Information Security
Midterm Exam – Part II

1. **(8 points)** In a public key system using RSA.
   (a) You intercept a ciphertext C = 15 sent to a user whose public key is (n = 91, e = 13). What is the plaintext M?
   (b) If the public key of a given user is (n, e) where n = 3599 and e is selected to be the smallest among all legitimate numbers to minimize the encryption complexity, what is the private key of this user?
2. **(6 points)** Please prove in detail why the RSA method works as showed in the class.
3. **(6 points)** Please compare the 4 public key distribution methods discussed in the class.
4. **(6 points)** Consider the Diffie-Hellman key exchange algorithm with a common prime 997 and its smallest primitive root.
   (a) If user A has public key Y_A = 1, what is A's private key X_A?
   (b) If user B has public key Y_B = 97, what is the shared secret key K that A calculates?
5. **(6 points)** Please answer the following questions.
   (a) Describe the principle of the probabilistic primality test discussed in the class.
   (b) Find the smallest nonnegative integer i that satisfies $3^i \equiv 7 \bmod 11$.
   (c) Calculate the multiplicative inverse modulo 35 of 11 using (1) the Euler's theorem and (2) the Euclid's algorithm, respectively.
6. **(4 points)** For a number n that is the product of two prime numbers p and q, if $\phi(n)$ (Euler totient function) is known to be 460, please find p and q.
7. **(14 points)** Consider the elliptic group $E_{23}(2,2)$ of 19 solutions, where G = (3,9) and B's private key is n_B = 12. Assume that the following results are known: 2G = (12,11), 4G = (8,1), 8G = (9,17), 16G = (8,22) and 32G = (9,6).
   (a) **(2 points)** Please show that (2,2) is a valid choice for (a,b) to form a legitimate elliptic group.
   (b) **(4 points)** What is the smallest n such that $nG = O$? (Hint: An efficient way is possible from a direct observation on the given results.) If another result 10G = (6,0) is also given, can you find another efficient way to calculate n? In addition, is G = (6,0) a good choice and why?
   (c) **(2 points)** Find B's public key P_B.
   (d) **(2 points)** If A wishes to exchange a secret key with B using this ECC system and choosing his/her private key as n_A = 3, what will be the secret key that A and B exchange?
   (e) **(2 points)** A wishes to encrypt the message P_m = (8,1) and chooses the random value k = 2. Determine the ciphertext C_m.
   (f) **(2 points)** Show the detailed calculation by which B recovers P_m from C_m.
   Hint: If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ with $P \neq -Q$, then $P + Q = (x_3, y_3)$ is determined by the following rules:

$$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod{p}$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod{p}$$

where

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } P = Q \end{cases}$$