Motilal Nehru National Institute of Technology Allahabad
Department of Computer Science & Engineering
End Semester Examination 2017-18
Cryptography (CS1506), B.Tech (CS/IT) – 5th Sem

Duration- 03 Hours. **Max Marks: 60**

Note: All questions are compulsory. State assumptions very clearly.

1. (a) Draw a detailed structure of an X.509 certificate. Also, discuss the fields used in X.509 certificate. (3)
(b) Write an elaborative note on Certificate revocation list. (3)

2. (a) Explain all steps of the Elliptic Curve Digital Signature Algorithm (ECDSA) with a neat diagram with correctness. (3)
(b) Elaborate all properties of Message Authentication Codes. (3)

3. (a) Explain Diffie- Hellman Key exchange between Alice and Bob. Show, how Man in the middle attack performed in between by Oscar, and Message manipulation after Man in the middle attack. Show all three parts in separate elaborative diagram. (3)
(b) Compute a session key in a Diffie- Hellman Key exchange (DHKE) protocol based on elliptic curves. Your private key is a = 6. You receive Bob's public key B = (5, 9). The elliptic curve being used is defined by $y^2 \equiv x^3+x+6 \bmod 11$. (3)

4. What is hashing? What are the properties of cryptographic hash function? Compare MD5, SHA1, and SHA 2 and its variants, with respect to Input and output bits, number of rounds and other relevant parameter. Prefer to draw a table for comparison. (6)

5. Compare the RSA signature scheme with the Elgamal signature scheme. What are their relative advantages and drawbacks? (6)

6. (a) What is the difference between diffusion and confusion? Also, name the operations which are part of diffusion in AES. (3)
(b) Show how Digital Signature Algorithm (DSA) can be attacked if the same ephemeral key is used to sign two different messages. (3)

7. Show that the condition $4a^3+27b^2 = 0 \bmod p$ is fulfilled for the curve $y^2 \equiv x^3+2x+2 \bmod 17$. If this is true then calculate the order of the curve by using Hasse's theorem. (6)

8. Given is an Elgamal signature scheme with p = 31, α = 3 and β = 6. You receive the message x = 10 twice with the signatures (r, s): (3+3=6)
(i) (17, 5) (ii) (13,15)
a.) Are both signatures valid?
b.) How many valid signatures are there for each message x and the specific parameters chosen above?

9. Imagine a peer-to-peer network where 1000 users want to communicate in an authenticated and confidential way without a central Trusted Third Party (TTP). (3+3=6)
a. How many keys are collectively needed, if symmetric algorithms are deployed?
b. How these numbers are changed, if we bring in a central instance (Key Distribution Center, KDC)?

P.T.O

10. We consider RSA encryption with certificates in which Bob has the RSA keys. Oscar manages to send Alice a verification key $k_{pr,CA}$ which is, in fact, Oscar's key. Show an active attack by which he can decipher encrypted messages that Alice sends to Bob. Should Oscar run a man in the middle attack or should he set up a session only between himself and Alice? **(6)**