Examination	: Block Exam	Seat No.	:
Date	: 17/10/2013	Day	: Thursday
Time	: 11:00 TO 12:15	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) Explain di-gram and what is its important.   [2]
   (b) If user A1 is registered under X11 C.A. and user B1 registered under X21 C.A. then   [2]
        how both can communicate?
   (c) Compare traditional cryptosystem with public key cryptosystem.   [2]
   (d) Explain difference between tunnel mode and transport mode?   [2]
   (e) What is difference between message digest and encryption   [2]
   (f) Write Difference between application firewall and packet filtering firewall.   [2]

Q.2   Attempt *Any Two* from the following questions.
   (a) Explain Secure Electronic Transaction where how processing is done at customer-side   [6]
        and merchant side.
   (b) Calculate RSA public key and private key for p=3 and q=7 e=11   [6]
   (c) Explain key generation of s-des.   [6]

Q.3   Attempt following questions.
   (a) Explain ANSI X9.17 PRN generator with proper figure.   [6]
   (b) Explain MD 5 Message digest with appropriate figure   [6]
                                    OR
Q.3   Attempt following questions.
   (a) Draw X.509 certificate format and explain each field of certificate   [6]
   (b) Explain Deffie-hellman algorithm with its importance   [6]