APPLICATION OF NUMBER THEORY
TO CRYPTOGRAPHY

Indulata Sukla
Department of Mathematics, Sambalpur University, Sambalpur

1. Introduction

Cryptography is the science of making communication unintelligible to all except authorized parties. It has come from the Greek word Kryptos meaning hidden and graphein - to write. In the classical age the making and breaking of secret codes has usually been confined to diplomatic and military practices. With the growing quantity of digital data stored and communicated by electronic data processing systems, organisations in both the public and commercial sectors have felt the need to protect information from unwanted instructions. There is now a surge of interest among mathematicians and computer scientists in cryptography.

The codes are called enciphers. The information to be concealed is called plaintext. After transformation to a secret form, a message is called Ciphertext. The process of converting from plaintext to ciphertext is said to be encrypting or enciphering while the reverse process of changing from ciphertext back to plaintext is called decrypting or deciphering. Cryptographic system was used by the Roman emperor Julius Caesar around 50 B.C. Caesar wrote to Marcus Cicero using a rudimentary cipher using alphabets A-Z.

\[ P \rightarrow C \rightarrow C^{-1} \rightarrow P. \]

Caesar Cipher:


Example : Plaintext message:

(1) CAESAR WAS GREAT
is transferred in Ciphertext:
FDHVDU ZDV JUHDV

It can be described easily using congruence theory. If we assign numerical values
01 to 26 for A-Z, then if C stands for ciphertext and P for plaintext,

\[ C \equiv P + 3 \pmod{26}. \]

The message (1) is converted to its equivalent:

030105 19 01 18/ 2301 19/07 18050120;

using \( C \equiv P + 3 \pmod{26} \) (2) becomes

060408 220421 / 260422/10 210804 23

To get plaintext from ciphertext we use

\[ P \equiv C-3 \equiv C + 23 \pmod{26}. \]

Caesar cipher is very simple and insecure. Caesar himself abandoned this scheme
because he did not trust Cicero.

In the process of Cryptography both the sender and the receiver jointly have a
secret key: the same key is used by both. But the Public key Cryptography differs from
conventional cryptography in that it uses two keys, an encryption key and a decryption
key. Though there is inverse process by which both keys are related, there is no easily
computed method of deriving the decryption key from encryption key. Thus an encryption
key can be made public so that each user can use it, but only the intended recipient
(whose decryption key is secret) can decipher them. It is advantageous over the previous
system in that they will not change the key in advance for communication.

Recent Development: In 1977, R Rivest, A. Shamir and L. Adleman in short RSA,
proposed a public key cryptosystem which uses only elementary ideas from Number
theory, their enciphering system is called RSA. It depends on the prime factorization of
composite numbers. Its security depends on the assumption that in the current computer
technology, the factorization of composite numbers with large prime factors is
prohibitively time-consuming.

2. Brief description of RSA system

In this system each user chooses a pair of distinct primes p and q large enough so
that their product \( n = pq \), called the enciphering modulus, is

beyond current computational capabilities. For example, one user chooses p
and \( q \) with 200 digits each; then \( n \) has too many digits. Having selected \( n \), the user chooses a random positive integer \( k \), the 'enciphering exponent' satisfying \( (k, \varphi(n)) = 1 \). The pair \((n,k)\) is placed in a public file, like telephone directory which is the user's personal encryption key. This will allow anyone else in the communication network to encrypt and send a message to the individual. Here the public key does not mention the factors \( p \) and \( q \) of \( n \).

**Encryption process.**

First we have to convert the message to an integer \( M \) by means of "digital alphabet" in which each one is replaced by a two-digit integer.

\[
\begin{align*}
    A-Z & \rightarrow 27 \quad 1 = 31 \quad 9 = 39 \\
    01-26 & \rightarrow 28 \quad 2 = 32 \quad ! = 40 \\
    ? & \rightarrow 29 \quad 3 = 33 \\
    0 & = 30 \\
    \text{...}
\end{align*}
\]

with 00 indicating a space between words.

\[P: \text{message} \]

```plaintext
The brown fox is quick
```

\[M = 2008050002181523140006152400090900172109031128\]

Assume

\( M < n, \) \( n \) is enciphering modulus.

\( M \) can also be broken up into blocks of digits \( M_1M_2 \ldots M_r \) of appropriate size; each one is encrypted separately.

Raise \( M \) to \( k^{th} \) power and reduce it to modulo \( n \)

\[M^k \equiv r \pmod{n},\]

\( k \) is selected according to g. c. d. \( (k, \varphi(n)) = 1 \). \( k \) can also be chosen as prime factor of \( \varphi(n) + 1 \); \( r \) is the ciphertext number.

At the other end the authorised recipient deciphers the transmitted informations by determining the integer \( j \), called secret recovery exponent for which

\[k_j \equiv 1 \pmod{\varphi(n)}\]
Since \((k, \varphi(n)) = 1\), \(j\) is unique modulo \(\varphi(n)\).

and \(j \equiv k^{\varphi(n)-1} \mod \varphi(n)\)

(\text{By Euler's Theorem})

It can be calculated by some one who knows both \(k\) and \(\varphi(n) = (p-1)(q-1)\) for \(n = pq\), hence knows the prime factors \(p\) and \(q\) of \(n\). Thus \(j\) is secure from the party where knowledge is limited to the public key \((n,k)\).

The recipient can now receive \(M\) from \(d\) by simply calculating \(r \mod n\). Because \(k^j = 1 + \varphi(n)t\) for some integer \(t\), it follows that \(d \equiv (M^k)^j \equiv M^{1+\varphi(n)t} \equiv M^{(M \varphi(n))^t} \equiv M \mod n\)

when \(\text{g.c.d.} (M,n) = 1\).

Thus raising the ciphertext number to the \(j\)th power and reducing it to modulo \(n\) recovers original plaintext integer \(M\). The assumption \((M,n) = 1\) is required to use Euler's Theorem.

**Example of RSA public key Algorithm:** Let \(p = 29\), \(q = 53\). Then \(n = 29 \cdot 53 = 1537\)

\(\varphi(n) + 1 = 52 \times 28 + 1 = 1457 = 31.47\). The enciphering exponent \(\text{k} = 47\) (Chosen)

\(\text{g.c.d.} (k, \varphi(n)) = 1\)

The recovery exponent, the unique integer \(j\), satisfies \(k^j \equiv 1 \mod \varphi(n)\); \(j = 31\).

Suppose the message is: NO WAY

Equivalent integer \(M = (1415 00 2301 25); M\text{ must be }< n\). So break \(M\) to blocks.

The 1st is 141; 141 \(47 \equiv 658 \mod 1537\). The recovery exponent is 31.

The authorized recipient would begin to recover the plaintext by computing

\[(658)^{31} \equiv 141 \mod 1537\]. The total ciphertext to our message is 0658, 1408, 1250, 1252.

RSA is more advantageous and secure; for to find \(j\) one has to know the prime factors \(p\) and \(q\) of \(n\). Given unlimited computing time and some
unimaginably efficient factoring algorithm, the RSA cryptosystem could be broken, but for
the present it appears to be safe.

Exercise 1: Encrypt the message GOLD MEDAL, using RSA system with key \((n,k) = (2149,3)\).

2. Using cipher \(C = 5P + 11 \pmod{26}\) encrypt the message

\[\text{NUMBER THEORY IS EASY.}\]

3. **Detailed descriptions of some simple cryptosystems**

   The plaintext and ciphertext are broken up into *message units*. A message unit might be a single letter, a pair of letters (digraph), a triple of letters (trigraph) or a block of

   50 letters.

   **Enciphering transformation** \(f : P \rightarrow C\)

   **Deciphering transformation** \(f^{-1} : C \rightarrow P\).

   We can also take A-Z, 0-25; 27 letters A-Z and a blank; a digraph corresponding to \(x, y \in \{0, 1, 2, \ldots, 26\}\) we label by the integer \(27x + y \in \{0, 1, 2, \ldots, 728\}\). We view individual letters as digits to the base 27, a digraph as a 2-digit integer to that base.

   The digraph "NO" corresponds to 27. 13+14 = 365. \(N = 13, O = 14\).

   If trigraph is used as message unit, then we label it by the integer \((27)^2x + 27y + z \in \{0, 1, \ldots, 19682\}\). 19682 = 27^3-1.

   In general we can label blocks of \(k\) letters in an \(N\)-letter alphabet by integers between 0 and \(N^{k-1}\) by regarding each such block as a \(k\)-digit integer to the base \(N\).

   We consider \(\{0, 1, 2 \ldots N-1\}\) as \(\text{Z/NZ}\).

   \[
   C = f(P) = P + 3 \text{ if } x < 23 \\
   = P - 23 \text{ if } x \geq 23.
   \]

   **Example**: Encipher "YES" : 240418

   We add 3 mod 26 and get 010721 i.e. "BHV" The ciphertext "ZKB" yields the plaintext "WHY". It is called *shift transformation*.

   **General Transformation**: \(f(P) \equiv P + b \pmod{N}\)

   \[
   P = f^{-1}(C) \equiv C - b \pmod{N}
   \]

   \(b\) is called the *parameter* and it has to be changed from time to time to keep the

   secrecy of the code. It is also called 'key'.
4. Frequency Analysis Method

Example: \( P: "FQOCUDEM" \)

which was enciphered by using a shift transformation on single letters of 26-letter alphabet. It remains to find \( b \), the key. We know 'e' is the most frequently occurring letter in the English language. Suppose \( U \) is the most frequently occurring character in the ciphertext. The shift takes e = '4' to "U" = 20, i.e. \( 20 \equiv 4 + b \pmod{26} \), so that \( b = 16 \).

So to get Plaintext, subtracting 16,

\[ \text{"FQOCUDEM"} = 516142203412 \rightarrow 15024124131422 = "PAY ME NOW" \]

There are 26 possibilities for \( b \) and only one makes a sensible sentence and that \( b \) is the enciphering key. It is very simple and easy to break.

**Affine transformation**: A general type of transformation of \( \mathbb{Z}/\mathbb{Z} \) is called affine transformation or affine map: \( C \equiv aP + b \pmod{N} \), where \( a \) and \( b \) are fixed integers (together they form the enciphering key).

Ex. "PAY ME NOW". Using \( a = 7 \ b = 12 \), we get

\[
15024124131422 \rightarrow 131224181425610 = "NMYSOZGK"
\]

If \( C \equiv aP + b \pmod{N} \) then \( P \equiv a^{-1}c + b' \pmod{N} \),

where \( a' \) is inverse of \( a \mod N \) i.e. \( aa' \equiv 1 \pmod{N} \), \( b' = -a^{-1}b \)

This works only if g.c.d. (\( a, N \)) = 1. Otherwise we cannot solve for \( P \) in terms of \( C \).

An Affine cryptosystem is an \( N \)-letter alphabet with parameter \( a \in (\mathbb{Z}/\mathbb{Z})^* \) and \( b \in \mathbb{Z}/\mathbb{Z} \), consists of rule: \( C \equiv aP + b \pmod{N} \), \( P \equiv a'C + b' \pmod{N} \),

where \( a' = a^{-1} \) in \( (\mathbb{Z}/\mathbb{Z})^* \), \( b' = -a^{-1}b \).

Example: Suppose the most frequently occurring letter in the ciphertext is "K" and the second most is "D"; these are encryption of "E" and "T" respectively which are most frequently occurring letters in the English language; we get

\( P \equiv 10a' + b' \equiv 4 \pmod{26} \); \( 3a' + b' \equiv 19 \pmod{26} \)

Evaluating \( a' \) and \( b' \) we get \( 7a' \equiv 11 \pmod{26} \) \( \Rightarrow a' \equiv 7^{-1} \equiv 11 \equiv 9 \pmod{26} \);

\( b' \equiv 4 - 10a' \equiv 18 \pmod{26} \).

So the message can be deciphered by the formula \( P \equiv 9C + 18 \pmod{26} \).
**Digraph transformation.** Suppose that plaintext and ciphertext message units are two letter blocks called digraphs. In digraph an enciphering transformation is a rearrangement of the integers \( \{ 0, 1, 2, ..., N^2-1 \} \)

We now denote this set of integers as \( Z/N^2Z \) and define the encryption of \( P \) to be the non-negative integers \( < N^2 \) satisfying the congruence \( C \equiv a P + b \mod N^2 \). \( a \) has no common factor with \( N \). Inverse transformation tells us how to decipher \( P \equiv a'c + b' \mod N^2 \), where \( a' = a^{-1} \mod N^2 \), \( b' \equiv -a^{-1} b \mod N^2 \). We translate \( C \) into a two-letter block of ciphertext by writing it in the form \( C = x' N + y' \) and looking up the letters with numerical equivalents \( x' \) and \( y' \).

**Example:**

Suppose we use digraph enciphering transformation \( C \equiv 159P + 580 \mod 676 \) (26^2).

The digraph "NO" has numerical equivalent 13. 26 + 14 = 352 and taken to \( C \equiv 159.352 + 580 \equiv 440 \mod 676 \), which is "QY". The digraph "ON" has numerical equivalent 377 and is taken to \( 359 = "NV" \).

In the digraph, a frequency analysis means finding which two letter blocks occur most often in a long string of ciphertext and comparing with known frequency of digraphs in English language texts. For example, if we use the 26 letter alphabet, statistical analysis seem to show that "TH" and "HE" are the two most frequently occurring digraphs, in the order. Two plaintext - ciphertext pairs of digraphs will often be enough to determine \( a \) and \( b \).

**Example:**

suppose the most frequently occurring digraphs are "ZA", "IA" and "IW"; suppose that the most frequently occurring digraphs in the English language are "E" (E blank) "S", "T". The cryptosystem uses an affine enciphering transformation modulo \( 27^2 = 729 \). Find the deciphering key and read the message "NDXBHO" Also find the enciphering key.

**Solution:** We know that plaintexts are enciphered by means of the rule \( C \equiv a P + b \mod 729 \) and that ciphertexts can be deciphered by means of the rule \( P \equiv a'C + b' \mod 729 \), here \( a \) and \( b \) form the enciphering key and \( a', b' \) form the deciphering key. To find \( a', b' \)

ZA

"E"
\[ 675 \ a' + b' \equiv 134 \mod 729 \]  \hspace{1cm} (1)

IA

\[ 216 \ a' + b' \equiv 512 \mod 729 \]  \hspace{1cm} (2)

IW

\[ 238 \ a' + b' \equiv 721 \mod 729 \]  \hspace{1cm} (3)

Eliminate \( b' \) by subtraction from the first two congruences (1) and (2); we get

\[ 459 \ a' \equiv 351 \mod 729 \]

which does not have a unique solution \( a' \mod 729 \) (as there are 27 solutions)

(2) \( \rightarrow \) (3) gives

\[ 437 \ a' \equiv 142 \mod 729 \]

\[ a' \equiv 437^{-1} 142 \mod 729. \]

To find \( 437^{-1} \)

\[ 729 = 437 + 292 \]

\[ 437 = 292 + 145 \]

\[ 292 - 145 = 147 + 2 \]

\[ 147 = 72 \cdot 2 + 1 \]

and 

\[ 1 = 145 - 72.2 = 145 - 72 (292 - 2.145) \]

\[ = 145 \cdot 145 - 72.292 \]

\[ = 145 (437 - 292) - 72.292 \]

\[ = 145 \cdot 437 - 217.292 \]

\[ = 145 \cdot 437 - 217 (729 - 437) \]

\[ = 362.437 \mod 729. \]

\( (437)^{-1} = 362. \)

\[ a' \equiv 362 \cdot 142 \equiv 374 \mod 729. \]

and 

\[ b' \equiv 134 - 675.374 \equiv 647 \mod 729. \]

Now applying the deciphering transformation to the digraphs "ND", "XB" and "HO" of our message, they correspond to
354, 622 and 203 respectively - we obtain the integers 365, 724 and 24.

Writing

\[
365 = 13.27 + 14 \\
724 = 26.27 + 22 \\
24 = 0.27 + 24
\]

we get the plaintext digraphs into the message "NO WAY"

To find the enciphering key we compute

\[
a \equiv a^{-1} \equiv 374^{-1} \equiv 614 \mod 729.
\]

and

\[
b \equiv -a^{-1}b' \equiv -614.647 \equiv 47 \mod 729.
\]

Drawback :

Though it is better than the affine transformation using single letter (i.e. modulo N) it has the drawback that the second letter of each ciphertext digraph depends only on the second letter of the plaintext digraph.

**Enciphering Matrices**

Suppose we have an N-letter alphabet and want to send digraphs as our message units. We will show how each digraph corresponds to a vector i.e. a pair of integers \( \begin{pmatrix} x \\ y \end{pmatrix} \) with x & y each considered modulo N. We use 26 letters A-Z with numerical equivalents 0 - 25.

Digraph "NO" corresponds to the vector \( \begin{pmatrix} 13 \\ 14 \end{pmatrix} \); each digraph P is a point in N x N square array. N x N array is denoted by \((Z/NZ)^2\).

\[ f : P \rightarrow C \] an enciphering map is a 1-1 function from \((Z/NZ)^2\) to itself. For some fixed k, regard blocks of k letters as vectors in \((Z/NZ)^k\).

**Some results :**

\[
A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}
\]

has an inverse iff its determinant \( D \) = ad - bc \neq 0 and that its inverse is

\[
D^{-1} = \begin{pmatrix} D^{-1}b & -D^{-1} \b \\ -D^{-1}c & D^{-1}a \end{pmatrix}
\]

Solution of \( AX = B \):

If \( D \neq 0 \), \( X = \begin{pmatrix} x \\ y \end{pmatrix} \). If \( D = 0 \) either there is no solution or there are infinite no. of solutions.
Let $X_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$ ..., $X_k = \begin{pmatrix} x_k \\ y_k \end{pmatrix}$

Then $A \times X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1,...,x_k \\ y_1,...,y_k \end{pmatrix}$

$= \begin{pmatrix} ax_1 + by_1,...,ax_k + by_k \\ cx_1 + dy_1,...,cx_k + dy_k \end{pmatrix}$

(a) Linear maps $C = aP$, where $a$ is invertible in $\mathbb{Z}/\mathbb{N}$.

(b) Affine maps $C = aP + b$, where $a$ is invertible in $\mathbb{Z}/\mathbb{N}$.

$A^{-1} = \begin{pmatrix} D^{-1}d - D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix}$

Let $M_2(\mathbb{R})$ denote the set of all $2 \times 2$ matrices with entries in $\mathbb{R}$.

Example: Find the inverse of $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(\mathbb{Z}/26\mathbb{Z})$

$D = 2.8 - 3.7 = -5 = 21$ in $\mathbb{Z}/26\mathbb{Z}$.

Since g.c.d. $(21, 26) = 1$, $D$ has an inverse, namely $21^{-1} = 5$; then

$A^{-1} = \begin{pmatrix} 5.8 & -5.3 \\ 5.7 & 5.2 \end{pmatrix} = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix} = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix}$

$\begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

A public key cryptosystem has the property that someone who knows how to encipher cannot use the enciphering key to find the deciphering key without a prohibitively lengthy computation. $f: P \rightarrow C$ is easy once $KE$ (enciphering key) is known. But $f^{-1}: C \rightarrow P$ is difficult to compute as $f$ is not always invertible. Hence $f$ is a one-way i.e. a trapdoor function.

Besides RSA system there are other types of public key cryptosystems.

1. Discrete log cryptosystem.
2. Diffie - Hellman cryptosystem
3. The ElGamal cryptosystem.
4. The Massey - Omura Cryptosystem.
Discrete log Method:

If \( G \) is a finite group, \( b \) is an element of \( G \), and \( g \) is an element of \( G \) and is a power of \( b \), then the discrete log of \( y \) to the base \( b \) is any integer \( x \) such that \( b^x = y \).

Example:

Let \( G = \mathbb{F}_{19}^* = (\mathbb{Z}/19\mathbb{Z})^* \cdot b = 2 \). Then discrete log of 7 to base 2 is 6.

Diffie-Hellman key exchange system:

To generate a random element of a large finite field \( \mathbb{F}_q \), suppose \( q \) is publicly known. Suppose \( g \) is some fixed element of \( \mathbb{F}_q \) which is not kept secret. We have to generate a key.

Suppose two users A and B want to agree upon a key-random element of \( \mathbb{F}_q^* \). A chooses an integer \( a \) between 1 and \( q-1 \) which he keeps secret and computes \( g^a \in \mathbb{F}_q \) which is made public. B chooses integer \( b \) between 1 and \( q-1 \) and makes \( g^b \) public. The secret key they use is \( g^{ab} \). For example A knows \( g^b \) and his secret key \( a \). A third party knows only \( g^a \) and \( g^b \), not \( a \) and \( b \). Without solving discrete log problem i.e. finding \( a \), knowing \( g \) and \( g^b \) - there is no way to compute \( g^{ab} \) knowing \( g^a \) and \( g^b \). Discrete log problem is not easy: to compute \( a \) from \( g^a \) or \( b \) from \( g^b \). So this system is secret.

The ElGamal Cryptosystem:

Fix very large finite field \( \mathbb{F}_q \) and an element \( g \in \mathbb{F}_q^* \). Suppose plaintext message unit has numerical equivalent \( P \) in \( \mathbb{F}_q \). Each user chooses an integer \( a = a_A \) in the range \( 0 < a < q-1 \). This \( a = a_A \) is the secret deciphering key, \( g^a \in \mathbb{F}_q \) is public enciphering key.

To send the message \( P \) to the user \( A \), we choose an integer \( k \) at random, and send \( A \) the pair \( (g^k, P \cdot g^{ak}) \).

Remark:

We can compute \( g^{ak} \) without knowing \( a \), simply raising \( g^a \) to the \( k \)th power. \( A \) can recover \( P \) from this pair raising \( g^k \) to the \( a \)th power and dividing the result into the second element or raising \( g^k \) to \( (q-1-a) \)th power and multiplying by \( g \) the second element. Here \( g^{ak} \) is the 'clue' or secret key.
There is no way to go from \( g^a \) and \( g^k \) to \( g^{ak} \) without solving discrete log problem.

**The Massey - Omura Cryptosystem:**

Here also the finite field \( \mathbb{F}_q \) is publicly known. Each user selects secretly an integer \( e = e_A \), \( 0 < e < q - 1 \) such that \( \text{g.c.d} \ (e, \ q - 1) = 1 \) and compute \( d = e^{-1} \mod q - 1 \).

Suppose \( A \) wants to send message \( P \) to \( B \). \( A \) sends \( P^{e_A} \).

Since \( B \) does not know \( d_A \) (or \( e_A \)) he cannot recover \( P \). \( B \) raises it to his chosen \( e_B \) and sends \( P^{e_A e_B} \) to \( A \). \( A \) unravels the message by raising to \( d_A \)-th power \( P^{d_A e_A} = P \) and \( A \) returns \( P^{e_B} \) to \( B \) who can read it by raising to his \( d_B \)-th power.

**5. Caution**

To maintain secrecy one has to use a good signature scheme with this system. Otherwise any person \( C \) who is not supposed to know \( P \), pretending to be \( B \) can send \( P^{e_A e_C} \) to \( A \) and he knows \( P \). From the pair \((P, P^{e_A})\), \( B \) can determine \( e_A \) and compute \( d_A = e_A^{-1} \mod q - 1 \) to recover the message.

**6. Application of Elliptic Curves in Cryptography**

In Number Theory and Algebraic Geometry, Elliptic curves are defined as follows:

Let \( K \) be a field of characteristic \( \neq 2, 3 \).

Let \( x^3 + ax + b \ (a, b \in K) \) be a cubic polynomial with no multiple root. An elliptic curve \( E \) over \( K \) is the set of points \((x, y)\) with \( x, y \in K \) which satisfy

(a) \( y^2 = x^3 + ax + b \)

together with a single element \( O \) (point at infinity).

**7. Application to Cryptosystem**

We encode our plaintext as points on some given elliptic curve \( E \) defined over a finite field \( \mathbb{F}_q \). The plaintext \( m \) can be determined from the knowledge of Co-ordinates of the corresponding points \( P_m \).

Discrete log on \( E \). Define an elliptic curve \( E \) over a finite field \( \mathbb{F}_q \). If \( B \) is a point of \( E \) then the discrete log problem on \( E \) (to the base \( B \)) is the problem,
given a point \( P \in E \), of finding an integer \( x \in \mathbb{Z} \) such that \( xB = P \) if such an integer exists.

8. ElGamal Cryptosystem for Elliptic Curve

Let the plaintext be \( P_m \). Let \( F_q \) be the fixed publicly known finite field. Let \( E \) be defined over \( F_q \). Let base point \( B \in E \). Each user chooses a random integer \( a \), which is kept secret and then computes and publishes \( aB \).

To send message \( P_m \) to \( B \), \( A \) chooses a random integer \( k \) and sends the pair of points \( (kB, P_m + k(aB)) \), where \( aB \) is \( B \)'s public key. To read the message, \( B \) multiplies the first point in the pair by his secret key \( aB \) and subtracts the result from the second point:

\[
P_m + k(aB) - aB(kB) = P_m.
\]

Thus \( A \) sends a disguised \( P_m \) along with a 'clue' \( kB \) which is enough to 'mark' \( aB \) if one knows the secret integer \( aB \). Here the main thing lies in choosing \((E, B)\), where \( B = (x,y) \in E \) and \( E \) is the elliptic curve defined in \( F_q \).

Elliptic curves have application to other cryptosystems also.

9. Analog of Diffie - Hellman key Exchange system

Suppose there are two users \( A \) and \( C \). Let us choose a finite field \( F_q \) and elliptic curve \( E \) defined over \( F_q \). \( A \) chooses an integer \( a \) (secret) and then computes \( aB \in E \) (basic known to both \( A \) and \( B \)) and makes \( aB \) public. Similarly \( C \) chooses \( c \) and make \( cB \in E \) public. Secret key is \( acBe E \). There is no way to compute \( acB \) knowing only \( aB \) and \( cB \), not \( a \) and \( c \).

10. Analog of Massey - Omura System

For message \( m \) suppose we have imbedded as points \( P_m \) on fixed elliptic curve \( E \) over \( F_q \). \( q \) is large. Suppose the number \( N \) of points on \( E \) has been computed. First \( A \) chooses \( e_A \) between 1 and \( N \) such that \( (e_A, N) = 1 \). Compute \( d_A = e^{-1}_A \pmod N \). \( A \) sends \( B \) the point \( e_A P_m \). \( B \) multiplies this with \( e_B \) and sends \( e_B e_A P_m \) to \( A \). Then \( A \) unravels the message part \( P_m \) to \( B \) by multiplying with \( d_A \) and returns back \( e_B P_m \) to \( B \). Now \( B \) reads the message by multiplying with \( d_B \), since \( P_m = d_B (e_B P_m) \).

Knowing \( e_B P_m, e_A P_m, e_B e_A P_m \) without solving discrete log problem the third party cannot read the message.
Conclusion:

The invention of the computer in the 20th century revolutionized cryptography. IBM corporation created a code, Data Encryption Standard (DES) that has not been broken to this day.

Watermarking with quadratic residue:

Very recently novel methods of watermarking data using quadratic residues and random numbers have been developed. These methods are fast, generic and improve the security of the watermark in most watermarking techniques. Watermarking is a technique for adding message, perhaps secret, to data to identify the owner or originators or to detect tampering with the data.

REFERENCES