Quiz-I Cryptography Max Time 10 Mins

Max Marks 10 ME Information Security

All questions carry Single Mark and have single answer.

Q1. A Known Popular Attack on PKCS1 v1.5 is known as

a) Timing Attack
b) Bleichenbacher Attack
c) Replay Attack
d) Eavesdropping Attack

Q2. In PKCS1 v 2.0 OAEP construction we should use the following for H and G

a) SHA-128
b) SHA-256
c) SHA-512
d) SHA-64

Q3. For Public Key Encryption One Time Security implies many time security.

a) True
b) False
c) Depending upon the application area
d) depends upon the security attack

Q4. Trapdoor Function is a triple of

a) $(G,F,F^{-1})$
b) (G,E,D)
c) (G,Sk,Pk)
d) (K,M,C)

Q5. Write the set $Z_{14}^*$

Q6. $7^{1/3}$ in $Z_{11}$ is

a) 4
b)5
c)6
d)7

Q7. Order of 2 in $Z_7$ is

a) 6
b) 4
c) 2
d) 3

Q8. What is G() in Public Key Encryption triple (G,E,D) One line only

Q9. What is the best known algorithm for Diffie Hellman Function mod p

a) OAEP
b) GNFS
c) TTP
d) SAEP

Q10. Write Fermat Theorem (One line Only)