DHARMSINH DESAI UNIVERSITY, NADIAD
FACULTY OF TECHNOLOGY
B.TECH. SEMESTER V [INFORMATION TECHNOLOGY]
SUBJECT: E- COMMERCE & E-SECURITY [IT-718]

Examination	**: Second Sessional**	**Seat No.**	**: _____**
Date	**: 03/09/2019**	**Day**	**: Tuesday**
Time	**: 1:45 to 3:00 pm**	**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.

(a) To authenticate the data origin, one needs a **[1]**
(A) Message Detection Code **(B)** Message Authentication Code
(C) Both (A) or (B) **(D)** Neither (A) nor (B)

(b) Hash function is a function which usually takes an arbitrary size of data and **[1]**
(A) creates a small flexible size of data. **(B)** creates a small, fixed size of data.
(C) creates a permutation on input data. **(D)** none of the mentioned

(c) Certification authority issues the digital certificate which must include **[1]**
(A) the signer's private key and identity **(B)** the signer's public key and identity
(C) the certificate authority's private key **(D)** a certificate revocation list

(d) Which property indicates that it must be extremely difficult to create the message if the message digest is given **[1]**
(A) one-wayness **(B)** Weak collision resistance
(C) Strong collision resistance **(D)** none of the above

(e) On which property of Hash function, Birthday attack is mounted? **[1]**

(f) What is one way function? **[1]**

(g) How many number of keys required for a set of n individuals to be able to communicate with each other using secret key and public key crypto-systems respectively? **[2]**

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

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

Q.2 Attempt from the following questions.

(a) Anil and Shiv agreed on two global elements p=23 and g=5 where p is common prime and g is primitive root. **[6]**
(1) Anil shared its public key 8, What is the private key of Anil?
(2) Shiv chooses private key 15, Which key he will share with Anil?
(3) What will be the shared secret key calculated independently by Anil and Shiv, state whether both are equal or not.

(b) Draw and explain a public key distribution scenario using certificate authority. **[6]**

OR

(b) Explain SHA-1 algorithm with proper steps and diagram. **[6]**

Q.3 (a) Seema publishes her RSA public key as: {11,221}.

(1) Compute the Private Key of Seema. **[2]**

(2) Anjana Wants to send message M = 15 to Seema. What ciphertext does Anjana send to Seema? **[3]**

(3) How does Seema retrieve the original message from encrypted message? Show calculations. **[3]**

(b) Explain types of attacks possible in RSA along with its counter measures. **[4]**

OR

(b) Draw and explain HMAC algorithm. **[4]**
