VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering
A1 + TA1-Slot CAT-II (Mar -2018)
Subject: Cybersecurity – CSE4003

Time: 1 Hr 30 Mins **Max.Marks:50**

Answer ALL questions
(5 X 10 = 50 marks)

1. (a) In an RSA digital signature scheme, Bob signs messages x_i and sends them together with the signatures s_i and her public key to Alice. Bob's public key is the pair *(n,e)*; her private key is *d*. Oscar can perform man-in-the-middle attacks, i.e., he can replace Bob's public key by his own on the channel. His goal is to alter messages and provide these with a digital signature which will check out correctly on Alice's side. Show everything that Oscar must do for a successful attack. [5M]

(b) With DSS (Digital Signature Scheme), because the value of *k* is generated for each signature, even if the same message is signed twice on different occasions, the signatures will differ. This is not true of RSA signatures. What is the practical implication of this difference? [5M]

2. (a) An early proposal for a digital signature scheme using symmetric encryption is based [7M]
on the following: To sign an n-bit message, the sender randomly generates in advance 2n 56-bit cryptographic keys: *k1, K1, k2, K2,..., kn, Kn* which are kept secret. The sender prepares in advance two sets of corresponding nonsecret 64-bit validation parameters, which are made public: *u1, V1, u2, V2,..., un, Vn* and *v1, V1, v2, V2,..., vn, Vn,* where *vi = E(ki, ui), Vi = E(ki, Ui)*. The message *M* is signed as follows. For the i th bit of the message, either ki or Ki is attached to the message, depending on whether the message bit is 0 or 1. For example, if the first three bits of the message are 011, then the first three keys of the signature are *K1, K2, K3*.
(a). How does the receiver validate the message?
(b). Is the technique secure?
(c). How many times can the same set of secret keys be safely used for different messages?
(d). What, if any, practical problems does this scheme present?

(b) In the Diffie Hellman key exchange, the private keys are chosen from the set *{2,..., p−2}*. Why are the values 1 and p − 1 excluded? Describe the weakness of these two values. [3M]

3. (a) Given is an Elgamal signature scheme with $p = 31$, $\alpha = 3$ and $\beta = 6$. You receive the message $x=10$ twice with the signatures (r,s): **[5M]**

(i) *(17,5)* (ii) *(13,15)*

(a). Are both signatures valid?

(b). How many valid signatures are there for each message x and the specific parameters chosen above?

(b) Encrypt the following messages with the Elgamal scheme ($p = 467$ and $\alpha = 2$) **[5M]**

1. $k_{pr} = d = 105, i=213, x=33$
2. $k_{pr} = d = 105, i=123, x=33$

Decrypt every ciphertext and show all steps

4. (a) Compute the output of the first round of stage 1 of SHA-1 for a 512-bit input block of **[6M]**

1. *x={0...00}*
2. *x={0...01}(i.e., bit 512 is one).*

Ignore the initial hash value H0 for this problem (i.e., A0 =B0 =...=00000000hex).

(b) Show that the condition $4a^3+27b^2 \neq 0 \bmod p$ is fulfilled for the curve $y^2 \equiv x^3+2x+2 \bmod 17$ **[2M]**

(c) Is *(4,7)* a point on the elliptic curve $y^2 = x^3 + 5x + 5$ over real numbers **[2M]**

5. Explain the below concept by stating a real time example?

(a) Denial of service
(b) Phishing
(c) Virus dissemination
(d) Computer vandalism
(e) Cyber terrorism

30 × 30

a30

VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

A1

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
Continuous Assessment Test - I, Jan 2018
B.Tech, Winter Semester, 2017-18

Course Code	: CSE4003		**Duration**	: 90 Minutes
Course Name	: Cyber Security		**Max. Marks**	: 50

Answer **All** Questions 5 x 10 = 50 Marks

1. A) Using Euclidean algorithm, the GCD(a,b)=GCD(?) (1)

   B) Find GCD(2740,1740) (3)

   C) (12432+23432)mod 9 = ? (2)

   D) Find multiplicative inverse of 8 in Z_{10} using extended Euclidean algorithm (4)

2. A) Using Fermat's theorem, check whether 19 is prime or not?. Consider a is 7. (4)

   B) Using Miller-Robin theorem, check whether 29 is prime or not? Consider a is 10 (6)

3. A) Alice and Bob are securely communicating using RSA Algorithm. Alice generates two prime keys 11, 13 and sends a message M (simply, a "I") to Bob. Explains the generation of public key and private key, the process of encryption and decryption in the RSA based secure communication. (6)

   B) Draw functional diagram and briefly explain: Round operation in IDEA (4)

4. A) In DES, what is the output of IP function, if the hexadecimal message is "5faf3e2c1234abcd"? The IP is shown below: (6)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

'c|0|.0 1 0

0

143)16387(
143
208
143
654

(740)1000(1
740
260

10
11
1 →
26

   B) Draw round function in DES with no of bits on each process. (4)

5. A) Explain with sample data: Four transformations in AES (8)

   B) In finite field arithmetic, $(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = ?$ (2)

1740)2740(1
1740

(12891

Scanned by CamScanner