Kadi Sarva Vishwavidhyalaya

M.E. Sem – I

Subject : Information and Network Security

Date : 21st January, 2013 Max. Marks : 70

Time : 3 Hours

Instruction : (1) Answer each section in separate Answer sheet

(2) No calculator is permitted.

Section – I

Q.1 Each carries equal marks **[15]**

[A] Draw and explain the basic model of network Security

[B] Explain in short the following :

1. Security Attack
2. Encryption

[C] Differentiate between following :

1. Symmetric and Asymmetric Cryptography
2. Stream Cipher and Block Cipher

OR

[C] Assume that n is a nonnegative integer

1. Find gcd(2n+1,n)
2. Find gcd(3n+1, 2n+1)

Q.2 **[10]**

[A] Find the inverses in Z_m of the following elements a modulo m:

(1) a = 7, m = 26 (2) a = 19, m = 999

[B] Using the basic form of Euclid's algorithm, compute the greatest common divisor of

(1) 7469 and 2464 (2) 2689 and 4001

OR

Q.2 **[10]**

[A] Find the orders of all elements in the following group

1. $G = <Z_8,+>$ 2. $G=<Z_7^*,*>$

[B] Using Chinese Remainder Theorem solve following

x = 2 (mod 3) ; x = 3 (mod 5); x = 2 (mod 7)

Q.3 **[10]**

[A] Use a Hill cipher to encipher the message "India is a great nation". Use the following key. $K = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$

[B] Explain Digital Signature. How it can provide source authentication. What should one do, if he wants to provide confidentiality also?

OR

Q.3 **[10]**

[A] Draw the structure of a single round of DES Algorithm

[B] Let the two primes p = 41 and q = 17 be given as set-up parameters for RSA. Which of the parameters e1 = 32, e2 = 49 is a valid RSA exponent? Justify your choice.

SECTION – II

Q.4 Each carries equal marks **[15]**

[A] What is a message authentication code?

[B]
1. Whether a MAC function based on Symmetric Encryption can provide Digital Signature? Why?
2. Differentiate Enveloped Data and Clear Signed data in S/MIME

[C] Users A and B use the Diffie – Hellman key exchange technique with a common prime q=11 and a primitive root $\alpha = 2$.
1. If user A has public key $Y_A = 9$, what is A's private key Y_A?
2. If user B has a public key $Y_B = 3$, what is the shared secret key between A and B?

OR

[C] How the Man-in-the middle attack is possible in Diffie-Hellman Key exchange protocol.

Q.5 **[10]**

[A] Explain the Kerberos protocol with appropriate figure.

[B] Which are the classes of functions that may be used to produce an authenticator?

OR

Q.5 **[10]**

[A] Draw and Explain the Data Authentication Algorithm based on DES

[B] Describe the properties of a secure Hash function.

Q.6 **[10]**

[A] See the following code :

```
int main() {
  int result;
  .....
 result = fact(5);
.... }
```

```
int fact(int a) {
 int temp;
..... }
```

Show the contents of memory stack when the fact function is called from main method. Also specify the offset of variables *a* and *temp* with respect to new EBP.

[B] Explain TCP SYN flooding attack.

OR

Q.6 **[10]**

[A]
- When a function is executed, which information is stored on the stack?
- While a function is executed, the arguments and variables stored on the stack are accessed by using EBP (Extended Base Pointer) as a fixed reference point instead of ESP (Extended Stack Pointer). Why?

[B] Explain ARP cache poisoning.

**********Best of Luck **********