? Define the different categories of Malwares and how they work. 7

(b) What are the three security functions that an OS should deal with? How does the OS deal with these issues? 7

9. Write short notes on the following: 7×2

(a) Fiestel Cipher

(b) Salami Attack

***