Name: Student ID:

Information Security, Fall 2016

Homework #3: Part 2 Asymmetric Ciphers, Part 3 Cryptographic Data Integrity Algorithms, Part 4 Mutual Trust (Graded out of 10 points)

Due: 1/3, Tuesday(End of the class)

1. Alice and Bob use the Diffie-Hellman key exchange technique with a common prime *q = 23* and a primitive root *α = 5*.
(a) If bob has a public key $Y_B = 10$, what is Bob's private key X_B?
(b) If Alice has a public key $Y_A = 8$, what is the shared key *K* with Bob?
(c) Show that 5 is a primitive root of 23.

2. Section 10.1 describes a man-in-the-middle attack on the Diffie-Hellman key exchange protocol in which the adversary generates two public–private key pairs for the attack. Could the same attack be accomplished with one pair? Explain.

3. On the elliptic curve over the real numbers $y^2 = x^3 - 36x$, let P = (-3.5, 9.5) and Q = (-2.5, 8.5). Assume a = -36. Find:
(a) P + Q
(b) 2P

4. Calculate the hash function $h = \left(\sum_{i=1}^{t}(a_i)^2\right) mod\ n$ for *M = (189, 632, 900, 722, 349)* and *n = 989*.

5. What are some approaches to producing message authentication?

6. List two disputes that can arise in the context of message authentication.
(a) from sender's aspect:
(b) from receiver's aspect:

7. Assume the sender A and the receiver B are using Elgamal digital signature scheme in their messages. Please specify the formulas in the following steps and calculate the values.

(a) A select q = 19, α = 3, generate a random integer X_A = 16. Then what is the public key and private key pair of A?

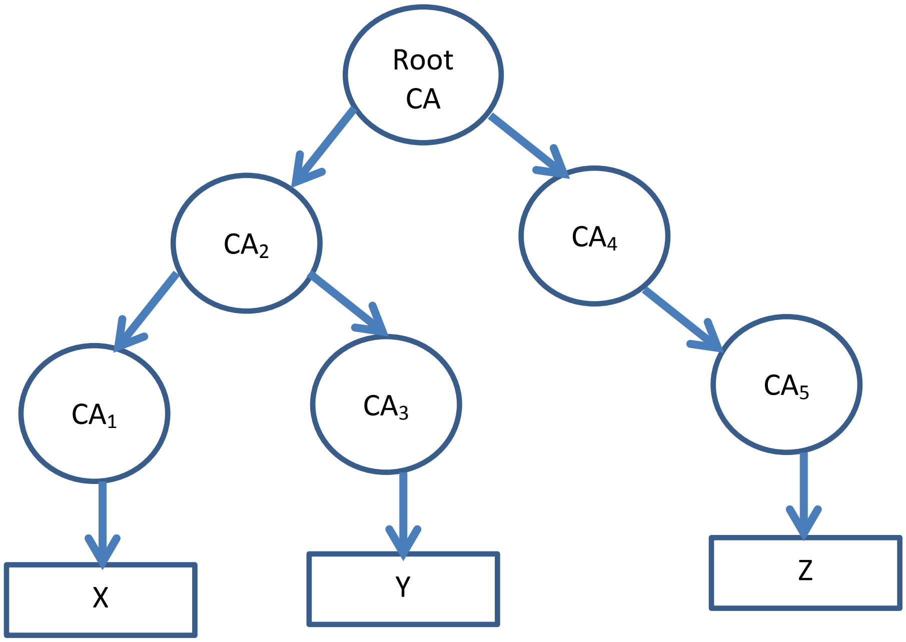
To sign a message M, A computes the hash m = H(M) = 14. A then forms a digital signature as follows.

(b) A choose a random integer K = 5, then what are the values of signature pair (S_1 , S_2) generated from A?

(c) How can B verify the signature? And what are the values of V_1 and V_2?

8. What is a public-key certificate?

9. Show how user Y establishes a certification path to Z.



10. In what order should the signature function and the confidentiality function be applied to a message, and why?