VIT UNIVERSITY
(Estd. u/s 3 of UGC Act 1956)
VELLORE • CHENNAI
www.vit.ac.in

School of Computer Science and Engineering
F1-Slot CAT-II (Oct -2017)
B.Tech (CSE, BCB, BCI)-III Semester
Subject: Cryptography Fundamentals – CSE1011

Faculty(s) Name: Dr.M.Anand / Dr.K.Marimuthu

Time: 1 Hr 30 Mins Max.Marks:50

Answer ALL questions
(5 X 10 = 50 marks)

1. (a) Let the two primes $p = 41$ and $q = 17$ be given as set-up parameters for RSA. [5]
(a) Which of the parameters $e1 = 32$, $e2 = 49$ is a valid RSA exponent? Justify your choice.
(b) Compute the corresponding private key $Kpr = (p,q,d)$

(b) 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. [5]
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?

2. (a) Compute the two public keys and the common key for the DHKE (Deffie Hellman Key Exchange) scheme with the parameters $p = 467$, $\alpha = 2$, and [5]
(1) $a = 3$, $b = 5$
(2) $a = 400$, $b = 134$
(3) $a = 228$, $b = 57$
In all cases, perform the computation of the common key for Alice and Bob.

(b) In the Diffie-Hellman protocol, each participant selects a secret number x and sends the other participant $\alpha^x \bmod q$ for some public number α. What would happen if the participants sent each other x^{α} for some public number α instead? Give at least one method Alice and Bob could use to agree on a key. Can Eve break your system without finding the secret numbers? Can Eve find the secret numbers? [5]

3. (a) Given an RSA signature scheme with the public key ($n = 9797, e = 131$), which of the following signatures are valid? [5]
(1) ($x = 123$, $sig(x) = 6292$)
(2) ($x = 4333$, $sig(x) = 4768$)
(3) ($x = 4333$, $sig(x) = 1424$)

(b) 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. [5]

4. (a) Compute the output of the first round of stage 1 of SHA-1 for a 512-bit input block of [5]

(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) Draw a block diagram for the following hash functions built from a block cipher $e()$: [5]

(1) $e(H_{i-1}, x_i) \oplus x_i$

(2) $e(x_i, x_i \oplus H_{i-1}) \oplus x_i \oplus H_{i-1}$

(3) $e(x_i, H_{i-1}) \oplus x_i \oplus H_{i-1}$

(4) $e(x_i, x_i \oplus H_{i-1}) \oplus H_{i-1}$

(5) $e(x_i \oplus H_{i-1}, x_i) \oplus x_i$

5. Now consider the opposite problem: using an encryption algorithm to construct a oneway hash function. Consider using RSA with a known key. Then process a message consisting of a sequence of blocks as follows: Encrypt the first block, XOR the result with the second block and encrypt again, etc. Show that this scheme is not secure by solving the following problem. Given a two-block message ***B1***, ***B2***, and its hash

$$RSAH(B1, B2) = RSA(RSA(B1) \oplus B2)$$

Given an arbitrary block ***C1***, choose ***C2*** so *that* $RSAH(C1, C2) = RSAH(B1, B2)$. Thus, the hash function does not satisfy weak collision resistance.