DHARMSINH DESAI UNIVERSITY, NADIAD
FACULTY OF TECHNOLOGY
B.TECH. SEMESTER V [INFORMATION TECHNOLOGY]
SUBJECT: E- COMMERCE & E-SECURITY

Examination	**: Second Sessional**	**Seat No.**	**: _____**
Date	**: 04/09/2017**	**Day**	**: Monday**
Time	**: 1:15 to 2:30**	**Max. Marks**	**: 36**

INSTRUCTIONS:
1. Figures to the right indicate maximum marks for that question.
2. The symbols used carry their usual meanings.
3. Assume suitable data, if required & mention them clearly.
4. Draw neat sketches wherever necessary.

Q.1 Do as directed.(No Marks Without Justification)

(a) Let (PUa, PRa) are the public and private key of Alice, and (PUb, PRb) are the public & private key of Bob. Let H() be a hash function, E(Key, Data) denote an encryption,& D(Key, Data) decryption operation, || denote a concatenation and Doc be a document. The digital signature algorithm performed by Alice on the document Doc can be described as: **[2]**

I. Send: Doc || E(PUa, H(Doc)) II. Send: Doc || E(PUb, H(Doc))
III. Send: Doc || D(PRb, H(Doc)) IV. Send: Doc || D(PRa, H(Doc))
V. Send: Doc || E(PRb, H(Doc))

(b) Let C(Key, M) denote a message authentication code function, produced for the message M and a shared key Key. Let E(Key, M) denote encryption of a message M with a key Key, and let || denote the concatenation. If Alice send to Bob the following information: **[2]**

E(K2, M) || C(K1, E(K2, M)) where K1 and K2 are shared secret keys, then it is

I) Just a message authentication.

II) Message authentication and confidentiality where authentication is tied to the Plaintext.

III) Message authentication and confidentiality where authentication is tied to the Ciphertext.

IV) Just a message confidentiality.

V) Message authentication and confidentiality where authentication is tied both to the plaintext and to the ciphertext.

(c) If we have a hash function with a digest size of n bits, with the birthday paradox attack approximately how much hash operations we need in order to find a collision? **[2]**

I) $2^{n/2}$ (II) 2n (III) 2^n (IV) 2^{n-1} (V) n^n

(d) List different ways of distribution of public key. **[2]**

(e) Differentiate: Direct Digital Signature and Arbitrated Digital Signature. **[2]**

(f) How cryptography is different than message digest, explain with appropriate example. **[2]**

Q.2 Attempt ***Any Two*** from the following questions.

(a) Write an algorithm of RSA and compute Cipher text using following data p=11, q=13 e=11 and M=7 **[6]**

(b) Write a key distribution scenario using public key authority with proper figure. **[6]**

(c) Compute 82^{29} MOD 91 by Modular Exponentiation Algorithm. **[6]**

Q.3 (a) Consider a Diffie-Hellman scheme with common prime q=11 and a primitive root $\alpha = 2$. **[6]**

(I) Show that 2 is a primitive root of 11.

(ii) If a user A has a public key 9, What is A's private key?

(iii) If user B has public key 3, what is the shared secret key?

(b) Explain message digest algorithm which generate 160 bits of message digest with Proper figure. **[6]**

OR

Q.3 (a) Explain Arbitrated digital signature techniques. **[6]**

(b) Explain Hash Function which uses four 32 bit buffer registers for generating message digest with proper figure. **[6]**