Elliptic Curve Cryptography Problems

V. Balasubramanian
SSN College of Engineering

Q&A

- Explain Diffie-Hellman key exchange?
- What is the sum of three points on an elliptic curve that lie on a straight line?

- Two parties each create a public-key, private-key pair and communicate the public key to the other party. The keys are designed in such a way that both sides can calculate the same unique secret key based on each side's private key and the other side's public key.

- If three points on an elliptic curve lie on a straight line, their sum is O

Users A and B use the Diffie-Hellman key exchange technique with a common prime $q = 71$ and a primitive root $\alpha = 7$.

a. If user A has private key $X_A = 5$, what is A's public key Y_A?

b. If user B has private key $X_B = 12$, what is B's public key Y_B?

c. What is the shared secret key?

a. $Y_A = 7^5 \bmod 71 = 51$

b. $Y_B = 7^{12} \bmod 71 = 4$

c. $K = 4^5 \bmod 71 = 30$

Consider a Diffie-Hellman scheme with a common prime $q = 11$ and a primitive root $\alpha = 2$.

a. Show that 2 is a primitive root of 11.
b. If user A has public key $Y_A = 9$, what is A's private key X_A?
c. If user B has public key $Y_B = 3$, what is the secret key K shared with A?

a. $\phi(11) = 10$
$2^{10} = 1024 = 1 \bmod 11$
If you check 2^n for $n < 10$, you will find that none of the values is 1 mod 11.

b. 6, because $2^6 \bmod 11 = 9$

c. $K = 3^6 \bmod 11 = 3$

Bob:	Oh, let's not bother with the prime in the Diffie-Hellman protocol, it will make things easier.
Alice:	Okay, but we still need a base α to raise things to. How about $\alpha = 3$?
Bob:	All right, then my result is 27.
Alice:	And mine is 243.

What is Bob's private key X_B and Alice's private key X_A? What is their secret combined key? (Don't forget to show your work.)

$x_B = 3$, $x_A = 5$, the secret combined key is $(3^3)^5 = 3^{15} = 14348907$.

Is (4, 7) a point on the elliptic curve $y^2 = x^3 - 5x + 5$ over real numbers?

Yes, since the equation holds true for $x = 4$ and $y = 7$:

$$7^2 = 4^3 - 5(4) + 5$$

$$49 = 64 - 20 + 5 = 49$$

Does the elliptic curve equation $y^2 = x^3 + 10x + 5$ define a group over Z_{17}?

$(4a^3 + 27b^2) \bmod p = 4(10)^3 + 27(5)^2 \bmod 17 = 4675 \bmod 17 = 0$

This elliptic curve does not satisfy the condition of Equation (10.6) and therefore does not define a group over Z_{17}.

What are the negatives of the following elliptic curve points over Z_{17}? P = (5, 8); Q = (3, 0); R = (0, 6).

The negative of a point $P = (x_P, y_P)$ is the point $-P = (x_P, -y_P \bmod p)$.
Thus

$$-P = (5,9);\ -Q = (3,0);\ -R = (0,11)$$

For $E_{11}(1, 6)$, consider the point $G = (2, 7)$. Compute the multiples of G from $2G$ through $13G$.

We follow the rules of addition described in Section 10.4. To compute $2G = (2, 7) + (2, 7)$, we first compute

$$\lambda = (3 \times 2^2 + 1)/(2 \times 7) \bmod 11$$
$$= 13/14 \bmod 11 = 2/3 \bmod 11 = 8$$

Then we have

$$x_3 = 8^2 - 2 - 2 \bmod 11 = 5$$
$$y_3 = 8(2 - 5) - 7 \bmod 11 = 2$$
$$2G = (5, 2)$$

Similarly, $3G = 2G + G$, and so on. The result:

2G = (5, 2)	3G = (8, 3)	4G = (10, 2)	5G = (3, 6)
6G = (7, 9)	7G = (7, 2)	8G = (3, 5)	9G = (10, 9)
10G = (8, 8)	11G = (5, 9)	12G = (2, 4)	13G = (2, 7)

This problem performs elliptic curve encryption/decryption using the scheme outlined in Section 10.4. The cryptosystem parameters are $E_{11}(1, 6)$ and $G = (2, 7)$. B's private key is $n_B = 7$.

a. Find B's public key P_B.

b. A wishes to encrypt the message $P_m = (10, 9)$ and chooses the random value $k = 3$. Determine the ciphertext C_m.

c. Show the calculation by which B recovers P_m from C_m.

a. $P_B = n_B \times G = 7 \times (2, 7) = (7, 2)$. This answer is seen in the preceding table.

b. $C_m = \{kG, P_m + kP_B\}$

$= \{3(2, 7), (10, 9) + 3(7, 2)\} = \{(8,3), (10, 9) + (3, 5)\} = \{(8, 3), (10, 2)\}$

c. $P_m = (10, 2) - 7(8, 3) = (10, 2) - (3, 5) = (10, 2) + (3, 6) = (10, 9)$

True or False

- 1. The Diffie-Hellman key exchange is a simple public-key
- algorithm.

- 2. The security of ElGamal is based on the difficulty of
- computing discrete logarithms.

- 3. For purposes of ECC, elliptic curve arithmetic involves
- the use of an elliptic curve equation defined over an
- infinite field.

- 4. The Diffie-Hellman algorithm depends on the difficulty of
- computing discrete logarithms for its effectiveness.

- 5. There is not a computational advantage to using ECC
- with a shorter key length than a comparably secure TSA.

- T
- T
- F
- T
- F

- 6. Most of the products and standards that use public-key
- cryptography for encryption and digital signatures use RSA.
-
- 7. ECC is fundamentally easier to explain than either RSA or
- Diffie-Hellman.
-
- 8. A number of public-key ciphers are based on the use of
- an abelian group.
-
- 9. Elliptic curves are ellipses.
-
- 10. For determining the security of various elliptic curve
- ciphers it is of some interest to know the number of
- points in a finite abelian group defined over an elliptic
- curve.

- T
- F
- T
- F
- T

- 11. The form of cubic equation appropriate for cryptographic applications for elliptic curves is somewhat different for GF(2m) than for Zp.
-
- 12. An encryption/decryption system requires that point Pm be encrypted as a plaintext.
-
- 13. The security of ECC depends on how difficult it is to determine k given kP and P.
-
- 14. A considerably larger key size can be used for ECC compared to RSA.
-
- 15. Since a symmetric block cipher produces an apparently random output it can serve as the basis of a pseudorandom number generator.

- T
- F
- T
- F
- T

- The _____________ protocol enables two users to establish a secret key using a public-key scheme based on discrete logarithms.
-
- A. Micali-Schnorr B. Elgamal-Fraiser
-
- C. Diffie-Hellman D. Miller-Rabin
-

- ___________ can be used to develop a variety of elliptic curve cryptography schemes.
-
- A. Elliptic curve arithmetic B. Binary curve
-
- C. Prime curve D. Cubic equation
-

- The key exchange protocol is vulnerable to a ___________ attack because it does not authenticate the participants.
-
- A. one-way function B. time complexity
-
- C. chosen ciphertext D. man-in-the-middle

- The ___________ cryptosystem is used in some form in a number of standards including DSS and S/MIME.
-
- A. Rabin B. Rijnedel
-
- C. Hillman D. ElGamal
-
- A(n) ___________ is defined by an equation in two variables with coefficients.
-
- A. abelian group B. binary curve
-
- C. cubic equation D. elliptic curve

- C
- A
- D
- D
- D

- ___________ are best for software applications.
-
- A. Binary curves B. Prime curves
-
- C. Bit operations D. Abelian groups
-
- An encryption/decryption system requires a point G and an elliptic group __________ as parameters.
-
- A. Eb(a,q) B. Ea(q,b)
-
- C. En(a,b) D. Eq(a,b)

- For cryptography the variables and coefficients are restricted to elements in a ___________ field.
-
- A. primitive B. infinite
- C. public D. Finite

- If three points on an elliptic curve lie on a straight line their sum is ___________ .
- A. 0 B. 1
- C. 6 D. 3

- ______________ makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field.
-
- A. Prime curve B. Elliptic curve cryptography(ECC)
-
- C. abelian group D. Micali-Schnorr
-

- B
- D
- D
- A
- B

- For a ____________ defined over GF(2m), the variables and coefficients all take on values in GF(2m) and in calculations are performed over GF(2m).
-
- A. cubic equation B. prime curve
- C. binary curve D. abelian group
-
-
- If a secret key is to be used as a __________ for conventional encryption a single number must be generated.
-
- A. discrete logarithm B. prime curve
- C. session key D. primitive root

- The Diffie-Hellman key exchange formula for calculation of a secret key by User A is:
- A. K = nB x PA   B. K = nA x PB
- C. K = nP x BA   D. K = nA x PA

- Included in the definition of an elliptic curve is a single element denoted O and called the point at infinity or the __________ .
-
- A. prime point   B. zero point
- C. abelian point   D. elliptic point

- The ___________ key exchange involves multiplying pairs of nonzero integers modulo a prime number q. Keys are generated by exponentiation over the group with exponentiation defined as repeated multiplication.
-
- A. Diffie-Hellman B. Rabin-Miller
- C. Micali-Schnorr D. ElGamal

- C
- C
- B
- B
- A

- Elliptic curve arithmetic can be used to develop a variety of elliptic curve cryptography schemes, including key exchange, encryption, and ____________ .
- The purpose of the ____________ algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages.

- The key exchange protocol vulnerability can be overcome with the use of digital signatures and ___________ certificates.
-
- The principal attraction of ___________, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.
-
- A(n) ____________ G is a set of elements with a binary operation, denoted by *, that associates to each ordered pair (a,b) of elements in G an element (a*b) in G.

- digital signature
- Diffie-Hellman key exchange
- public-key
- elliptic curve cryptography (ECC)
- abelian group

- Two families of elliptic curves are used in cryptographic applications: prime curves over Zp and ___________ over GF(2m).
-
- We use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through p - 1 and in which calculations are performed modulo p for a ___________ over Zp.
-
- A ___________ GF(2m) consists of 2m elements together with addition and multiplication operations that can be defined over polynomials.

- The addition operation in elliptic curve cryptography is the counterpart of modular multiplication in RSA, and multiple addition is the counterpart of ___________ .
-
- To form a cryptographic system using ___________ we need to find a "hard-problem" corresponding to factoring the product of two primes or taking the discrete logarithm.

- binary curves
- prime curve
- finite field
- modular exponentiation
- elliptic curves

- Eq(a,b) is an elliptic curve with parameters a, b, and q, where ____________ is a prime or an integer of the form 2m.
- The fastest known technique for taking the elliptic curve logarithm is known as the ____________ method.