CONTEMPORARY CRYPTOSYSTEMS

TIAN MA

Abstract. This paper mainly focuses on contemporary cryptography principles and methods, and how number theory and elliptic cruves are used to establish the foundations of two widely used cryptosystems, namely the RSA public-key cryptosystem, and the elliptic curve cryptosystem.

Contents

1. Introduction

The word *cryptography* is derived from Greek words *kryptos*, meaning "hidden", and *graphein*, meaning "write". Therefore, the meaning of the word *cryptography* is "hidden writing". Nowadays, cryptography protects people's privacy from sending text messages to shopping online. Frankly speaking, cryptography has penetrated into almost every aspect of our lives. In this paper, I would like to discuss two most important cryptosystems that people use nowadays - RSA cryptography, and Elliptic curve cryptography.

2. RSA Public-Key Cryptography

RSA is one of the most widely used cryptosystems in the world recently, and the algorithm behind this cryptosystem is heavily based on number theory. Therefore, in order to understand how RSA works, we will need some basic background on number theory first.

2.A. Basics of Number Theory.

Definition 2.1. For any $a, b \in \mathbb{Z}$, if there exists $q \in \mathbb{Z}$ such that $a = qb$, then we say b divides a, denoted by $b \mid a$.

Definition 2.2. If $n \in \mathbb{N}$, then we say that a is congruent to b modulo n if $n \mid (a-b)$, denoted by $a \equiv b (\text{mod } n)$.

Lemma 2.3. *(The Division Algorithm) If $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, then there exists unique $q, r \in \mathbb{Z}$ with $0 \leq r < b$, such that $a = bq + r$.*

Proof. The proof is left out. □

Definition 2.4. If $a \in \mathbb{Z}, b \in \mathbb{N}$ such that $a = bq + r$, where $0 \leq r < b$ is the remainder when a is divided by b, given by the Division Algorithm, then r is called the least non-negative residue of $a \mod b$, and $\{0, 1, 2, ..., b-1\}$ is called the set of least non-negative residues $\mod b$.

Lemma 2.5. *If $a, b \in \mathbb{Z}$ and $b = aq + r$, then $\gcd(a, b) = \gcd(a, r)$.*

Proof. The proof is left out. □

Theorem 2.6. *(The Euclidean Algorithm) Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$, and let $a = r_{-1}, b = r_0$. After repeatedly applying the Division Algorithm, we get $r_{j-1} = r_j q_{j+1} + r_{j+1}$, with $0 < r_{j+1} < r_j$, for all $0 \leq j \leq n$, where n is the least non-negative number such that $r_{n+1} = 0$, in which case $\gcd(a, b) = r_n$.*

Proof. Let $\{r_j\}$ be a sequence such that it is generated by repeated application of the Division Algorithm. Then $\{r_j\}$ is strictly decreasing and is bounded below, and so stops for some non-negative $n \in \mathbb{Z}$ with $r_{n+1} = 0$. By repeated application of Lemma 2.5, $\gcd(a, b) = \gcd(r_j, r_{j+1})$, for all $0 \leq j \leq n$. In particular, $\gcd(a, b) = \gcd(r_n, r_{n+1}) = r_n$. □

Example 2.7. Apply the Euclidean Algorithm to calculate $\gcd(1492, 1066)$.

Solution. Let $a = r_{-1} = 1492, b = r_0 = 1066$.

$$\begin{aligned} r_{-1} &= 1492 = 1 \times 1066 + 426 \\ r_0 &= 1066 = 2 \times 426 + 214 \\ r_1 &= 426 = 1 \times 214 + 212 \\ r_2 &= 214 = 1 \times 212 + 2 \\ r_3 &= 212 = 2 \times 106 + 0 \end{aligned}$$

So $\gcd(1492, 1066) = 2$. □

Theorem 2.8. *(Bezout's identity) If $a, b \in \mathbb{Z}$ such that they are not both 0, then there exists $u, v \in \mathbb{Z}$ such that $\gcd(a, b) = au + bv$.*

Proof. We use the equations which arise when we apply Euclidean algorithm to calculate $d = \gcd(a, b)$ as the last non-zero remainder r_n. The penultimate equation, in the form

$$d = r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$$

expressed d as a multiple of r_{n-3} plus a multiple of r_{n-2}. We then use the second to the last equation in the form

$$r_{n-2} = r_{n-4} - q_{n-2} r_{n-3}$$

to eliminate r_{n-2} and express d as a multiple of r_{n-4} plus a multiple of r_{n-3}. We gradually work backwards through the equations in the algorithm, eliminating $r_{n-3}, r_{n-4}, ...$ in succession, until eventually we have expressed d as a multiple of a plus a multiple of b, that is, $d = au + bv$ for some $u, v \in \mathbb{Z}$. □

Theorem 2.9. *(The Extended Euclidean Algorithm) Let $a, b \in \mathbb{N}$, and let q_i for $i = 1, 2, ..., n+1$ be the quotients obtained from the application of the Euclidean Algorithm to find $g = \gcd(a, b)$, where n is the least non-negative integer such that $r_{n+1} = 0$. If $s_{-1} = 1, s_0 = 0$, and $s_i = s_{i-2} - q_{n-i+2}s_{i-1}$, for $i = 1, 2, ..., n+1$, then $g = s_{n+1}a + s_n b$.*

Proof. We use induction to prove this theorem.
If $i = 0$, then $s_i r_{n-i+1} + s_{i-1}r_{n-i} = s_0 r_{n+1} + s_{-1}r_n = r_n$.
Assume that $r_n = s_i r_{n-i+1} + s_{i-1}r_{n-i}$.
By the definition of s_{i+1},

$$r_{n-i}s_{i+1} + s_i r_{n-i-1} = r_{n-i}(s_{i-1} - s_i q_{n-i+1}) + s_i r_{n-i-1}$$

If we rearrange this, it becomes

$$s_i(r_{n-i-1} - r_{n-i}q_{n-i+1}) + s_{i-1}r_{n-i}$$

By the Euclidean Algorithm, this is

$$s_i r_{n-i+1} + s_{i-1}r_{n-i}$$

which is r_n by the induction hypothesis. Therefore, if $i = n+1$, then

$$g = r_n = s_{n+1}r_0 + s_n r_{-1} = s_{n+1}a + s_n b$$

□

2.B. RSA Public-Key Cryptosystem Algorithm.

Definition 2.10. For such a function

$$f : \mathcal{M} \mapsto \mathcal{C}$$

there is information, called trapdoor (information), the knowledge of which makes it feasible to find $m \in \mathcal{M}$ such that $f(m) = c$ for any c in the image of f, but without the trapdoor, this task becomes infeasible.

Remark 2.11. We introduced the trapdoor one-way function because number theory plays a significant role in RSA, and number theory is a treasure trove of one-way trapdoor functions.

Now we break the algorithm into two parts: (I) RSA Key Generation, and (II) RSA Public-Key Cipher.

(I) RSA Key Generation.
Each individual involved in the communications should perform the following procedures.

(1) Generate two large, random primes p, q such that $p \neq q$, and p, q should be of roughly the same size.
(2) Compute $n = pq$, and $\phi(n) = (p-1)(q-1)$. The integer n is called the RSA modulus.
(3) Select a random $e \in \mathbb{N}$ such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. The integer e is called RSA enciphering exponent.

(4) Use the Extended Euclidean Algorithm to compute the unique $d \in \mathbb{N}$ with $1 < d < \phi(n)$ such that $ed \equiv 1(\text{mod}\phi(n))$. The integer d is called RSA deciphering exponent.
(5) The RSA public-key is (n, e), and the RSA private key is d.

(II) RSA Public – Key Cipher.

If Alice wants to send a message to Bob, then Alice must perform the following procedures.

enciphering stage:

(1) Obtain Bob's public-key (n, e).
(2) Translate the plaintext message into base-N numerical equivalents for a suitable $N > 1$. These numerical equivalents are then subdivided into blocks of equal size $l \in \mathbb{N}$. (l may be chosen such that $N^l < n < N^{l+1}$)
(3) Encipher each block $m \in \mathcal{M}$ separately by computing $c \equiv m^e(\text{mod } n)$.
(4) Send each block $c \in \mathcal{C}$ to Bob.

Once Bob receives $c \in \mathcal{C}$, then the following is performed.

deciphering stage:

(1) Use d to compute $m \equiv c^d(\text{mod } n)$.

Example 2.12. Encipher the sentence "EXAMS ARE HARD" using the RSA method introduced above.

Solution. We follow the above steps and get the following.

(1) Choose $p = 29$, and $q = 67$.
(2) Then $n = 29 \times 67 = 1943$, and $\phi(n) = 28 \times 66 = 1848$.
(3) Choose $e = 701$ such that $1 < 701 < 1848$ and $\gcd(701, 1848) = 1$.
(4) Calculate d from $ed - 1 = x\phi(n)$ using the Extended Euclidean Algorithm. Therefore,
$$701d + 1848x = 1$$
So we get $d = 29, x = -11$.
(5) Therefore, the public-key is $(1943, 701)$, and the private key is 29.
(6) Choose base $N = 26$. Since $26^2 < n < 26^3$, we choose the blocks of length $l = 2$. Therefore, we get the following table.

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

The message then becomes $\mathcal{M} = \{04, 23, 00, 12, 18, 00, 17, 04, 07, 00, 17, 03\}$.
(7) Then we encipher each $m \in \mathcal{M}$ via $m^{701} \equiv c(\text{mod } 1943)$. Therefore, we get the ciphered message
$$\mathcal{C} = \{613, 458, 0, 1926, 1439, 0, 1119, 613, 616, 0, 1119, 206\}$$

We can then verify that by plugging each $c \in \mathcal{C}$ into $c^{29} \equiv m(\text{mod } 1943)$, we get the original $m \in \mathcal{M}$. For example, $613^{29} \equiv 4(\text{mod } 1943)$. □

Remarks 2.13. (1) We should not choose p, q such that they are close to each other.
(2) We should choose $p - 1$ and $q - 1$ such that they do not have any large common factors.

(3) $\phi(n)$ should have a large prime factor.

Suppose that $p > q$, and q is very close to p. Then we have $\frac{p+q}{2}$ is slightly greater than $\sqrt{n} = \sqrt{pq}$. Given that

$$(\frac{p+q}{2})^2 - n = (\frac{p-q}{2})^2,$$

then we have a solution $(x, y) \in \mathbb{N} \times \mathbb{N}$ to $x^2 - n = y^2$.
To factor n, since $n = (x+y)(x-y)$, we only need to test $x \in \mathbb{Z}$ such that $x > \sqrt{n}$ until $x^2 - n = y^2, y \in \mathbb{N}$. In example 2.12, $n = 1943$, $\lfloor\sqrt{n}\rfloor = 44$.
For $x = 45, 46, 47$, we do not have such y.
For $x = 48$, we have $y = 19$. Therefore, $n = (48 + 19) \times (48 - 19)$.

Suppose that $p - 1$ and $q - 1$ do have some large common factors. Since the inverse of the enciphering exponent e modulo $\text{lcm}(p - 1, q - 1)$ suffices for d, it is easy to obtain d. For example, if $p = 23, q = 67$, and $e = 5$. Then we get $22 = (p - 1) \mid (q - 1) = 66$, so we only need to compute the inverse of e modulo $q - 1$, which is $d = 53$.

2.C. Validity of the Algorithm.

Lemma 2.14. *(Euclid's Lemma) Let d be a prime, and $a, b \in \mathbb{Z}$. If $d \mid ab$, then either $d \mid a$ or $d \mid b$.*

Proof. The proof is left out. □

Lemma 2.15. *Let m be a prime, and let a be a positive integer such that a and m are coprime. Then calculating the least residues of the number $a, 2a, ..., (m-1)a$ modulo m gives the numbers $1, 2, ..., m - 1$.*

Proof. Let $b_1, b_2, ..., b_{m-1}$ be the least residues of $a, 2a, ..., (m-1)a$ modulo m. That is, for each j, b_j is the number with $0 \leq b_j \leq m - 1$ such that $b_j \equiv j \cdot a (\text{mod } m)$. In order to prove that $b_1, b_2, ..., b_{m-1}$ are the numbers $1, 2, ..., m - 1$, we need to prove that each b_j satisfies $1 \leq b_j \leq m - 1$ and that the numbers b_j are distinct.

First we prove that $b_j \neq 0$. Suppose $b_j = 0$, then $0 \equiv j \cdot a (\text{mod } n)$ and $m \mid j \cdot a$. By Euclid's Lemma, either $m \mid j$ or $m \mid a$. Since $\gcd(a, m) = 1, m \nmid a$. Therefore, $m \mid j$. Since $j \in \mathbb{Z}$ such that $j < m$, we have a contradiction. Therefore, each b_j satisfies $1 \leq b_j \leq m - 1$.

Then we prove that the numbers $b_1, b_2, ..., b_{m-1}$ are distinct. It is enough to prove that if $i \neq j$, then $b_i \neq b_j$. Suppose that we have $b_i = b_j$, with $i \neq j$. Then $i \cdot a \equiv j \cdot a (\text{mod } m)$. Since a and m are coprime, then we have $i \equiv j (\text{mod } m)$. Therefore, we have $m \mid (i - j)$. Since i and j are both positive integers less than the modulus m, then for each $m \mid (i - j)$ to happen, i must be equal to j, contradicting $i \neq j$. Therefore, $b_1, b_2, ..., b_{m-1}$ are distinct.

We have proved that $\{b_1, b_2, ..., b_{m-1}\} \subseteq \{1, 2, ..., m - 1\}$. Since both sides of the set inclusion have $m - 1$ distinct numbers, both sides of the set inclusion must equal. □

Theorem 2.16. *(Fermat's Little Theorem) If p is a prime, and $a \in \mathbb{Z}$ such that a and p are coprime, then $a^{p-1} \equiv 1 (\text{mod } p)$.*

Proof. Since p is a prime, and a and p are coprime, then by Lemma 2.15, the least residues of $a, 2a, ..., (p-1)a$ modulo p are the numbers $1, 2, ..., p - 1$. Therefore, we

have the following congruence equation:

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) (\text{mod } p)$$

By rearranging the equation, we get:

$$a^{p-1} 1 \cdot 2 \cdots (p-1) \equiv 1 \cdot 2 \cdots (p-1) (\text{mod } p)$$

Now we cancel out $(p-1)!$ on both sides of the last congruence equation, and then we will get $a^{p-1} \equiv 1 (\text{mod } p)$. □

Lemma 2.17. *Let $M \in \mathbb{Z}$, and let p, q be primes such that $p \neq q$. If $a \equiv M (\text{mod } q)$ and $a \equiv M (\text{mod } p)$, then $a \equiv M (\text{mod } pq)$.*

Proof. Suppose that we have $a \equiv M (\text{mod } p)$ and $a \equiv M (\text{mod } q)$. Then for some $i, j \in \mathbb{Z}$, we have $a = M + pi$ and $a = M + qj$. Therefore, we have $pi = qj$. This implies that $p \mid qj$. By Euclid's Lemma 2.14, we have either $p \mid q$ or $p \mid j$. Since p and q are primes such that $p \neq q$, we have $p \mid j$. Therefore, there exists $w \in \mathbb{Z}$ such that $j = pw$. Now we have the equation

$$a = M + qj = M + qpw$$

Therefore, we have proved that $a \equiv M (\text{mod } pq)$. □

Proposition 2.18. *For RSA Public-Key Cryptosystem, we know that once the creator of the public key receives an encrypted message $c = f(m) \equiv m^e (\text{mod } n)$, he/she uses the decryption equation $g(c) \equiv c^d (\text{mod } n)$ to get the original message m. Therefore, the following equation must hold:*

$$g(c) = g(f(m)) = (m^e)^d = m^{ed} \equiv m (\text{mod } n)$$

Proof. It is enough for us to show that $m^{ed} \equiv m (\text{mod } p)$ and $m^{ed} \equiv m (\text{mod } q)$.

Case 1: Suppose that $m \equiv 0 (\text{mod } p)$. Then we have $m = pw$, for some $w \in \mathbb{Z}$. Therefore $m^{ed} = (pw)^{ed} = p \cdot p^{ed-1} \cdot w^{ed}$. This implies that $m^{ed} \equiv m (\text{mod } p)$.

Case 2: Suppose that $m \not\equiv 0 (\text{mod } p)$. Then p and m are coprime. Therefore, by Fermat's Little Theorem 2.16, we have $m^{p-1} \equiv 1 (\text{mod } p)$. Since for some $k \in \mathbb{Z}, ed - 1 = k(p-1)(q-1)$, then we have

$$\begin{aligned} m^{ed} &= m^{ed-1} \cdot m \\ &= m^{k(p-1)(q-1)} \cdot m \\ &= (m^{p-1})^{k(q-1)} \cdot m \\ &\equiv 1^{k(q-1)} \cdot m (\text{mod } p) \\ &\equiv m (\text{mod } p) \end{aligned}$$

Similarly we have $m^{ed} \equiv m (\text{mod } q)$. Therefore, $m^{ed} \equiv m (\text{mod } pq)$. □

2.D. Security Analysis - Factorization.

Theorem 2.19. *(The Fundamental Theorem of Arithmetic) Let $n \in \mathbb{N}, n > 1$. Then n can be factored into the product of several primes. Moreover, if $n = \prod_{i=1}^{p} p_i = \prod_{i=1}^{s} q_i$, where p_i and q_i are primes, then $r = s$, and the factors are the same if their order is ignored.*

Proof. First we prove the existence of such factorizations. If n is prime, then we are done with $n = p_k$, where $k = 1 = a_k$. If n is not prime, with $n = n_1 n_2$, we can apply the same argument to n_1 and n_2. The process must terminate since each subsequent factorization leads to positive integers less than the former, so ultimately all of these natural numbers are prime.

Now we prove the uniqueness of such factorizations by contradiction. Let $n > 1$, and

$$n = \prod_{i=1}^{r} p_i^{a_i} = \prod_{i=1}^{s} q_i^{b_j}$$

be the smallest natural number such that it does not have a unique factorization, where $p_1 < p_2 < ... < p_r$, and $q_1 < q_2 < ... < q_s$, with $a_i, b_j \in \mathbb{N}$. Suppose that $p_u = q_v$ for some $u, v \in \mathbb{N}$ with $1 \leq u \leq r$ and $1 \leq v \leq s$. If $n = p_n$, then the proof is trivial. Suppose that $n > p_u$. Since $1 < \frac{n}{p_u} < n$, $\frac{n}{p_u}$ has a unique factorization, and therefore we have

$$\frac{n}{p_u} = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_{u-1}} p_{u+1}^{a_{u+1}} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_u^{b_{v-1}} q_{v+1}^{b_{v+1}} \cdots q_s^{b_s}$$

with $r = s, p_i = q_i$, and $a_i = b_i$, for all $i = 1, 2, ..., r = s$. Therefore,

$$n = p_u p_1^{a_1} p_2^{a_2} \cdots p_u^{a_{u-1}} p_u^{a_{u+1}} \cdots p_r^{a_r} = q_v q_1^{b_1} q_2^{b_2} \cdots q_v^{b_{v-1}} q_v^{b_{v+1}} \cdots q_s^{b_s}$$

has a unique factorization, which is a contradiction. Therefore, for all $u, v \in \mathbb{N}, p_u \neq q_v$. However, by Euclid's Lemma 2.14, since $p_1 \mid \prod_{j=1}^{s} q_j^{b_j}$, then $p_1 \mid q_j$ for some j. Therefore, $p_1 = q_j$, which is a contradiction. Therefore, we have proved the unique factorization. □

Definition 2.20. If $B \in \mathbb{N}$, then $n \in \mathbb{N}$ is said to be B-smooth provided that all primes dividing n are not greater than B. The bound B is called a smoothness bound.

Example 2.21. Determine the smoothness bound B for 1620.

Solution. $1620 = 2^2 \times 3^4 \times 5$. Therefore, 1620 is 5-smooth. □

In order to know whether RSA Public-Key Cryptography is safe or not, we would like to know whether it is difficult for us to factor a large number $n \in \mathbb{N}$ into the product of two primes. Therefore, we would like to introduce two common ways to factor a natural number.

<u>Pollard's $p - 1$ Factoring Algorithm</u>

(1) We would like to factor $n \in \mathbb{N}$, and $B \in \mathbb{N}$ is selected.
(2) Choose a base $a \in \mathbb{N}$, where $2 \leq a < n$ and compute $g = \gcd(a, n)$. If $g > 1$, then we have a factor of n. Or go to (3).
(3) For all primes $p \leq B$, compute $m = \left\lfloor \frac{\ln(n)}{\ln(p)} \right\rfloor$ and replace a by $a^{p^m} \pmod{n}$.
(4) Compute $g = \gcd(a - 1, n)$. If $g > 1$, then we have a factor of n, and the algorithm is successful, otherwise it fails.
(5) Running time is $O(B \ln(B) \ln^2(n))$.

Example 2.22. Factor $n = 13193$ into the product of two primes.

Solution. We choose $B = 13, a = 2$. By following the procedures described above, we have the following results:

p	2	3	5	7	11	13
m	13	8	5	4	3	3
a	6245	1365	1884	3133	5472	396
gcd(a-1, n)	1	1	1	1	1	79

Therefore, 13193 can be factored into the product of 79 and 167, with $p-1 = 78 = 2 \times 3 \times 13$, which is B-smooth. $\square$

Definition 2.23. If $q_j \in \mathbb{R}$, where $j \in \mathbb{Z}$ is nonnegative and $q_j \in \mathbb{R}^+$ for $j > 0$, then an expression of the form

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}}}$$

is called a continued fraction.

<u>Continued Fraction Factoring Algorithm</u>

(1) We would like to factor $n \in \mathbb{N}$, and $B \in \mathbb{N}$ is selected.
(2) Choose a factor base of primes $\mathcal{F} = \{p_1, p_2, ..., p_k\}$ for some $k \in \mathbb{N}$ determined by $B \in \mathbb{N}$ and a large upper index value J.
(3) Set $Q_0 = 1, P_0 = 0, A_{-1} = 1, A_0 = \lfloor\sqrt{n}\rfloor = q_0 = P_1$. For each natural number $j \leq J$, recursively compute Q_j using the following formulas:

$$Q_j = \frac{n - {P_j}^2}{Q_{j-1}}$$

$$q_j = \left\lfloor \frac{P_j + \lfloor\sqrt{n}\rfloor}{Q_j} \right\rfloor$$

$$A_j = q_j A_{j-1} + A_{j-2}$$

$$P_{j+1} = q_j Q_j - P_j$$

and trial divide Q_j by the primes in $\mathcal{F}$ to determine if Q_j is P_k-smooth. If it is, then use its factorization $Q_j = \prod_{i=1}^{k} P_i^{a_{i,j}}$ to form the binary $k+1$-tuple $v_j = (v_{0,j}, v_{1,j}, ..., v_{k,j})$, where $v_{0,j}$ is respectively 0 or 1 according as j is even or odd, and for $1 \leq i \leq k, v_{i,j}$ is respectively 0 or 1 according as $a_{i,j}$ is even or odd. If Q_j is not P_k-smooth, discard it and return to calculate Q_{j+1}.
(4) For each set $\mathcal{S}$ of the vectors v_j constructed in (2), for which it is discovered that $\sum_{j\in\mathcal{S}} \equiv 0 (\text{mod } 2), 0 \leq i \leq k$, we have $x^2 \equiv y^2 (\text{mod } n)$, where $x = \left\lfloor \prod_{j\in\mathcal{S}} (-1)^j Q_j \right\rfloor^{1/2}$, and $y \equiv \prod_{j\in\mathcal{S}} A_{j-1} (\text{mod } n)$. If $x \not\equiv \pm y (\text{mod } n)$, then $\gcd(x \pm y, n)$ gives a factor of n.
(5) Running time is $O(e^{\sqrt{2\log(n)\log\log(n)}})$.

Remark 2.24. As we can see from the running times of the algorithms mentioned above, both algorithms will take quite long time to factor a given number into the product of two primes. Therefore, it makes RSA Public-Key Cryptography safe.

3. Elliptic Curve Cryptography

Elliptic Curve Cryptography was discovered and introduced later, but it can provide equivalent security with shorter keys and lower memory. RSA Public-Key systems are secure assuming that it is difficult to factor a large integer composed of two large prime factors. For elliptic-curve-based protocols, it is safe to assume that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible. Therefore, in order to better understand Elliptic Curve Cryptography, we will need some background on algebra.

3.A. Basics of Algebra.

Definition 3.1. A group can be defined as an algebraic structure $\langle S, * \rangle$ that satisfies the following:

(1) for all $a, b \in S, a * b \in S$.
(2) for all $a, b \in S, a * (b * c) = (a * b) * c$.
(3) there exists unique $e \in S$ such that for all $a \in S, a * e = e * a = a$.
(4) for all $a \in S$, there exists unique a^{-1} such that $a * a^{-1} = a^{-1} * a = e$.

Definition 3.2. A subset H of a group G is a subgroup of G if it is closed under the operation of G and also forms a group.

Definition 3.3. Let G be a group, and $H \subseteq G$ be a subgroup. for all $a \in G$, the sets $a * H = \{a * h : h \in H\}$ are called left cosets of H. for all $a \in G$, the sets $H * a = \{h * a : h \in H\}$ are called right cosets of H.

Definition 3.4. Let G be a group and $H \subseteq G$ be a subgroup. for all $a \in G$, then if the sets $a * H$ and $H * a$ are equal, then they are called cosets of H.

Theorem 3.5. *(Lagrange's Theorem) If H is a subgroup of G, then $|H| \mid |G|$.*

Proof. Since the cosets are equivalent, a left coset yH has the same number of elements as H, namely $|H|$. Since left cosets are identical or disjoint, each element of G belongs to exactly one left coset. From the definition of index of subgroup, there are $[G : H]$ left cosets, and therefore:

$$|G| = [G : H]|H|$$

If G is of finite order, then all three numbers are finite, and the result follows.
If G is of infinite order, then we get the following:
If $[G : H] = n$ is finite, then $|G| = n|H| \Rightarrow |H|$ is infinite.
If $|H| = n$ is finite, then $|G| = [G : H]n \Rightarrow [G : H]$ is infinite. □

Definition 3.6. A ring is an algebraic structure $\langle S, +, \times, \rangle$, with a set S and two associative binary operations $+, \times$ that satisfy the following:

(1) $\langle S, + \rangle$ is a commutative group with identity 0
(2) $\langle S, \times \rangle$ is a monoid with identity 1
(3) for all $a, b, c \in S, a \times (b+c) = (a \times b) + (a \times c)$ and $(b+c) \times a = (b \times a) + (c+a)$.

Definition 3.7. A ring $\langle S, +, \times \rangle$ in which $\langle S \setminus \{0\}, \times \rangle$ is a commutative group is a field.

Definition 3.8. Galois Field is a finite field with n elements, denoted by $\mathbb{F}_n$, where n is a prime power.

Definition 3.9. The characteristic of a ring R, denoted by $\mathrm{char}(R)$, is defined to be the smallest positive n such that $nx = 0$, for all $x \in R$ if such n exists, otherwise $\mathrm{char}(R) = 0$.

3.B. Introduction to Elliptic Curves.

Definition 3.10. Let F be a field such that $\mathrm{char}(F) \neq 2$ or 3. Let $a, b \in F$ such that $4a^3 + 27b^2 \neq 0$ in F, then an elliptic curve E defined over F is given by Weierstrass equation $y^2 = x^3 + ax + b \in F[x]$ with no repeated roots.

Definition 3.11. The discriminant of an elliptic curve E is $\Delta(E) = -16(4a^3 + 27b^2)$.

Remark 3.12. The discriminant of an elliptic curve needs to be non-zero, because this guarantees that $x^3 + ax + b = 0$ has no multiple roots.

Definition 3.13. Let $E : y^2 = f(x)$ be an elliptic curve over the field F. The set of F-rational points on E, denoted by $E(F)$, is the set $\{(x, y) \in F \times F : y^2 = f(x)\}$.

Definition 3.14. Let E be an elliptic curve over a field F with $\mathrm{char}(F) \neq 2$ or 3. For any two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on E, we define

$$P + Q = \begin{cases} \mathcal{O} & \text{if} x_1 = x_2 \text{ and } y_1 = y_2 \\ Q = Q + P & \text{if } P = \mathcal{O} \\ (x_3, y_3) & \text{otherwise} \end{cases}$$

where

$$\begin{cases} x_3 = m^2 - x_1 - x_2 \\ y_3 = m(x_1 - x_3) - y_1 \end{cases}$$

and

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & P = Q \end{cases}$$

Remark 3.15. If $P, Q, R \in E$ are collinear, then $P + Q + R = 0$.

Example 3.16. For an elliptic curve $E : y^2 = x^3 + 4x + 16$, given $P = (-2, 0), Q = (0, -4)$, compute $P + Q$.

Solution. If we use definition 3.14 to compute $P + Q$, we have $m = \frac{-4}{2} = -2, x_3 = 4 - (-2) - 0 = 6, y_3 = -2(-2 - 6) - 0 = 16$. Therefore, $P + Q = (6, 16)$.
If we compute with basic algebra, we have the equation that passes through P, Q is $y = -2(x + 2)$. Now if we plug $y = -2(x + 2)$ into $y^2 = x^3 + 4x + 16$, we get $x(x - 6)(x + 2) = 0 \Rightarrow x = 0, -2, 6$. We rule out $x = 0, -2$, and therefore, $P + Q = (6, 16)$. □

Definition 3.17. Let E be an elliptic curve over a field F. If there exists $P \in E(F)$ such that $nP = \mathcal{O}$ for some $n \in \mathbb{N}$, then P is called a torsion point or a point of finite order. The smallest such value of n is called the order of P.

Example 3.18. Given $E : y^2 = x^3 + 1, P = (2, 3)$. Compute the order of P.

Solution. $2P = (0, 1), 3P = (-1, 0), 4P = (0, -1), 5P = (2, -3), 6P = \mathcal{O}$. Therefore, P is a torsion point of order 6 on E. □

Remark 3.19. The set of torsion points $E(F)_t$ forms a subgroup of $E(F)$, and it is called the torsion subgroup of $E(F)$.

Definition 3.20. Let $a/b \neq 0$ be a rational number, where a, b are relatively prime, and $a, b \in \mathbb{Z}$. Write $a/b = p^r a_1/b_1$ with $p \nmid a_1 b_1$. Define the p-adic valuation to be $v_p(a/b) = r$.

Definition 3.21. Let E be an elliptic curve over $\mathbb{Z}$ given by $y^2 = x^3 + ax + b$. Let $r \geq 1$ be an integer. Define

$$E_r = \{(x, y) \in E(\mathbb{Q}) : v_p(x) \leq -2r, v_p(y) \leq -3r\} \cup \{\infty\}$$

Lemma 3.22. *Let E be given by $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$. Let p be a prime and let r be a positive integer. If $(x, y) \in E(\mathbb{Q})$, then $v_p(x) < 0$ if and only if $v_p(y) < 0$. In this case, there exists an integer $r \geq 1$ such that $v_p(x) = -2r$ and $v_p(y) = -3r$.*

Proof. The denominator of $x^3 + ax + b$ equals the denominator of y^2. It is easy to see that the denominator of y is divisible by p if and only if the denominator of x is divisible by p. If p^j, with $j > 0$, is the exact power of p dividing the denominator of y, then p^{2j} is the exact power of p in the denominator of y^2. Similarly, if p^k, with $k > 0$, is the exact power of p dividing the denominator of x, then denominator of $x^3 + ax + b$ is exactly divisible by p^{3k}. Therefore, $2j = 3k$. It follows that there exists r such that $j = 3r$ and $k = 2r$. This concludes the proof. □

Corollary 3.23. *Let the notations be as in Lemma 3.22, and $\lambda_r : E_r/E_{5r} \to Z_{p^{4r}}$ be an injective homomorphism. If $n > 1$ and n is not a power of p, then E_1 contains no points of exact order n.*

Proof. Suppose $P \in E_1$ has order n. Since n is not a power of p, we may multiply P by the largest power of p dividing n and obtain a point, not equal to ∞, of order prime to p. Therefore, we may assume that P has order n with $p \nmid n$. Let r be the largest integer such that $P \in E_r$. Then

$$n\lambda_r(P) = \lambda_r(nP) = \lambda_r(\infty) \equiv 0 (\text{mod } p^{4r})$$

Since $p \nmid n$, we have $\lambda_r(P) \equiv 0 (\text{mod } p^{4r})$, so $P \in E_{5r}$. Since $5r > r$, this contradicts the choice of r. Therefore, P does not exist. □

Theorem 3.24. *(Lutz-Nagell) Let E be an elliptic curve over $\mathbb{Q}$ given by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$, and $P = (x, y) \in E(\mathbb{Q})$. Suppose P has finite order. Then $x, y \in \mathbb{Z}$. If $y \neq 0$, then $y^2 \mid (4a^3 + 27b^2)$.*

Proof. Suppose $x \notin \mathbb{Z}$ or $y \notin \mathbb{Z}$. Then there exists a prime p diving the denominator of one of them. By Lemma 3.22, $P \in E_r$ for some $r \geq 1$. Let l be a prime dividing the order n of P. Then $Q = (n/l)P$ has order l. By Corollary 3.23, we have $l = p$. Choose j such that $Q \in E_j, Q \notin E_{j+1}$. Then $\lambda_j(Q) \not\equiv 0 (\text{mod } p)$, and

$$p\lambda_j(Q) = \lambda_j(pQ) \equiv 0 (\text{mod } p^{4j})$$

Therefore,

$$\lambda_j(Q) \equiv 0 (\text{mod } p^{4j-1})$$

This contradicts the fact that $\lambda_j(Q) \not\equiv 0 (\text{mod } p)$. If follows that $x, y \in \mathbb{Z}$.

Assume that $y \neq 0$. Then $2P = (x_2, y_2) \neq \infty$. Since $2P$ has finite order, $x_2, y_2 \in \mathbb{Z}$. Therefore,

$$x_2 = \frac{x^4 - 2ax^2 - 8bx + a^2}{4y^2}$$

Since $x_2 \in \mathbb{Z}$, this implies that

$$y^2 \mid x^4 - 2ax^2 - 8bx + a^2$$

A calculation gives us that

$$(3x^2 + 4a)(x^4 - 2ax^2 - 8bx + a^2) - (3x^3 - 5ax - 27b)(x^3 + ax + b) = 4a^3 + 27b^2$$

Since $y^2 = x^3 + ax + b$, we see that y^2 divides both terms on the left. Therefore, we have $y^2 \mid 4a^3 + 27b^2$. □

3.C. Application - Factorization.

The following is the algorithm for factoring an odd composite $n \in \mathbb{N}$, which we assume to have checked in advance is neither a perfect power nor a prime, and is relatively prime to 6.

Lenstra's Elliptic Curve Factoring Method

(1) Generate a pair (E, P), where E is an elliptic curve over $\mathbb{Q}$ with equation $y^2 = x^3 + ax + b$ $(a, b \in \mathbb{Z})$, and P is a point on E.
(2) Check that $\gcd(n, 4a^3 + 27b^2) = 1$. If not, then we have a factor of n, unless $\gcd(n, 4a^3 + 27b^2) = n$, in which case we choose a different pair (E, P).
(3) Choose $M \in \mathbb{N}$ and bounds $A, B \in \mathbb{N}$ such that $M = \prod_{j=1}^{l} p_j^{a_{p_j}}$, for small primes $p_1 < p_2 < ... < p_l \leq B$, where $a_{p_j} = \lfloor \ln(A)/\ln(p_j) \rfloor$ is the largest exponent such that $p_j^{a_{p_j}} \leq A$.
(4) For a sequence of divisors s of M, compute $\overline{sP}(\text{mod } n)$ as follows:
First compute
$$\overline{sP} = \overline{p_1^k P}$$
for $1 \leq k \leq a_{p_1}$, then
$$\overline{sP} = \overline{p_2^k p_1^{a_{p_1}} P} = (x_k, y_k)$$
for $1 \leq k \leq a_{p_2}$ and so on, until all primes p_j dividing M have been exhausted or the following occurs.
(5) If the calculation of either $(x_2 - x_1)^{-1}$ or $(2y_1)^{-1}$ for some $s \mid M$ in step (4), shows that one of them is not prime to n, then there is a prime $p \mid n$ such that $\overline{sP} = \mathcal{O}$. This will give us a nontrivial factor of n unless $\overline{sP} = \mathcal{O}$ for all primes $p \mid n$. In that case, $\gcd(s, n) = n$, and we go back and try the algorithm with a different (E, P) pair.
(6) Running time is $O(e^{\sqrt{(2+\epsilon)\ln(p)(\ln\ln(p))}}(\ln n)^2)$, where p is the smallest prime factor of n and ϵ goes to 0 as p gets large.

Remark 3.25. Through the study of elliptic curves, the composite number factoring method described above (Lenstra's Elliptic Curve Factoring Method) was discovered by Hendrik Lenstra. However, given the running time of this one, which is faster than the other two introduced in 2.D, this algorithm still remains to be insufficient to attack RSA Public-Key Cryptosystem.

3.D. Elliptic Curve Cryptography Algorithm.

Definition 3.26. If E is an elliptic curve over a field F, then the elliptic curve discrete log problem to base $Q \in E(F)$ is the problem of finding an $x \in \mathbb{Z}$ such that $P = xQ$ for a given $P \in E(F)$.

Suppose that Alice wants to send a message m to Bob. The ElGamal Public Key Cryptosystem consists of three parts: key generation by Bob, encryption by Alice, and decryption by Bob.

(**I**) **Key Generation**.
Bob establishes his public key as follows:

(1) Choose an elliptic curve E over a finite field $\mathbb{F}_q$.
(2) Choose a point P on E.
(3) Choose a private key $s \in \mathbb{Z}$ and compute $B = sP$.

(**II**) **Encryption**.
To send a message m to Bob, Alice does the following:

(1) Get Bob's public key.
(2) Encrypt her message as a point $M \in E(\mathbb{F}_q)$.
(3) Choose a secret random $k \in \mathbb{Z}$ and compute $M_1 = kP$.
(4) Compute $M_2 = M + kB$.
(5) Send M_1, M_2 to Bob.

(**III**) **Decryption**.
Bob decrypts the message by calculating $M = M_2 - sM_1$.

Remark 3.27. It is easy to see the validity of the ElGamal ECC. The decryption works because

$$M_2 - sM_1 = (M + kB) - skP = M + ksP - skP = M$$

3.E. Security Analysis - Attacks on Discrete Logs.

In this section, we would like to discuss given a group G, with $P, Q \in G$, how to solve $kP = Q$. Let N be the order of G, and assume N is unknown.

Baby Step, Giant Step

(1) Fix an integer $m \geq \sqrt{N}$ and compute mP.
(2) Make and store a list of iP for $0 \leq i \leq m$.
(3) Compute the points $Q - jmP$ for $j = 0, 1, ..., m-1$ until one matches an element from the stored list.
(4) If $iP = Q - jmP$, then we have $Q = kP$ with $k \equiv i + jm (\text{mod } N)$.

Remarks 3.28.
(1) This method requires approximately $\sqrt{N}$ steps and around $\sqrt{N}$ storage, and therefore, it only works well for moderate sized N.
(2) The point iP is calculated by adding P (a baby step) to $(i-1)P$. The point $Q - jmp$ is computed by adding $-mP$ (a giant step) to $Q - (j-1)mP$.

Theorem 3.29. *Prove the validity of baby step, giant step algorithm.*

Proof. Since $m^2 > N$, we assume the solution k satisfies $0 \leq k \leq m^2$. Write $k = k_0 + mk_1$, with $k_0 \equiv k (\text{mod } m)$, and $0 \leq k_0 < m$ and let $k_1 = (k - k_0)/m$. Then $0 \leq k_1 < m$. When $i = k_0$ and $j = k_1$, we have

$$Q - k_1 mP = kP - k_1 mP = k_0 P$$

Therefore, there is a match. □

Example 3.30. Let $G = E(\mathbb{F}_{41})$, where E is given by $y^2 = x^3 + 2x + 1$. Let $P = (0, 1)$ and $Q = (30, 40)$. Find the $k \in \mathbb{Z}$ such that $kP = Q$.

Solution. The order of G is at most 54, so we let $m = 8$. Then the points iP for $1 \leq i \leq 7$ are

$$(0,1),(1,39),(8,23),(38,38),(23,23),(20,28),(26,9)$$

We calculate $Q - jmP$ for $j = 0,1,2$ and obtain

$$(30,40),(9,25),(26,9)$$

at which point we stop since this third point matches $7P$. Since $j = 2$ yielded the match, we have

$$(30,40) = (7 + 2 \cdot 8)P = 23P$$

Therefore, $k = 23$. □

The Pohlig-Hellman Method

Theorem 3.31. *(Chinese Remainder Theorem) Suppose that $k > 1$ is an integer, $n_i \in \mathbb{N}$ for natural numbers $i \leq k$ are pairwise relatively prime, and $r_i \in \mathbb{Z}$ for $i \leq k$ are arbitrary. Then there exists $x_i \in \mathbb{Z}$ for $1 \leq i \leq k$ such that*

$$n_1x_1 + r_1 = n_2x_2 + r_2 = ... = n_kx_k + r_k$$

Proof. We use induction on k. If $k = 2$, the result holds since when $\gcd(n_1, n_2) = 1$, then $n_1x - n_2y = r_2 - r_1$ has a solution. Now we assume that the result holds for $k \geq 2$, the induction hypothesis, and we prove it for $k + 1$. Let $n_1, n_2, ..., n_{k+1} \in \mathbb{N}$ be pairwise relatively prime and let $r_1, r_2, ..., r_{k+1} \in \mathbb{Z}$ be chosen randomly. By the induction hypothesis, there exist integers $x_1, x_2, ..., x_k \in \mathbb{Z}$ satisfying $n_1x_1 + r_1 = n_2x_2 + r_2 = ... = n_kx_k + r_k$. The relative primality assumption implies that $\gcd(n_1n_2 \cdots n_k, n_{k+1}) = 1$. Therefore, there exists $X, Y \in \mathbb{Z}$ such that $n_1n_2 \cdots n_kX - n_{k+1}Y = r_{k+1} - n_1x_1 - r_1$. Set

$$X_j = \frac{n_1n_2 \cdots n_kX}{n_j} + x_j \in \mathbb{Z}, \text{for } 1 \leq j \leq k \text{ and } X_{k+1} = Y$$

Therefore, $n_1X_1 + r_1 = n_2X_2 + r_2 = \cdots = n_{k+1}X_{k+1} + r_{k+1}$, so we can conclude the proof by induction. □

As before, P, Q are elements in a group G and we want to find an integer k with $kP = Q$. We also know the order N of P and we know the prime factorization

$$N = \prod_i q_i^{e_i}$$

of N. The idea of Pohlig-Hellman is to find $k(\text{mod } q_i^{e_i})$ for each i, then use the Chinese Remainder Theorem to combine these and obtain $k(\text{mod } N)$.

Let q be a prime, and let q^e be the exact power of q dividing N. Write k in its base q expansion as

$$k = k_0 + k_1q + k_2q^2 + \cdots$$

with $0 \leq k_i < q$. We will evaluate k (mod q^e) by successively determining $k_0, k_1, \cdots, k_{e-1}$ as follows:

(1) Compute $T = \{j(\frac{N}{q}P) : 0 \leq j \leq q - 1\}$.
(2) Compute $\frac{N}{q}Q$. This will be an element $k_0(\frac{N}{q}P)$ of T.
(3) If $e = 1$, stop. Otherwise, continue.
(4) Let $Q_1 = Q - k_0P$.
(5) Compute $\frac{N}{q^2}Q_1$. This will be an element $k_1(\frac{N}{q}P)$ of T.

(6) If $e = 2$, stop. Otherwise, continue.
(7) Suppose we have computed k_0, k_1, k_{r-1}, and $Q_1, \cdots, Q_{r-1}$.
(8) Let $Q_r = Q_{r-1} - k_{r-1}q^{r-1}P$.
(9) Determine k_r such that $\frac{N}{q^{r+1}}Q_r = k_r(\frac{N}{q}P)$.
(10) If $r = e - 1$, stop. Otherwise, return to step (7).

Then

$$k \equiv k_0 + k_1 q + \cdots + k_{e-1}q^{e-1}$$

Remark 3.32. The algorithm's running time is $O(\sum_i e_i(\log n + \sqrt{p_i}))$.

Theorem 3.33. *The Pohlig-Hellman Method is valid.*

Proof. Since $NP = \infty$, we have

$$\frac{N}{q}Q = \frac{N}{q}(k_0 + k_1 q + \cdots)P$$
$$= k_0\frac{N}{q}P + (k_1 + k_2 q + \cdots)NP = k_0\frac{N}{q}P$$

Therefore, step (2) finds k_0. Then

$$Q_1 = Q - k_0 P = (k_1 q + k_2 q^2 + \cdots)P$$

so

$$\frac{N}{q^2}Q_1 = (k_1 + k_2 q + \cdots)\frac{N}{q}P$$
$$= k_1\frac{N}{q}P + (k_2 + k_3 q + \cdots)NP = k_1\frac{N}{q}P$$

Therefore, we find k_1. Similarly, the method produces $k_2, k_3, \cdots$ We have to stop after $r = e - 1$ since $\frac{N}{q^{e+1}}$ is no longer an integer, and we cannot multiply Q_e by the noninteger $\frac{N}{q^{e+1}}$. □

Example 3.34. Let $E : y^2 = x^3 + 1$ be defined over $E(\mathbb{F}_{599})$. Let $P = (60, 19)$ and $Q = (277, 239)$. Solve for $kP = Q$.

Solution. P has order $N = 600$. Then the prime factorization of N is

$$600 = 2^3 \times 3 \times 5^2$$

We will compute $k \mod 8$, $\mod 3$, and $\mod 25$, then recombine to obtain $k \mod 600$.

$k \mod 8$. We compute $T = \{\infty, (598, 0)\}$. Since

$$(N/2)Q = \infty = 0 \cdot (\frac{N}{2}P)$$

we have $k_0 = 0$. Therefore,

$$Q_1 = Q - 0P = Q$$

Since $(N/4)Q_1 = 150Q_1 = (598, 0) = 1 \cdot \frac{N}{2}P$, we have $k_1 = 1$. Therefore,

$$Q_2 = Q_1 - 1 \cdot 2 \cdot P = (35, 243)$$

Since $(N/8)Q_2 = 75Q_2 = \infty = 0 \cdot \frac{N}{2}P$, we have $k_2 = 0$. Therefore,

$$k = 0 + 1 \cdot 2 + 0 \cdot 4 + \cdots \equiv 2 (\mathrm{mod}\ 8)$$

$k \mod 3$. We have $T = \{\infty, (0,1), (0,598)\}$. Since

$$(N/3)Q = (0,598) = 2 \cdot \frac{N}{3} P$$

we have $k_0 = 2$. Therefore,

$$k \equiv 2 (\text{mod } 3)$$

$k \mod 25$. We have

$$T = \{\infty, (84,179), (491,134), (491,465), (84,420)\}$$

Since $(N/5)Q = (84,179)$, we have $k_0 = 1$. Then

$$Q_1 = Q - 1 \cdot P = (130,129)$$

Since $(N/25)Q_1 = (491,465)$, we have $k_1 = 3$. Therefore,

$$k = 1 + 3 \cdot 5 + \cdots \equiv 16 (\text{mod } 25)$$

We now have the simultaneous congruences

$$\begin{cases} x \equiv 2 (\text{mod } 8) \\ x \equiv 2 (\text{mod } 3) \\ x \equiv 16 (\text{mod } 25) \end{cases}$$

These combine to yield $k \equiv 266 (\text{mod } 600)$, so $k = 266$. □

Acknowledgments. It is a pleasure to thank my mentors, Peter Xu and Yun Cheng, for inspiring me to think about cryptography, and guiding me through all the studies.

References

[1] Kenneth H. Rosen. Elementary Number Theory and its Applications. Addison Wesley Longman, Inc., 2000.
[2] Gareth A. Jones and J. Mary Jones. Elementary Number Theory. Springer. 1998.
[3] Lawrence C. Washington. Elliptic Curves. Chapman & Hall/CRC. 2008.
[4] Richard A. Mollin. An Introduction to Cryptography. Chapman & Hall/CRC. 2001.
[5] Rolf Oppliger. Contemporary Cryptography. Artech House. 2005.
[6] Anthony W. Knapp. Elliptic Curves. Princeton University Press. 1992.
[7] Richard A. Mollin. Fundamental Number Theory with Applications. Chapman & Hall/CRC. 2008.