OTHER PUBLIC-KEY CRYPTOSYSTEMS

March 24, 2009

Internetwork Security - EE548

- The ElGamal Cryptosystem is based on Discreate Logarithm problem
- The ElGamal Cryptosystem is non-deterministic, since the ciphertext depends on both the plaintext x and on the random value k chosen by encryptor. So there will be many ciphertexts that are encryptions of the same plaintext.

The discrete logarithm problem in Z_p

- **Problem Instance:** $I = (p, \alpha, \beta)$, where p is prime, $\alpha \in Z_p$ is a primitive element, and $\beta \in Z_p^*$.
- **Objective:** Find the unique integer a, $0 \leq a \leq p-2$, such that

$$\alpha^a \equiv \beta \pmod{p}.$$

We will denote this integer a by $\log_\alpha \beta$.

ElGamal Public-key Cryptosystem in Z_p^*

- Let p be a prime such that the discrete log problem in Z_p is intractable, and let $\alpha \in Z_p^*$ be a primitive element.
- Let $\mathcal{P} = Z_p^*$, $\mathcal{C} = Z_p^* \times Z_p^*$, and define

$$\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod{p}\}.$$

- The values p, α and β are public, and a is secret.

- $K = (p, \alpha, a, \beta)$, for a (secret) random number $k \in Z_{p-1}$, define

$$e_K(x, k) = (y_1, y_2),$$

where

$$y_1 = \alpha^k \bmod p$$

and

$$y_2 = x\beta^k \bmod p.$$

- For $y_1, y_2 \in Z_p^*$, define

$$d_K(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p.$$

- The plaintext x is "masked" by multiplying it by β^k, yielding y_2. The value α^k is also transmitted as part of the ciphertext. The decryptor, who knows the secret exponent a, can compute β^k from α^k. Then he can "remove the mask" by dividing y_2 by β^k to obtain the plaintext x.

Example

- Suppose $p = 2579, \alpha = 2, a = 765$, and hence

$$\beta = 2^{765} \bmod 2579 = 949.$$

- Now, suppose that Alice wishes to send the message $x = 1299$ to Bob. Say $k = 853$ is the random integer she chooses. Then she compute

$$y_1 = 2^{853} \bmod 2579 = 435$$

and

$$y_2 = 1299 \times 949^{853} \bmod 2579 = 2396.$$

- When Bob receives the ciphertext $y = (435, 2396)$, he compute

$$x = 2396 \times (435^{765})^{-1} \bmod 2579 = 1299,$$

which was the plaintext that Alice encrypted.

Algorithm for the Discrete Log Problem

- Given $\beta \in Z_p^*$, find the unique exponent $a, 0 \leq a \leq p_2$, such that $\alpha^a \equiv \beta \pmod{p}$.
- Clearly, the discrete logarithm (DL) problem can be solved by exhaustive search in $O(p)$ time.
- Other algorithms to the solve the DL problem.
  - *–Shanks' algorithm*
  - *–Pohlig-Hellman algorithm*
  - *–Index Calculus method*

The discrete logarithm problem in $(G, \circ)$

- **Problem Instance:** $I = (G, \alpha, \beta)$, where G is a finite group with group operation $\circ$, $\alpha \in G$ and $\beta \in H$, where $H = \{\alpha^i : i \geq 0\}$ is the subgroup generated by α.
- **Objective:** Find the unique integer a such that $0 \leq a \leq |H| - 1$ and $\alpha^a = \beta$, where the notation α^a means

$$\alpha \circ \alpha \circ \ldots \circ \alpha \qquad (a \text{ times})$$

Generalized ElGamal Public-key Cryptosystem

- Let G be a finite group with group operation $\circ$, and let $\alpha \in G$ be an element such that the discrete log problem in H is intractable, where $H = \{\alpha^i : i \geq 0\}$ is the subgroup generated by α.
- Let $\mathcal{P} = G$, $\mathcal{C} = G \times G$, and define

$$\mathcal{K} = \{(G, \alpha, a, \beta) : \beta = \alpha^a\}.$$

- The values α and β are public, and a is secret.

- $K = (G, \alpha, a, \beta)$, for a (secret) random number $k \in Z_{|H|}$, define

$$e_K(x, k) = (y_1, y_2),$$

where

$$y_1 = \alpha^k$$

and

$$y_2 = x \circ \beta^k.$$

- For a ciphertext $y = (y_1, y_2)$, define

$$d_K(y_1, y_2) = y_2 \circ (y_1^a)^{-1}.$$

Elliptic Curves over the Reals

- **Definition:** Let $a, b \in R$ be constants such that $4a^3 + 27b^2 \neq 0$. A non-singular elliptic curve is the set E of solutions $(x, y) \in R \times R$ to the equation

$$y^2 = x^3 + ax + b,$$

together with a special point $\mathcal{O}$ called the point at infinity.

- It can be shown that the condition $4a^3 + 27b^2 \neq 0$ is necessary and sufficient to ensure that the equation $x^3 + ax + b = 0$ has three distinct roots (which may be real or complex numbers).
- If $4a^3 + 27b^2 = 0$ then the corresponding elliptic curve is called a *singular elliptic curve*.
- Suppose E is a non-singular elliptic curve. We will define "+" operation over E which makes E into an abelian group.
- *Identity element:* The point at infinity, $\mathcal{O}$ is the identity element, so $P + \mathcal{O} = \mathcal{O} + \mathcal{P} = \mathcal{P}$ for all $P \in E$

Addition operation

- Suppose $P, Q \in E$, where $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. We consider three cases:
  1. $x_1 \neq x_2$
  2. $x_1 = x_2$ and $y_1 = -y_2$
  3. $x_1 = x_2$ and $y_1 = y_2$

Case 1: $x_1 \neq x_2$

- We define L to be line through P and Q. L intersects E in the two points P and Q, and it is easy to see that L will intersect E in one futher point, which we call R'. If we reflect R in the x-axis, then we get a point which we name R. We define $P + Q = R$.
- $R = (x_3, y_3)$, where $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, and $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$

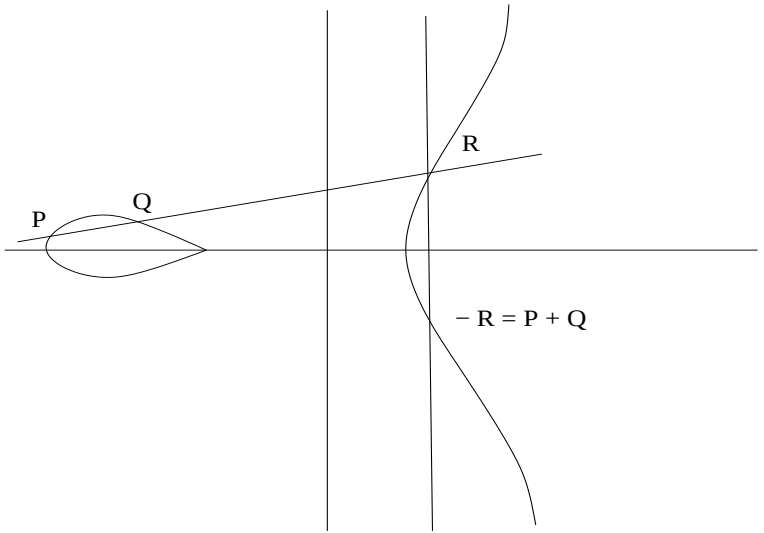

Figure 1: Chord and Tangent law

Case 2: $x_1 = x_2$ and $y_1 = -y_2$

- We define $(x, y) + (x, -y) = \mathcal{O}$ for all $(x, y) \in E$.
- $Q = -P$, then $P + Q = \mathcal{O}$, *i.e.* $\mathcal{O}$ is the third point of intersection of any vertical line through P (or Q) with the curve E. Any vertical line through P (or Q) meets the curve E at infinity. This is why $\mathcal{O}$ is called point at infinity. $\mathcal{O}$ serves as the identity of the abelian group E.
- Therefore $P = (x, y)$ and $-P = (x, -y)$ are inverses with respect to the elliptic curve addition operation.

Case 3: $x_1 = x_2$ and $y_1 = y_2$

- Here we are adding a point $P = (x_1, y_1)$ to itself. We can assume that $y_1 \neq 0$, for then we would be in case 2. Case 3 is handled much like case 1, expect that we define L to be tangent to E at the point P.
- If $P = (x_1, y_1) \in E$ then $P + P = (x_3, y_3)$, where $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$, and $\lambda = \frac{3x_1^2 + a}{2y_1}$

- If $P = (x_1, y_1) \in E$, $Q = (x_2, y_2) \in E$, $P \neq -Q$, then $P + Q = (x_3, y_3)$, where $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, and

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ if } P \neq Q;$$
$$\lambda = \frac{3x_1^2 + a}{2y_1} \text{ if } P = Q.$$

(E, +) is an abelian group

- At this point the following properties of the addition operation, as defined above, should be clear:
  1. addition is closed on the set E
  2. addition is commutative
  3. $\mathcal{O}$ is an identity with respect to addition, and
  4. every point on E has an inverse with respect to addition
- The proof of assiociativity is quite messy by algebric method. But this proof can be made simpler by using some results from geometry.

Elliptic Curves Modulo a Prime

- **Definition:** Let $p > 3$ be prime. The elliptic curve $y^2 = x^3 + ax + b$ over Z_p is the set of solutions $(x, y) \in Z_p \times Z_p$ to the congruence

$$y^2 \equiv x^3 + ax + b \pmod{p}, \qquad (1)$$

where $a, b \in Z_p$ are constants such that $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$, together with a special point $\mathcal{O}$ called the point at infinity.

- If $P = (x_1, y_1) \in E$, $Q = (x_2, y_2) \in E$, $P \neq -Q$, then $P + Q = (x_3, y_3)$, where $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, and

$$\begin{aligned} \lambda &= (y_2 - y_1)(x_2 - x_1)^{-1} && \text{if } P \neq Q; \\ \lambda &= (3x_1^2 + a)(2y_1)^{-1} && \text{if } P = Q. \end{aligned}$$

- To determine points on E we look at each possible $x \in Z_p$ and compute $x^3 + ax + b \pmod{p}$ which is y^2 and then need to check whether this is a quadratic residue module p.

Quadratic Residue Modulo p

- **Definition:** Let p be an odd prime and x is an integer, $1 \leq x \leq p-1$. x is defined to a quadratic residue modulo p if the congruence $y^2 \equiv x \pmod{p}$ has a solution $y \in Z_p$.
- Example: The quadratic residues modulo 11 are $1, 3, 4, 5$ and 9. Note that $(\pm 1)^2 = 1, (\pm 5)^2 = 3, (\pm 2)^2 = 4, (\pm 4)^2 = 5$ and $(\pm 3)^2 = 9$ (where all arithmetic is in Z_{11}).

- **Problem:** An add prime p, and an integer x such that $1 \leq x \leq p-1$. Is x is a quadratic residue modulo p?
- **Eular's Criterion:** x is a quadratic residue modulo p *if and only if*

$$x^{\frac{(p-1)}{2}} \equiv 1 \pmod{p}.$$

- Suppose z is a quadratic residue and $p \equiv 3 \pmod{4}$. Then, the two square roots of z modulo p are $\pm z^{(p+1)/4} \bmod p$.

Example

- Let E be the elliptic curve $y^2 = x^3 + x + 6$ over Z_{11}.
- For each possible $x \in Z_{11}$, compute $x^3 + x + 6 \bmod 11$.
- For a given x, we can test to see if $z = x^3 + x + 6 \bmod 11$ is a quadratic residue by applying Eular's criterion.
- We have that the square roots of a quadratic residue z are

$$\pm z^{(11+1)/4} \bmod 11 = \pm z^3 \bmod 11.$$

- Points on the elliptic curve $y^2 = x^3 + x + 6$ over Z_{11}:

x	$x^3 + x + 6 \bmod 11$	quadratic residue?	y
0	6	no	
1	8	no	
2	5	yes	4, 7
3	3	yes	5, 6
4	8	no	
5	4	yes	2, 9
6	8	no	
7	4	yes	2, 9
8	9	yes	3, 8
9	7	no	
10	4	yes	2, 9

- E has 13 points on it including $\mathcal{O}$
- We take a point $\alpha = (2, 7)$ and compute the "power" of α (which we will write as multiples of α, since the group operation is additive).
- To compute $2\alpha = (2, 7) + (2, 7)$, we first compute

$$\lambda = (3 \times 2^2 + 1)(2 \times 7)^{-1} \bmod 11 = 2 \times 3^{-1} \bmod 11$$

$$= 2 \times 4 \bmod 11 = 8.$$

- Then we have $x_3 = 8^2 - 2 - 2 \bmod 11 = 5$ and $y_3 = 8(2 - 5) - 7 \bmod 11 = 2$, so $2\alpha = (5, 2)$.

- The next multiple would be $3\alpha = 2\alpha + \alpha = (5,2) + (2,7)$.

$\alpha = (2,7)$	$2\alpha = (5,2)$	$3\alpha = (8,3)$
$4\alpha = (10,2)$	$5\alpha = (3,6)$	$6\alpha = (7,9)$
$7\alpha = (7,2)$	$8\alpha = (3,5)$	$9\alpha = (10,9)$
$10\alpha = (8,8)$	$11\alpha = (5,9)$	$12\alpha = (2,4)$

- $\alpha = (2,7)$ is a primitive element.
- We now look at an example of ElGamal encryption and decryption using elliptic curve of this example.

- $\alpha = (2, 7)$ and Bob's (the receiver) private key is 7, so

$$\beta = 7\alpha = (7, 2).$$

Thus the encryption operation is

$$e_K(x, k) = (k(2, 7), x + k(7, 2)),$$

where $x \in E$ and $0 \leq k \leq 12$, and the decryption operation is

$$d_K(y_1, y_2) = y_2 - 7y_1.$$

- Suppose Alice (the sender) wishes to encrypt the plaintext $x = (10, 9)$ (which is a point on E). If she chooses the random value $k = 3$, then she will compute

$$y_1 = 3(2, 7) = (8, 3)$$

and

$$y_2 = (10, 9) + 3(7, 2) = (10, 9) + (3, 5) = (10, 2).$$

- Hence $y = ((8,3),(10,2))$. Now if Bob receives the ciphertext y, he decrypts it as follows:

$$x = (10,2) - 7(8,3) = (10,2) - (3,5)$$

$$= (10,2) + (3,6) = (10,9).$$

- Hence, the decryption yields the correct plaintext.