DHARMSINH DESAI UNIVERSITY, NADIAD
FACULTY OF TECHNOLOGY
B.TECH. SEMESTER V [INFORMATION TECHNOLOGY]
SUBJECT: E- COMMERCE & E-SECURITY [IT-710]

Examination	**: Second Sessional**	**Seat No.**	**: _____**
Date	**: 04/09/2018**	**Day**	**: Tuesday**
Time	**: 2:30 – 3:45**	**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) What is one way function? **[1]**
(b) What are three broad categories of applications of public key cryptosystem? **[1]**
(c) What is factoring problem in RSA? **[1]**
(d) What is timing attack in RSA? **[1]**
(e) What are the approaches to produce message authentication? **[2]**
(g) Define: (1) weak collision resistance (2) Strong Collision resistance **[2]**
(h) Differentiate : MD5 Vs SHA1 **[2]**
(i) List four general categories of schemes for the distribution of public keys. **[2]**

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

(a) Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 73 and a primitive root α = 7. **[6]**
   a. If user A has private key X = 5, what is A's public key ?
   b. If user B has private key X = 12, what is B's public key ?
   c. What is the shared secret key?
(b) Draw and explain Secret key distribution scenario with confidentiality and authentication. **[6]**
(c) Explain Hash Function which produces 160 bits message digest with proper figure. **[6]**

Q.3 (a) Write Fast exponentiation algorithm and use the algorithm to determine 5^596 mod 1234. Show the steps involved in the computation. **[8]**
(b) Draw and explain HMAC structure. **[4]**

OR

Q.3 (a) Consider following scheme: **[8]**
   1. pick an odd number
   2. Pick two prime numbers, P and Q, where (P-1)(Q-1) - 1 is evenly divisible by E.
   3. Multiply P and Q to get N.
   4. calculate D=((P-1)(Q-1)(E-1) + 1) / E
   Is this scheme is equivalent to RSA ? with example Show why or why not.
(b) Draw and explain compression function of MD5. **[4]**
