EasyChair Preprint

№ 5137

Algebraic Methods for Cryptographic Bijective Functions

Narayanaswamy Chandramowliswaran

March 12, 2021

Algebraic Methods for Cryptographic Bijective Functions

N. Chandramowliswaran

Amity University, Haryana 122413

In this paper, we study an encryption scheme based on group algebra **G** over the boolean ring **R**. The key idea of the proposal is that for a given commutative ring, we can define different functions over $\mathbb{Z}_N$ and use them as the underlying structure. Using this group algebra **RG**, we are giving a criterion to encrypt the message and to retrieve it using the RSA Algorithm. For the decryption algorithm to work, without any loss of data, the invertibility of the latin square over **R** is the necessary condition.

Keywords: Cryptographic bijective functions; One-way functions; Boolean Rings; Trace; Automorphism; Group Algebra; Partition of a set

AMS Classification: 94A60, 94A62, 03G05

1. Introduction

1.1 Public Key Cryptography

In 1976, Whitefield Diffie and Martin Hellman published the first practical public key cryptosystem for secure data transmission [10]. The Diffie-Hellman Algorithm was based on the discrete log problem. Since then, many public key cryptography algorithms have been created. The RSA scheme [9] discovered in 1978 by Ron Rivest, A. Shamir and Adleman was based on the factorization problem of the modulus, factorising of $\boldsymbol{mod\ N}$ is an impractical task if the integer $\boldsymbol{N}$ is sufficiently large, where $\boldsymbol{N}$ is the product of two distinct large primes. Since then, many developments have been made in the field of cryptography. Elliptic Curves based Cryptography has an advantage over the non-elliptic curve cryptography with the smaller key sizes [4][5]. Elliptic Curve cryptography is based on the algebraic structure of elliptic curves over finite fields.

Here, we are using Special finite non-abelian groups in order to make the bijective functions more efficient and suitable for encryption and decryption purpose. We are introducing the concept strongly co – prime integers for constructing more trap door functions . In this paper , we study some important properties of strongly co-prime integers and their effective use in public key cryptography.

In recent past many works have been done to improve the cryptosystems using the group algebra over commutative and non-commutative rings.

It is necessary for a good cryptosystem to be practically impossible for the attacker to break [2]. A good cryptosystem would comparatively take more time while the attacker is trying to break into it. This can either be achieved by making a moderately longer key or by creating a more advance algorithm that would make the entire cryptosystem reluctant to any damage.

Here, in this paper, we present some new techniques to encrypt and decrypt the messages. Some basic concepts of group algebra and, linear algebra have been used and applied to make a new algorithm. The RSA Algorithm [8] has been used as the basis of the cryptosystem whose definition we would like to record:

Encryption: Given the public key $(n, e) = k_{pub}$ and the plaintext x, the encryption function is $\boldsymbol{y = e_{k_{pub}}(x) \equiv x^e\ mod\ n}$, where $x, y \in \mathbb{Z}_n$.

Decryption: Given the private key $d = k_{pr}$ and the ciphertext y, the decryption function is $\boldsymbol{x = d_{k_{pr}}(y) \equiv y^d mod\ n}$, where $x, y \in \mathbb{Z}_n$.

Here, $ed \equiv 1\ (mod\ (p-1)(q-1))$ and $n = pq$

Theorem 1.1 (RSA) *The mapping $f : \mathbb{Z}_n \to \mathbb{Z}_n$ where n is the product of k distinct odd primes, $f(x) = x^e (Mod\ n)$ such that $gcd(e, (p_1 - 1)(p_2 - 1) \dots (p_k - 1)) = 1$ is bijective.*

Here, $ed \equiv 1\left((Mod((p_1-1)(p_2-1)\dots(p_k-1))\right)$ *and* $n = p_1.p_2 \dots p_k$

For a function $'f'$, if there exist some secret information $'y'$, such that if $f(x)$ and y are known, then x can be computed easily. Such a function is known as the trapdoor function. A **trapdoor function** is a functionthat is easy to compute in one direction, yet difficult to compute in the opposite direction (finding its inverse) without special information, called the "trapdoor". A **one-way function** is a function that is easy to compute on every input, but hard to invert given the image of a random input. In this direction, many researchers started constructing trap door permutation polynomial over finite fields. Now we would like to recall an interesting result due to R.A. Mollin and C. Small. [8]

Theorem 1.2: *Let* $GF(q)$ *be a given finite field with q elements having characteristic different from* $'3'$.

Then $f(x) = ax^3 + bx^2 + cx + d \ \ (a \neq 0)$ *permutes* $GF(q)$ *if and only if*

$$b^2 = 3ac \text{ and } q \equiv 2(Mod\ 3)$$

Now, let us use this theorem for constructing a permutation polynomial over $\mathbb{Z}_p$ for large odd prime p $(p \neq 3)$.

Using the quadratic reciprocity law, we can deduce the following theorem

Choose an odd prime p such that $p \equiv 11\ (Mod\ 12)$

Then choose $a, c \in$ set of quadratic residues $mod\ p$ or $a, c \in$ set of quadratic non-residues $mod\ p$

Then the polynomial $f(x) = \ ax^3 + bx^2 + cx\ + d \in \ \mathbb{Z}_p[x]$ permutes $\mathbb{Z}_p$.

If we choose a prime p such that $p \equiv 5\ (Mod\ 12)$,

Then we have to select $a \in$ set of quadratic residues $mod\ p$ but $c \in$ set of quadratic non-residues $mod\ p$

or if $a \in$ set of quadratic non-residues $mod\ p$ and $c \in$ set of quadratic residues $mod\ p$

Then the polynomial $f(x) = \ ax^3 + bx^2 + cx\ + d \in \ \mathbb{Z}_p[x]$ permutes $\mathbb{Z}_p$.

Let us now observe, how we can use some elementary number theory to construct some simple encryption and decryption schemes.

For more works on Analytic Number theory, the reader may refer to [1].

1.2 Some examples to construct bijective functions

In this section, we give some more methods for the secure encryption of data using different fields like vectors, rings, matrices etc. This can be understood better with help of the following theorems and examples.

Example 1.1: Select Four Secret distinct positive integers a, b, P, Q where P and Q are very large odd primes such that $ab > PQ$

Define $M = ab - PQ$

Set $e = (PQ)^2M + a$ and $d = (PQ)M + b$

Consider $ed - PQ = M((PQ)^3M + a(PQ) + b(PQ)^2 + 1\ )$

Define $N = (PQ)^3M + a(PQ) + b(PQ)^2 + 1$

Then, we observe: $\gcd(e, N) = \gcd(d, N) = 1$

Define $\mathbb{Z}_N = \{0, 1, 2, \dots, N-1\}$

The map $f: \mathbb{Z}_N^{(2)} \to \mathbb{Z}_N^{(2)}$ defined by $f(x, y) = (ex\ (Mod\ N), dy\ (Mod\ N))$ is bijective.

Example 1.2: Let us now extend the above example further

Take four distinct positive integers a, b, c, P where P is an odd prime. such that $abc > P$.

Define $M = abc - P$

Set $e = P^3M + a$; $d = P^2M + b$, and $f = PM + c$.

Now, construct $edf - P = M(P^6M^2 + aP^3M + bP^4M + abP + P^5Mc + acP^2 + bcP^3 + 1)$

Then, we observe: $\gcd(e, N) = \gcd(d, N) = \gcd(f, N) = 1$

The map $\phi: \mathbb{Z}_N^{(3)} \to \mathbb{Z}_N^{(3)}$ defined by $\phi(x,y,z) = (ex\ (Mod\ N), dy\ (Mod\ N), fz\ (Mod\ N))$ is bijective.

Example 1.3: Let us take four distinct positive integers $\boldsymbol{a, b, c, d}$ greater than or equal to 2.
Define $N = \big(abcd(a+1)(b+1)(c+1)(d+1)\big) + 1$
Here, we observe that $\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{N}) = \mathbf{gcd}(\boldsymbol{b}, \boldsymbol{N}) = \mathbf{gcd}(\boldsymbol{c}, \boldsymbol{N}) = \mathbf{gcd}(\boldsymbol{d}, \boldsymbol{N}) = \mathbf{1}$
and, $\mathbf{gcd}(\boldsymbol{a+1}, \boldsymbol{N}) = \mathbf{gcd}(\boldsymbol{b+1}, \boldsymbol{N}) = \mathbf{gcd}(\boldsymbol{c+1}, \boldsymbol{N}) = \mathbf{gcd}(\boldsymbol{d+1}, \boldsymbol{N}) = \mathbf{1}$
also, $\mathbf{gcd}\big(\boldsymbol{a(a+1)^2}, \boldsymbol{N}\big) = \mathbf{1}$
Define $\mathbb{Z}_N = \{0, 1, 2, \ldots N-1\}\ (Mod\ N)$ a ring of integers with respect to $+_N$ and $\times_N$.
Now, let us construct a bijective function $f: \mathbb{Z}_N^{(3)} \to \mathbb{Z}_N^{(3)}$
$f(x,y,z) = (u,v,w)$
where $u = a^2x - ay + k$
$v = (2a+1)x + ay + l$
$w = az + m,$
Here, $k, l, m \in \mathbb{Z}_N$.
Similarly, $'a'$ can be replaced by $'b',\ 'c'\ and\ 'd'$.

Example 1.4: Define $\mathcal{F} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \begin{matrix} a,b,c,d\ \in \mathbb{Z}_{pos} \\ (a,b) = (c,d) = 1 \\ (a,c) = (b,d) = 1 \end{matrix} \right\}$

Proposition 1.1: Suppose $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathcal{F}$
Then $\begin{bmatrix} a\alpha & b\beta \\ c\gamma & d\delta \end{bmatrix} \in \mathcal{F}$ if and only if $\begin{bmatrix} a & \beta \\ \gamma & d \end{bmatrix}, \begin{bmatrix} \alpha & b \\ c & \delta \end{bmatrix} \in \mathcal{F}$.
Proof: $(a\alpha, b\beta) = (a,b) \times (\alpha,\beta) \times \left(\frac{a}{(a,b)}, \frac{\beta}{(\alpha,\beta)}\right) \times \left(\frac{b}{(a,b)}, \frac{\alpha}{(\alpha,\beta)}\right)$
Similarly, $(a\alpha, c\gamma) = (a,c) \times (\alpha,\gamma) \times \left(\frac{a}{(a,c)}, \frac{\gamma}{(\alpha,\gamma)}\right) \times \left(\frac{c}{(a,c)}, \frac{\alpha}{(\alpha,\gamma)}\right)$
Therefore, $(a\alpha, b\beta) = (a,\beta) \cdot (b,\alpha)$
Similarly, $(c\gamma, d\delta) = (c,\delta) \cdot (d,\gamma)$
$(b\beta, d\delta) = (b,\delta) \cdot (\beta,d)$
$(a\alpha, c\gamma) = (a,\gamma) \cdot (c,\alpha)$

Proposition 1.2: Suppose $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathcal{F}$
Define $\boldsymbol{N} = a\alpha d\delta + c\gamma b\beta$
$\boldsymbol{N_1} = ad + \beta\gamma$
$\boldsymbol{N_2} = \alpha\delta + bc$
Assume $\begin{bmatrix} a\alpha & b\beta \\ c\gamma & d\delta \end{bmatrix} \in \mathcal{F}$
Define $f: \mathbb{Z}_N^{(3)} \to \mathbb{Z}_N^{(3)}$
$f(x,y,z) = (\alpha' + (a\alpha + d\delta)x + d\delta y\ (Mod\ N), \beta' + c\gamma x + c\gamma y (Mod\ N), \gamma' + (b^2\beta^2 c\gamma)z\ (Mod\ N))$
$f_1: \mathbb{Z}_{N_1}^{(3)} \to \mathbb{Z}_{N_1}^{(3)}$
$f_1(x,y,z) = (\alpha'' + (a\gamma + d)x\ + dy(Mod\ N_1), \gamma x + \gamma y + \beta''(Mod\ N_1), \gamma'' + (\beta^2\gamma)z(Mod\ N_1))$
$f_2: \mathbb{Z}_{N_2}^{(3)} \to \mathbb{Z}_{N_2}^{(3)}$
$f_2\ (x,y,z) = (\alpha''' + (\alpha c + \delta)x\ + \delta y\ (Mod\ N_2), \beta''' + cx + cy\ (Mod\ N_2), \gamma''' + (b^2 c)z(Mod\ N_2))$
Then, f is bijective if and only if $f_1\ and f_2$ are bijective.

Example 1.5: Let p, q, r be three given (distinct) odd primes
Assume $r^2 + q \not\equiv 0\ (Mod\ p)$
Consider the following 2×2 matrix "A"

$$A = \begin{bmatrix} r & p + qr \\ pq + pr^2 & q^2 + pr + qr^2 \end{bmatrix}$$

$$Per(A) = rq^2 + pr^2 + qr^3 + p^2q + p^2r^2 + pq^2r + pqr^3$$
$$= (pq + q)r^3 + (p + p^2)r^2 + (pq^2 + q^2)r + p^2q$$

Define $N := Per\ (A)$
$$= (pq + q)r^3 + (p + p^2)r^2 + (pq^2 + q^2)r + p^2q\ ,$$

Now, we can show that
$\gcd(r(pq + pr^2), N) = 1$
$\gcd((p + qr)(q^2 + pr + qr^2), N) = 1$
$\gcd(r(p + qr), N) = 1$
$\gcd\big((pq + pr^2)(q^2 + pr + qr^2), N\big) = 1$
Define a bijective map $f : \mathbb{Z}_N^{(3)} \to \mathbb{Z}_N^{(3)}$ as follows:

$$f(x, y, z) = ([\alpha + (qr^2 + (p + 1)r + q^2)x + (q^2 + pr + qr^2)y]\ (Mod\ N),$$
$$[\beta + (pq + pr^2)(x + y)](Mod\ N), [\gamma + (p + qr)^2(pq + pr^2)z](Mod\ N))$$

$$Det \begin{bmatrix} qr^2 + (p + 1)r + q^2 & q^2 + pr + qr^2 \\ pq + pr^2 & pq + pr^2 \end{bmatrix} = [(pq + pr^2)(r)]\ (Mod\ N)$$

So, $\gcd([(pq + pr^2)(r)]\ , N) = 1$
Therefore "f" is bijective.

Proposition 1.3. *Let $\boldsymbol{a}$ be the non-zero vector in $\mathbb{R}^3$. Then $T_{\boldsymbol{a}}(x) = (\boldsymbol{a} \times \boldsymbol{x}) - \boldsymbol{a} - \boldsymbol{x}$, and $S_a(x) = \boldsymbol{x} \times \boldsymbol{a} - \boldsymbol{a} - \boldsymbol{x}$, $a \times x$, $x \times a$ denotes vector cross product in R^3 is bijective from $\mathbb{R}^3$ to $\mathbb{R}^3$.*
If we consider $\vec{\boldsymbol{a}} = (a_1, a_2, a_3) \in \mathbb{Z}_p^3$ over a finite field with p where p is an odd-prime. Then the map $T_a(x)$ is bijective if and only if $a_1^2 + a_2^2 + a_3^2 \not\equiv -1(mod\ p)$.

Theorem 1.3: *Let $\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}}$ be any non-zero vectors and y is any vector in R^3.*
Then $T_{(\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}})}(\vec{y}) = (\vec{\boldsymbol{b}} \cdot \vec{y})\vec{\boldsymbol{a}} - (\vec{b} \cdot \vec{a})\vec{y} + (\vec{y} \times \vec{a}) + (\vec{y} \times \vec{b}) + \vec{y} + (\vec{a} \times \vec{b}) + \vec{a} - \vec{b}$ is a bijective map from $\mathbb{R}^3$ onto $\mathbb{R}^3$.
Proof:
Let $\vec{a}$ be a given non-zero vector in R^3.
Define: $T_{\vec{a}}(\vec{x}) = \vec{a} \times \vec{x} - \vec{a} - \vec{x}$
$S_{\vec{a}}(\vec{x}) = \vec{x} \times \vec{a} - \vec{a} - \vec{x}$
$T_{\vec{a}}$, $S_{\vec{a}}$ both are bijective maps from R^3 onto itself.
Select $\vec{a}$, $\vec{b}$ are given non-zero vectors in R^3.
Now, let us compute $S_{\vec{b}} \circ T_{\vec{a}} : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$

$$S_{\vec{b}} \circ T_{\vec{a}} = S_{\vec{b}}(T_{\vec{a}}(x))$$
$$= S_{\vec{b}}(\vec{a} \times \vec{x} - \vec{a} - \vec{x})$$
$$= (\vec{a} \times \vec{x} - \vec{a} - \vec{x}) \times \vec{b} - (\vec{a} \times \vec{x} - \vec{a} - \vec{x}) - \vec{b}$$
$$= (\vec{a} \times \vec{x}) \times \vec{b} - (\vec{a} \times \vec{b}) - (\vec{x} \times \vec{b}) - (\vec{a} \times \vec{x}) + \vec{a} + \vec{x} - \vec{b}$$
$$= (\vec{a} \times \vec{x}) \times \vec{b} + (\vec{b} \times \vec{a}) + (\vec{b} \times \vec{x}) + (\vec{x} \times \vec{a}) + \vec{a} + \vec{x} - \vec{b}$$
$$= (\vec{a} \bullet \vec{b})\vec{x} - (\vec{x} \bullet \vec{b})\vec{a} + (\vec{x} \times \vec{a}) + (\vec{b} \times \vec{x}) + \vec{x} + (\vec{b} \times \vec{a}) + \vec{a} - \vec{b}$$

Now, we use the above-mentioned theorems to prove some corollaries.

Corollary 1.1: *Let* $\vec{a} = (a_1, a_2, a_3) \in \mathbb{Z}_N^{(3)}$ *form a commutative ring with respect to* $+_N$ *and* $\times_N$. $T_{\vec{a}} : \mathbb{Z}_N^{(3)} \longrightarrow \mathbb{Z}_N^{(3)}$ *defined by* $T_{\vec{a}}(x) = \vec{a} \times \vec{x} - \vec{a} - \vec{x}$ *for all* $x \in \mathbb{Z}_N$. Then $T_{\vec{a}}$ is a bijective function if and only if $(a_1^2 + a_2^2 + a_3^2) \equiv r' - 1 \ (mod\ N)$, where $\gcd(r', N) = 1$.

Proof:

Suppose $T_a(\vec{x}) = T_a(\vec{y})$ for all $x, y \in \mathbb{Z}_N$. Then

$\vec{a} \times \vec{x} - \vec{a} - \vec{x} = \vec{a} \times \vec{y} - \vec{a} - \vec{y}$

$(\vec{a}) \times \big((\vec{x}) - (\vec{y})\big) = \big((\vec{x}) - (\vec{y})\big)$

$$\begin{vmatrix} i & j & k \\ a_1 & a_2 & a_3 \\ x_1 - y_1 & x_2 - y_2 & x_3 - y_3 \end{vmatrix} = (x_1 - y_1, x_2 - y_2, x_3 - y_3)$$

$$\big(a_2(x_3 - y_3) - a_3(x_2 - y_2), \quad a_3(x_1 - y_1) - a_1(x_3 - y_3), \quad a_1(x_2 - y_2) - a_2(x_1 - y_1)\big) = (x_1 - y_1, x_2 - y_2, x_3 - y_3)$$

$-(x_1 - y_1) - a_3(x_2 - y_2) + a_2(x_3 - y_3) = 0$

$a_3(x_1 - y_1) - (x_2 - y_2) + a_1(x_3 - y_3) = 0$

$-a_2(x_1 - y_1) + a_1(x_2 - y_2) - (x_3 - y_3) = 0$

$$\begin{pmatrix} -1 & -a_3 & a_2 \\ a_3 & -1 & -a_1 \\ -a_2 & a_1 & -1 \end{pmatrix} \begin{pmatrix} x_1 - y_1 \\ x_2 - y_2 \\ x_3 - y_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

In order to get a trivial solution, we must have

$$\det \begin{pmatrix} -1 & -a_3 & a_2 \\ a_3 & -1 & -a_1 \\ -a_2 & a_1 & -1 \end{pmatrix} \in U(\mathbb{Z}_N)$$

Let us consider

$$l = \begin{vmatrix} -1 & -a_3 & a_2 \\ a_3 & -1 & -a_1 \\ -a_2 & a_1 & -1 \end{vmatrix}$$

then $\gcd(l \ mod\ N,\ N) = 1$

Now, let us compute $l \ mod\ N$

$\big(-1(1 + a_1^2) + a_3(-a_3 - a_1 a_2) + a_2(a_1 a_3 - a_2)\big) mod\ N$

$\gcd(-(1 + a_1^2 + a_2^2 + a_3^2) mod\ N, N) = 1$

$-(1 + a_1^2 + a_2^2 + a_3^2) \equiv r \ (mod\ N)$, where $\gcd(r, N) = 1$

$(1 + a_1^2 + a_2^2 + a_3^2) \equiv -r \ (mod\ N)$

$(a_1^2 + a_2^2 + a_3^2) \equiv N - r - 1 \ (mod\ N)$

$(a_1^2 + a_2^2 + a_3^2) \equiv r' - 1 \ (mod\ N)$, where $\gcd(r', N) = 1$

$T_{\vec{a}} : \mathbb{Z}_N^{(3)} \longrightarrow \mathbb{Z}_N^{(3)}$ is bijective if and only if $(a_1^2 + a_2^2 + a_3^2) \equiv r' - 1 \ (mod\ N)$, where $\gcd(r', N) = 1$

Corollary1. 2

Let, $\vec{a}, \vec{b} \in \mathbb{Z}_N^{(3)}$ with $\vec{a} = (a_1, a_2, a_3)$, $\vec{b} = (b_1, b_2, b_3)$.

$(a_1^2 + a_2^2 + a_3^2) \equiv r' - 1 \ (mod\ N)$

$(b_1^2 + b_2^2 + b_3^2) \equiv s' - 1 \ (mod\ N)$

where $\gcd(r', N) = \gcd(s', N) = 1$.

$T_{(\vec{a},\vec{b})}(\vec{x}) = \big(\vec{b} \bullet \vec{x}\big)\vec{a} - \big(\vec{b} \bullet \vec{a}\big)\vec{x} + (\vec{x} \times \vec{a}) + \big(\vec{x} \times \vec{b}\big) + \vec{x} + \big(\vec{a} \times \vec{b}\big) + \vec{a} - \vec{b}$ is bijective from $\mathbb{Z}_N^{(3)}$ *to* $\mathbb{Z}_N^{(3)}$.

2. Encryption and Decryption over Finite Boolean Rings

2.1 Boolean Rings

Now we shall see how to reconstruct the original message text using boolean rings over group algebras. In this context, let us review the definition of Boolean Rings [3].

Let X be any given finite set (non-empty).Consider $\mathcal{P}(X) = \{set\ of\ ALL\ subsets\ of\ X\}$

Define $\oplus$ and $\bullet$ on $\boldsymbol{\mathcal{P}(X)}$ as follows:

$$\boldsymbol{A \oplus B = (A - B) \cup (B - A)}$$

$$\boldsymbol{A \bullet B = A \cap B,} \qquad \boldsymbol{where\ A, B \in \mathcal{P}(X)}$$

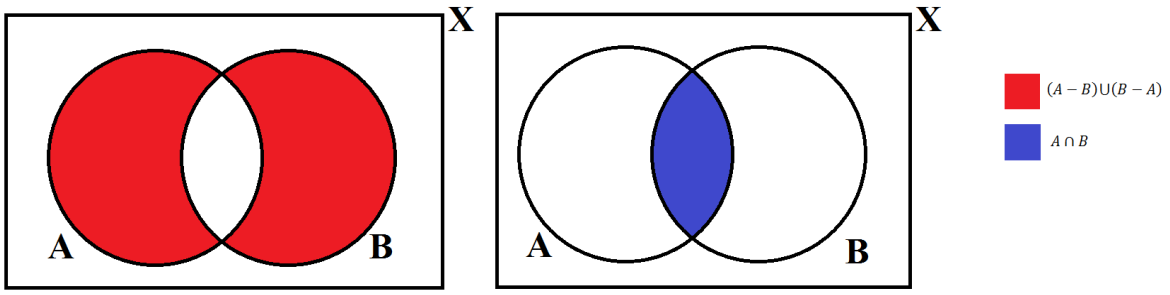

Figure 1 : Boolean Ring

This ring is:

a) Commutative

$A \oplus B = B \oplus A$

$A \bullet B = B \bullet A$, where $A, B \in \mathcal{P}(X)$

b) Associative

$A \oplus (B \oplus C) = (A \oplus B) \oplus C$

$A \bullet (B \bullet C) = (A \bullet B) \bullet C$, where $A, B, C \in \mathcal{P}(X)$

c) Distributive

$(A \oplus B) \bullet C = (A \bullet C) \oplus (B \bullet C)$

$(A \bullet B) \oplus C = (A \oplus C) \bullet (B \oplus C)$, where $A, B, C \in \mathcal{P}(X)$

The empty set (ϕ) is the **zero** of the ring.

The finite set X is the **one** of the ring.

Hence, $(\mathcal{P}(X), \oplus, \bullet, \phi, X)$ forms a *Boolean Ring*.

Let $\boldsymbol{\mathcal{U}} = \begin{bmatrix} A & B \\ C & D \end{bmatrix}, \boldsymbol{\mathcal{V}} = \begin{bmatrix} E & F \\ G & H \end{bmatrix}$,

then the matrix multiplication is defined as follows:

$$\boldsymbol{\mathcal{U} \cdot \mathcal{V}} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \cdot \begin{bmatrix} E & F \\ G & H \end{bmatrix} = \begin{bmatrix} AE \oplus BG & AF \oplus BH \\ CE \oplus DG & CF \oplus DH \end{bmatrix} \qquad \langle AB = A \bullet B \rangle$$

$$where, A, B, C, D, E, F, G, H \in \mathcal{P}(X)$$

While decrypting the message, the invertibility of the latin square, formed over the boolean ring **R,** is a necessary condition. That latin square can be formed using various techniques mentioned below.

Main Result: Encryption schemes over square matrices

In this section we give an algorithm to encrypt as well as decrypt the data using square matrices. Here, the square matrices are constructed with its elements from the power set of the boolean set $\boldsymbol{X}$.

Let $\boldsymbol{\mathcal{M}} = \begin{bmatrix} Y_1 \\ Y_2 \\ Y_3 \end{bmatrix}$ be the message that we have to encrypt. Where $Y_1, Y_2, Y_3 \in \boldsymbol{X}$

To encrypt the message, we need a key.

Let $\boldsymbol{\mathcal{K}} = \begin{bmatrix} X \oplus AE \oplus BF & A \oplus BG & B \\ E \oplus CF & X \oplus CG & C \\ F & G & X \end{bmatrix}$ be the Encryption key, $Det(\boldsymbol{\mathcal{K}}) = X$.

$where, A, B, C, E, F, G \in \mathcal{P}(X)$

Define $Enc(\boldsymbol{\mathcal{M}}) = \boldsymbol{\mathcal{K}} \cdot \boldsymbol{\mathcal{M}}$

$$= \begin{bmatrix} X \oplus AE \oplus BF & A \oplus BG & B \\ E \oplus CF & X \oplus CG & C \\ F & G & X \end{bmatrix} \cdot \begin{bmatrix} Y_1 \\ Y_2 \\ Y_3 \end{bmatrix} = \begin{bmatrix} Y_1' \\ Y_2' \\ Y_3' \end{bmatrix} \ (say)$$

$$= \begin{bmatrix} Y_1 \oplus BFY_1 \oplus AY_2 \oplus BGY_2 \oplus BY_3 \\ EY_1 \oplus CFY_1 \oplus Y_2 \oplus CGY_2 \oplus CY_3 \\ FY_1 \oplus GY_2 \oplus Y_3 \end{bmatrix} = \begin{bmatrix} Y_1' \\ Y_2' \\ Y_3' \end{bmatrix}$$

Here,

$Y_1' = Y_1 \oplus BFY_1 \oplus AY_2 \oplus BGY_2 \oplus BY_3$

$Y_2' = EY_1 \oplus CFY_1 \oplus Y_2 \oplus CGY_2 \oplus CY_3$

$Y_3' = FY_1 \oplus GY_2 \oplus Y_3$

To decrypt this message,

$D_n(\boldsymbol{\mathcal{M}}) = \boldsymbol{\mathcal{K}}^{-1}$

$$= \frac{1}{X} \begin{bmatrix} X & A & AC \oplus B \\ E & X \oplus AE & C \oplus CAE \oplus BE \\ F & G \oplus GAE \oplus AF & X \oplus BF \oplus CG \oplus EBG \oplus CGAE \end{bmatrix}$$

$$= \begin{bmatrix} X & A & AC \oplus B \\ E & X \oplus AE & C \oplus CAE \oplus BE \\ F & G \oplus GAE \oplus AF & X \oplus BF \oplus CG \oplus EBG \oplus CGAE \end{bmatrix} \qquad |\because X \ is \ the \ \boldsymbol{one} \ in \ the \ ring \ \mathcal{P}(X)|$$

Here, as we have mentioned, that in a Boolean Ring, the **one** $(\mathbf{1})$ of the ring is the finite set $\boldsymbol{X}$**.** In order to maintain the invertibility of the matrix, it is important that we construct the matrices with their determinant $= \boldsymbol{X}$**.** This determinant being equal to the **one** of the finite ring ensures the invertibility and hence the decryption is possible without the loss of data.

Some of the methods to construct such matrices have been discussed below.

2.1 To Construct a square matrix with determinant = *X using triangular matrices*

Let X be any given finite set (non-empty). Consider $\mathcal{P}(X) = \{set \ of \ ALL \ subsets \ of \ X\}$

Define $\oplus$ and $\bullet$ on $\mathcal{P}(X)$ as follows:

$$A \oplus B = (A - B) \cup (B - A) = B \oplus A$$
$$A \bullet B = A \cap B = B \bullet A, \qquad where \ A, B \in \mathcal{P}(X)$$

Define two square matrices λ and μ

$$\boldsymbol{\mathcal{U}} = \begin{bmatrix} X & A & B \\ \phi & X & C \\ \phi & \phi & X \end{bmatrix}; \ \boldsymbol{\mathcal{V}} = \begin{bmatrix} X & \phi & \phi \\ E & X & \phi \\ F & G & X \end{bmatrix} \ where \ A, B, C, E, F, G \in \mathcal{P}(X)$$

$$\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}} = \begin{bmatrix} X \oplus AE \oplus BF & \phi \oplus AX \oplus BG & \phi \oplus BX \\ \phi \oplus E \oplus CF & \phi \oplus X \oplus CG & \phi \oplus \phi \oplus C \\ \phi \oplus XF & \phi \oplus G & X \end{bmatrix}$$

$$\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}} = \begin{bmatrix} X \oplus AE \oplus BF & A \oplus BG & B \\ E \oplus CF & X \oplus CG & C \\ F & G & X \end{bmatrix} \rightarrow (\boldsymbol{K})$$

$$\det(\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}}) = [(X \oplus AE \oplus BF)(X \oplus CG \oplus CG)] \oplus [(A \oplus BG)(E \oplus CF \oplus CF)] \oplus [B(EG \oplus CFG \oplus F \oplus CGF)]$$
$$= X \oplus AE \oplus BF \oplus AE \oplus BGE \oplus BEG \oplus BF$$
$$= X$$

Example 2.1

Assume $X = \{1,2,3,4,5\}$ and $\mathcal{P}(X) be\ the\ power\ set\ of\ X$

$$\boldsymbol{\mathcal{U}} = \begin{bmatrix} X & \{1,2\} & \{2,3\} \\ \phi & X & \{1,2,3\} \\ \phi & \phi & X \end{bmatrix};\ \boldsymbol{\mathcal{V}} = \begin{bmatrix} X & \phi & \phi \\ \{1,3\} & X & \phi \\ \{1,2\} & \{3,4\} & X \end{bmatrix}$$

$$\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}} = \begin{bmatrix} \{3,4,5\} & \{1,2,3\} & \{2,3\} \\ \{2,3\} & \{1,2,4,5\} & \{1,2,3\} \\ \{1,2\} & \{3,4\} & X \end{bmatrix}$$

here, $\det(\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}}) = X$

Similarly, using different finite non-empty sets "X" and taking different elements from their power set, we can obtain infinite number of square matrices of any order.

Similarly, we can create a 4-square matrix by multiplying $\boldsymbol{\mathcal{U}} = \begin{bmatrix} X & A & B & C \\ \phi & X & D & E \\ \phi & \phi & X & F \\ \phi & \phi & \phi & X \end{bmatrix}$ and

$\boldsymbol{\mathcal{V}} = \begin{bmatrix} X & \phi & \phi & \phi \\ G & X & \phi & \phi \\ H & I & X & \phi \\ J & K & L & X \end{bmatrix}$ in order to get a 4-sqaure matrix $\boldsymbol{\mathcal{D}} = \boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}}$ whose determinant $= X$.

$\boldsymbol{\mathcal{D}} = \boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}} = \begin{bmatrix} X \oplus AG \oplus BH \oplus CJ & A \oplus BI \oplus CK & B \oplus CL & C \\ G \oplus DH \oplus EJ & X \oplus DI \oplus EK & D \oplus EL & E \\ H \oplus FJ & I \oplus FK & X \oplus FL & F \\ J & K & L & X \end{bmatrix}$ where $A, B, C, D, E, F, G, H, I, J, K, L \in \mathcal{P}(X)$.

2.2 To construct a square matrix with determinant = *X using square tridiagonal matrices*

Let X be any given finite set (non-empty). Consider $\mathcal{P}(X) = \{set\ of\ ALL\ subsets\ of\ X\}$

Let $\boldsymbol{\mathcal{U}} = \begin{bmatrix} X & A & \phi \\ B & X & A \\ \phi & B & X \end{bmatrix}$ and $\boldsymbol{\mathcal{V}} = \begin{bmatrix} X & C & \phi \\ D & X & C \\ \phi & D & X \end{bmatrix}$, we have $Det(\boldsymbol{\mathcal{U}}) = Det(\boldsymbol{\mathcal{V}}) = X$.

Here, $A, B, C, D \in \mathcal{P}(X)$

$\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}} = \begin{bmatrix} X \oplus AD & C \oplus A & CA \\ B \oplus D & X \oplus BC \oplus AD & C \oplus A \\ BD & B \oplus D & X \oplus BC \end{bmatrix}$, $Det(\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}}) = Det(\boldsymbol{\mathcal{U}}) \cdot Det(\boldsymbol{\mathcal{V}}) = X \cdot X = X$

Example 2.2

Assume $X = \{1,2,3,4,5\}$ and $\mathcal{P}(X) be\ the\ power\ set\ of\ X$.

$$\boldsymbol{\mathcal{U}} = \begin{bmatrix} X & \{2,3\} & \phi \\ \{1,2,3\} & X & \{2,3\} \\ \phi & \{1,2,3\} & X \end{bmatrix};\ \boldsymbol{\mathcal{V}} = \begin{bmatrix} \{3,4,5\} & \{1,2,3\} & \{2,3\} \\ \{2,3\} & \{1,2,4,5\} & \{1,2,3\} \\ \{1,2\} & \{3,4\} & X \end{bmatrix}$$

$$\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}} = \begin{bmatrix} \{2,4,5\} & \{1,2,3\} & \phi \\ \phi & \{4,5\} & \{1,2,3\} \\ \{1,3\} & \{1,2,3,4\} & \{4,5\} \end{bmatrix}$$

$Det(\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}}) = X$

2.3 To construct a square matrix with determinant = *X using partitions of a set*

Let "X" be a non-empty finite set,

$$X = \{a_1, a_2, a_3, \dots, a_n\}$$

Define $A_1, A_2, A_3, \dots, A_n$ as the partitions of the set X.

$$X = \bigcup_{i=1}^{n} A_i\ ;\ A_i \cap A_j = \phi\ \forall\ i \neq j.$$

Create a matrix "$\boldsymbol{\mathcal{U}}$" using the $A_i s$ as latin square.

$$Det(\boldsymbol{U}) = A_1 \oplus A_2 \oplus A_3 \oplus \ldots \oplus A_n = X$$

Example 2.3:
Let $X = \{a, b, c, d, e, f, g\}$
$A_1 = \{a, c, d\}$
$A_2 = \{b, e\}$
$A_3 = \{f\}$
$A_4 = \{g\}$
Here, A_1, A_2, A_3, A_4 are partitions of X.
Define $\boldsymbol{U} = \begin{bmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2 & A_1 & A_4 & A_3 \\ A_3 & A_4 & A_1 & A_2 \\ A_4 & A_3 & A_2 & A_1 \end{bmatrix}$

$$Determinant = \sum_{\sigma \in S_n} (-1)^{\sigma} a_{1\,\sigma(1)} \cdot a_{2\,\sigma(2)} \cdot a_{3\,\sigma(3)} \ldots a_{n\,\sigma(n)}$$

Hence, $Det(\boldsymbol{U}) = A_1 \oplus A_2 \oplus A_3 \oplus A_4 = X$

3. Public Key Cryptography using Permanent and Trace of Matrices

In a square matrix, the permanent of a matrix is defined as follows:

$$Per(U) = \sum_{\sigma \in S_n} a_{1\,\sigma(1)} \cdot a_{2\,\sigma(2)} \cdot a_{3\,\sigma(3)} \ldots a_{n\,\sigma(n)}$$

3.1 Encryption Scheme using the Permanent of a Matrix

1. Consider the following 3×3 matrix

$A = \begin{bmatrix} p & p^2 & s \\ q & q^3 & r^3 \\ r & p^4 & r^2 \end{bmatrix}$ where p, q, r, s are all distinct odd primes with

$p^3 + r \not\equiv 0\ (Mod\ q)$
$q^3 + p^4 r + pq + pr^2 \not\equiv 0\ (Mod\ s)$

STEP 1:
Arbitrary select p, r distinct odd primes.
STEP 2:
Choose an odd prime "q" which is distinct from p, r such that

$$p^3 + r \not\equiv 0\ (Mod\ q)$$

STEP 3:
Select an odd prime "s" which is distinct from p, q, r such that

$$q^3 + p^4 r + pq + pr^2 \not\equiv 0\ (Mod\ s)$$

2. Here,
$Per(A) = pq^3 r^2 + p^5 r^3 + p^2 qr^2 + p^2 r^4 + p^4 qs + q^3 rs$
$\gcd(pqr, Per(A)) = 1$
$\gcd(p^2 q^3 p^4 = p^6 q^3, Per(A)) = 1$
$\gcd\left(r^5 s, Per(A)\right) = 1$

3. In fact

$$\gcd\left(\prod_{x_j \in S} x_j \ , Per(A)\right) = 1$$

where $S = \{p, p^2, p^4, q, q^3, r, r^2, r^3, s\}$

4. Consider the Diagonal Matrix of order $k \times k$ (where k is very large)
$D_k = Diag(y_1, y_2, y_3, \dots, y_k)$ where $y_i = \prod_{x_j \in S} (x_j)$ for $1 \leq i \leq k$
D_k is private.
5. Take $P \in GL_k(\mathbb{Z})$ any $k \times k$ matrix with integral entries and $\det(P) = \pm 1$
P is private.
6. Construct **public key** $C = P^{-1} D_k P$
7. Define a **public key** $N = Per(A)$, where A is the **private 3 × 3 matrix.**
8. Suppose the given message

$$\vec{M} = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{bmatrix}_{k \times 1} \quad \text{with } m_j \in \mathbb{Z}_N.$$

9. **Encryption:**

$$E(\vec{M}) = C\vec{M}\ (Mod\ N)$$
$$= \begin{pmatrix} m_1' \\ m_2' \\ \vdots \\ m_k' \end{pmatrix} (Mod\ N)$$

Since, $\gcd(\det C\ (Mod\ N), N) = 1$, we can compute $C^{-1}(Mod\ N)$ easily using the private keys P, D_k. Since "k" is very large, computing C^{-1} is very difficult. Hence, the method is secure.

10. **Decryption** = $\boldsymbol{C^{-1}}(C\vec{M})(Mod\ N)$
$= \vec{M}$

3.2 Encryption Scheme using the Trace of a Matrix

Take a matrix $\mathbb{M}_4(\mathbb{Z}_N)$

Let "$\boldsymbol{N}$" be a given fixed large positive integer.

$$\mathbb{Z}_N^{(4)} = \left\{ \begin{bmatrix} \boldsymbol{x} \\ \boldsymbol{y} \\ \boldsymbol{z} \\ \boldsymbol{w} \end{bmatrix} \middle| \ \boldsymbol{x, y, z, w} \in \mathbb{Z}_N \right\}$$

Suppose message vector, $\boldsymbol{m} = \begin{bmatrix} \boldsymbol{m_1} \\ \boldsymbol{m_2} \\ \boldsymbol{m_3} \\ \boldsymbol{m_4} \end{bmatrix} \in \mathbb{Z}_N^{(4)}$

Now, define $\boldsymbol{M_1} = \begin{bmatrix} \boldsymbol{m_1} & \boldsymbol{m_2} & \boldsymbol{m_3} & \boldsymbol{m_4} \\ \boldsymbol{m_2} & \boldsymbol{m_3} & \boldsymbol{m_4} & \boldsymbol{m_1} \\ \boldsymbol{m_3} & \boldsymbol{m_4} & \boldsymbol{m_1} & \boldsymbol{m_2} \\ \boldsymbol{m_4} & \boldsymbol{m_1} & \boldsymbol{m_2} & \boldsymbol{m_3} \end{bmatrix}$

$$\boldsymbol{M_2} = \begin{bmatrix} \boldsymbol{m_3} & \boldsymbol{m_4} & \boldsymbol{m_1} & \boldsymbol{m_2} \\ \boldsymbol{m_4} & \boldsymbol{m_1} & \boldsymbol{m_2} & \boldsymbol{m_3} \\ \boldsymbol{m_1} & \boldsymbol{m_2} & \boldsymbol{m_3} & \boldsymbol{m_4} \\ \boldsymbol{m_2} & \boldsymbol{m_3} & \boldsymbol{m_4} & \boldsymbol{m_1} \end{bmatrix}$$

$$M_3 = \begin{bmatrix} m_1 & m_2 & m_3 & m_4 \\ m_2 & m_1 & m_4 & m_3 \\ m_3 & m_4 & m_1 & m_2 \\ m_4 & m_3 & m_2 & m_1 \end{bmatrix}$$

$$M_4 = \begin{bmatrix} m_1 & m_2 & m_3 & m_4 \\ m_4 & m_3 & m_2 & m_1 \\ m_2 & m_1 & m_4 & m_3 \\ m_3 & m_4 & m_1 & m_2 \end{bmatrix}$$

Define $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}], D = [d_{ij}] \in \mathbb{M}_4(\mathbb{Z}_N)$

Define $f: \mathbb{Z}_N^{(4)} \to \mathbb{Z}_N^{(4)}$

$$f\left(\begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \end{bmatrix}\right) = \begin{bmatrix} trace\ AM_1 \\ trace\ BM_2 \\ trace\ CM_3 \\ trace\ DM_4 \end{bmatrix}$$

Then *f* is bijective if and only if

$$B = \begin{bmatrix} a_{11}+a_{24}+a_{33}+a_{42} & a_{21}+a_{12}+a_{34}+a_{43} & a_{31}+a_{22}+a_{13}+a_{44} & a_{41}+a_{32}+a_{23}+a_{14} \\ b_{13}+b_{22}+b_{31}+b_{44} & b_{14}+b_{23}+b_{32}+b_{41} & b_{11}+b_{24}+b_{33}+b_{42} & b_{12}+b_{21}+b_{34}+b_{43} \\ c_{11}+c_{22}+c_{33}+c_{42} & c_{12}+c_{21}+c_{34}+c_{43} & c_{13}+c_{24}+c_{31}+c_{42} & c_{14}+c_{23}+c_{32}+c_{41} \\ d_{11}+d_{24}+d_{32}+d_{43} & d_{12}+d_{23}+d_{31}+d_{44} & d_{13}+d_{22}+d_{34}+d_{41} & d_{14}+d_{21}+d_{33}+a_{42} \end{bmatrix}$$

is invertible over $\mathbb{M}_4(\mathbb{Z}_N)$.

$\det(B) = \alpha\ (mod\ N)$

then $\gcd(\alpha, N) = 1$

Now, $Enc\left(\begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \end{bmatrix}\right) = \begin{bmatrix} trace\ AM_1 \\ trace\ BM_2 \\ trace\ CM_3 \\ trace\ DM_4 \end{bmatrix}$

4. Encryption using Commutative Ring with Unity

Given a multiplicative group **G,** and a commutative ring **R** with identity, the set **RG** consisting of all the finite formal sums $\sum_{\substack{g\in G \\ \alpha(g)\in R}} \alpha(g)g$ with addition defined coefficient-wise and multiplication induced by the multiplication in **G** together with distributivity is an algebra over **R** called the group algebra of the group **G** over the commutative ring **R** [3]**.**

Thus for $\alpha = \sum_{g\in G} \alpha(g)g \in RG$, $\beta = \sum_{h\in G} \beta(h)h \in RG$

$$\alpha + \beta = \sum_{g\in G} \big(\alpha(g) + \beta(g)\big)g$$

$$\alpha\beta = \sum_{g\in G} \left(\sum_{xy=g} \alpha(x)\beta(y) \right) g.$$

The element $1_R\, e_G$, where 1_R is the identity element of the ring **R** and e_G is the identity element of **G**, is the identity element of the group algebra **RG.**

Observe that the map $g \mapsto 1_R g$ is a $1-1$ group homomorphism from **G** into the group of units of **RG**, and the map $\lambda \mapsto \lambda e_G$ is a $1-1$ ring homomorphism $R \longrightarrow RG$**.** We can thus identify both **G** and **R** with their respective images in **RG** under the above maps.
In particular, we then have $1_R = e_G = 1_R e_G$ and this element is the identity element of **RG** which we will denote by 1.

For understanding more basic properties about Group Algebra the reader can refer [4]**.**

Let "N" be a given fixed large positive integer.

Define $\boldsymbol{R} = (\mathbb{Z}_n, +_n, \times_n; 1,0)$ be the given commutative ring with unity. (Ring of integers $modN$), where $\mathbb{Z}_N = \{0,1,2,\cdots, N-1\}$.
Let $f(\boldsymbol{x},\boldsymbol{y}) = a + b\boldsymbol{x} + c\boldsymbol{y} + d\boldsymbol{xy}$ be the given polynomial in the variables $\boldsymbol{x}$ and $\boldsymbol{y}$ over $(\mathbb{Z}_N, +_N, \times_N; 1,0)$; $a, b, c, d \in \mathbb{Z}_N$.
Choose a_1, b_1, c_1, d_1 in $\mathbb{Z}_N$ such that

$$\boldsymbol{gcd}(\boldsymbol{a_1}, \boldsymbol{N}) = \boldsymbol{gcd}(\boldsymbol{a_1} + \boldsymbol{b_1}, \boldsymbol{N}) = \boldsymbol{gcd}(\boldsymbol{a_1} + \boldsymbol{c_1}, \boldsymbol{N}) = \boldsymbol{gcd}(\boldsymbol{a_1} + \boldsymbol{b_1} + \boldsymbol{c_1} + \boldsymbol{d_1}, \boldsymbol{N}) = \boldsymbol{1}$$

Define $g(x,y) = a_1 + b_1 x + c_1 y + d_1 xy$
Here, we are considering the following semi associative group on $\{\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{xy}\}$.

•	x	y	xy
x	$\boldsymbol{x}$	$\boldsymbol{xy}$	$\boldsymbol{xy}$
y	$\boldsymbol{xy}$	$\boldsymbol{y}$	$\boldsymbol{xy}$
xy	$\boldsymbol{xy}$	$\boldsymbol{xy}$	$\boldsymbol{xy}$

Define $E\big(f(\boldsymbol{x},\boldsymbol{y})\big) = f(\boldsymbol{x},\boldsymbol{y}) \cdot g(\boldsymbol{x},\boldsymbol{y})$

$$= (a + b\boldsymbol{x} + c\boldsymbol{y} + d\boldsymbol{xy}) \cdot (a_1 + b_1\boldsymbol{x} + c_1\boldsymbol{y} + d_1\boldsymbol{xy})$$

$$= aa_1 + a_1 b\boldsymbol{x} + a_1 c\boldsymbol{y} + a_1 d\boldsymbol{xy} + ab_1\boldsymbol{x} + bb_1\boldsymbol{x} + cb_1\boldsymbol{xy} + b_1 d\boldsymbol{xy} + ac_1\boldsymbol{y} + bc_1\boldsymbol{xy} + cc_1\boldsymbol{y} + c_1 d\boldsymbol{xy} + ad_1\boldsymbol{xy} + bd_1\boldsymbol{xy} + cd_1\boldsymbol{xy} + dd_1\boldsymbol{xy}$$

$$= aa_1 + [ab_1 + (a_1 + b_1)b]\,\boldsymbol{x} + [ac_1 + (a_1 + c_1)c]\,\boldsymbol{y} + [ad_1 + (c_1 + d_1)b + (b_1 + d_1)c + (a_1 + b_1 + c_1 + d_1)d]\,\boldsymbol{xy}$$

Comparing the coefficients of $\boldsymbol{x}$ and $\boldsymbol{y}$

$aa_1 = a'$ → (1)
$ab_1 + (a_1 + b_1)b = b'$ → (2)
$ac_1 + (a_1 + c_1)c = c'$ → (3)
$ad_1 + (c_1 + d_1)b + (b_1 + d_1)c + (a_1 + b_1 + c_1 + d_1)d = d'$ → (4)

$$A = \begin{bmatrix} a_1 & 0 & 0 & 0 \\ b_1 & a_1 + b_1 & 0 & 0 \\ c_1 & 0 & a_1 + c_1 & 0 \\ d_1 & c_1 + d_1 & b_1 + d_1 & a_1 + b_1 + c_1 + d_1 \end{bmatrix}$$

$$Det(A) = a_1(a_1 + b_1)(a_1 + c_1)(a_1 + b_1 + c_1 + d_1)$$

Here, $\gcd(Det(A), N) = 1$
Now, we can describe encryption of $f(\boldsymbol{x},\boldsymbol{y})$ as
$Enc\,\big(f(\boldsymbol{x},\boldsymbol{y})\big) = f(\boldsymbol{x},\boldsymbol{y}) \cdot g(\boldsymbol{x},\boldsymbol{y})$.

5. Some encryption schemes using non-abelian groups

Now, we shall see few examples of interesting finite non-abelian groups **G** which are being used in Encryption & Decryption.

Example 5.1: Let G be a given group. Let R be a given normal subgroup of G.

1. G and R are given to public
2. Select an endomorphism $\alpha \in End(G)$ such that $\alpha(R) = R$ and α induces identity on $\frac{G}{R}$
3. $\alpha \in Aut(G) \Leftrightarrow \alpha \in Aut(R)$
4. α is fixed point free automorphism i.e $\alpha(g) = g \Leftrightarrow g = e$
5. Action of α on R is private (i.e) $\alpha(r)$ is private for all $r \in R$
6. Choose a message $r \neq e \in R$
   For this message $r \in R$, we can find a "g" $\in G$ such that $\alpha(g) = g \cdot r$

Here for this $r \in R$,we have one and only $g \in G$ such that $\alpha\ (g)\ =\ g \cdot r$
For, suppose $g_1, g_2 \in G$ such that

$$\alpha(g_1)\ =\ g_1 \cdot r \qquad \rightarrow (1)$$
$$\alpha(g_2) =\ g_2 \cdot r \qquad \rightarrow\ (2)$$
$$\therefore g_1^{-1}\alpha(g_1)\ =\ g_2^{-1}\alpha(g_2)$$
$$\Rightarrow g_2 g_1^{-1} =\ \alpha\ (g_2 g_1^{-1})$$
$$\Rightarrow g_2 g_1^{-1} =\ e \Rightarrow g_1 = g_2$$

7. For this message $r \in R,\ g$ is public and $\alpha^3(g)$ is also public.
   The action of α^3 on elements which are not in R is public.
   The action of α^3 on $G - R$ is public.
   Now $\alpha\ (g) =\ g \cdot r$
   $\alpha^2(g)\ =\ \alpha\ (g \cdot r)\ =\ \alpha\ (g)\ \alpha\ (r)$
   $= gr \cdot \alpha\ (r)$
   $\alpha^3(g) =\ \alpha\ (g) \cdot\ \alpha\ (r) \cdot\ \alpha^2(r)$
   $=\ gr\ \alpha\ (r)\alpha^2(r)$
8. **Encryption:**
   $h\ =\ \alpha^3(g)$
   $h\ =\ gr\ \alpha\ (r)\alpha^2(r)$
9. **Decryption:**
   $g^{-1}h \cdot [\ \alpha^2(r)]^{-1}[\ \alpha\ (r)]^{-1}\ =\ r$
   Here The action of α on R is private.

Example 5.2: Let G be a finite group of very large order.

1. H be a given subgroup of G such that $O(H)$ is also very large and H is given to public.
2. Let K be subset of G, which is not a subgroup of G such that K is private.
3. $G\ =\ H \cup K$
4. Choose a message $m \in H$ but $m \notin K$
5. For this m select a secret r such that $r \in K$ but $r\ \notin H$
6. Now the **encryption** of $E(m)\ =\ r \cdot m$
7. Since $r^{-1} \notin H$ but $r^{-1} \in K$
   Decryption $= r^{-1}(rm)$
   $=\ m$

Example 5.3: Let P, Q, R, S be any given positive integers greater than or equal to "2".

1. Define $\boldsymbol{N} = PQRS + 1$, then
   $g.c.d\ (P, N) = g.c.d\ (Q, N) = g.c.d\ (R, N) = g.c.d\ (S, N) = 1$
2. $G = \{\ (a, b, c, d, e)\ \mid a, b, c, d, e\ \epsilon\ \mathbb{Z}_{\boldsymbol{N}}\}$
   Now in **G,** we define following binary operation:
3. $(a_1, b_1, c_1, d_1, e_1) * (a_2, b_2, c_2, d_2, e_2) = (x, y, z, w, l)$
   where $x = a_1 + a_2\ \ (mod\ \boldsymbol{N})$
   $y = b_1 + b_2\ \ (mod\ \boldsymbol{N})$
   $z = c_1 + c_2\ \ (mod\ \boldsymbol{N})$
   $w = d_1 + d_2\ \ (mod\ \boldsymbol{N})$
   $l = a_2 b_1 + b_2 c_1 + c_2 d_1 + e_1 + e_2\ \ (mod\ \boldsymbol{N})$
4. Now, this **G** is a non-abelian group of order $\boldsymbol{N}^5$.
   In this group **G,** we can observe the following.
5. The mapping $f: G \longrightarrow G$, defined by $f(g) = g^e$, where $e \in \{P, Q, R, S\}$ is a permutation on **G.**

Now, using the above examples, we can construct a finite non-abelian group G using finite commutative ring with identity R. This finite group G can be further used for encryption and decryption of the messages.

Let **R** be a finite commutative ring with identity.

Define $\boldsymbol{G} = \{(x_1, x_2, x_3, x_4, x_5) \mid x_1, x_2, x_3, x_4, x_5 \in \boldsymbol{R}\}$

Now in **G**, we define the following binary operation:

$$(x_1, x_2, x_3, x_4, x_5) * (y_1, y_2, y_3, y_4, y_5) = (z_1, z_2, z_3, z_4, z_5)$$

where $z_1 = x_1 + y_1$

$z_2 = x_2 + y_2$

$z_3 = x_3 + y_3$

$z_4 = x_4 + y_4$

$z_5 = y_1x_3 + y_2x_4 + x_5 + y_5$

$$|\boldsymbol{G}| = |\boldsymbol{R}|^5$$

The mapping $f: \boldsymbol{G} \longrightarrow \boldsymbol{G}$, defined by $f(g) = g^e$, where $g.c.d\ (e, |\boldsymbol{R}|) = 1$ is a permutation on **G.**

Similarly, we can construct another finite non-abelian group **H** using **R.**

Define $\boldsymbol{H} = \{(x_1, x_2, x_3, x_4, x_5) \mid x_1, x_2, x_3, x_4, x_5 \in \boldsymbol{R}\}$

Now in **H**, we define the following binary operation:

$$(x_1, x_2, x_3, x_4, x_5) * (y_1, y_2, y_3, y_4, y_5) = (z_1, z_2, z_3, z_4, z_5)$$

where $z_1 = x_1 + y_1$

$z_2 = x_2 + y_2$

$z_3 = x_3 + y_3$

$z_4 = x_4 + y_4$

$z_5 = y_1x_2 + y_2x_2 + y_3x_4 + x_5 + y_5$

$$|\boldsymbol{H}| = |\boldsymbol{R}|^5$$

The mapping $\varphi: \boldsymbol{H} \longrightarrow \boldsymbol{H}$, defined by $\varphi(h) = h^e$, where $g.c.d\ (e, |\boldsymbol{R}|) = 1$ is a permutation on **H.**

6. Encryption schemes over Group Algebra RG

Taking $f(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = a + b\boldsymbol{x} + c\boldsymbol{y} + d\boldsymbol{z} + e\boldsymbol{xy} + f\boldsymbol{xz} + g\boldsymbol{yz} + h\boldsymbol{xyz} \in \boldsymbol{RG}$

where $a, b, c, d, e, f, g, h \in R$

$G = \{\boldsymbol{1}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{xy}, \boldsymbol{xz}, \boldsymbol{yz}, \boldsymbol{xyz}\}$

$\boldsymbol{x^2} = \boldsymbol{y^2} = \boldsymbol{z^2} = (\boldsymbol{xy})^2 = (\boldsymbol{xz})^2 = (\boldsymbol{yz})^2 = (\boldsymbol{xyz})^2 = \boldsymbol{1}$

$\boldsymbol{xy} = \boldsymbol{yx}$ and $\boldsymbol{yz} = \boldsymbol{zy}$ and $\boldsymbol{xz} = \boldsymbol{zx}$

Then we can reconstruct $f(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ from $f(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \cdot g(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$, where

$g(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = a_1 + b_1\boldsymbol{x} + c_1\boldsymbol{y} + d_1\boldsymbol{z} + e_1\boldsymbol{xy} + f_1\boldsymbol{xz} + g_1\boldsymbol{yz} + h_1\boldsymbol{xyz}$ if and only if

$$A = \begin{bmatrix} a_1 & b_1 & c_1 & d_1 & e_1 & f_1 & g_1 & h_1 \\ b_1 & a_1 & e_1 & f_1 & c_1 & d_1 & h_1 & g_1 \\ c_1 & e_1 & a_1 & g_1 & b_1 & h_1 & d_1 & f_1 \\ d_1 & f_1 & g_1 & a_1 & h_1 & b_1 & c_1 & e_1 \\ e_1 & c_1 & b_1 & h_1 & a_1 & g_1 & f_1 & d_1 \\ f_1 & d_1 & h_1 & b_1 & g_1 & a_1 & e_1 & c_1 \\ g_1 & h_1 & d_1 & c_1 & f_1 & e_1 & a_1 & b_1 \\ h_1 & g_1 & f_1 & e_1 & d_1 & c_1 & b_1 & a_1 \end{bmatrix}$$

is invertible over $\boldsymbol{R}$

In this case, we are taking $R = (\mathcal{P}(X),\ \oplus,\ \bullet;\ 1 = X,\ 0 = \phi)$

where $a_1, b_1, c_1, d_1, e_1, f_1, g_1, h_1 \in \mathcal{P}(X)$ such that

$a_1, b_1, c_1, d_1, e_1, f_1, g_1, h_1$ forms a partition of $\boldsymbol{X}$

$A =$

a_1	b_1	c_1	d_1	e_1	f_1	g_1	h_1
b_1	a_1	e_1	f_1	c_1	d_1	h_1	g_1
c_1	e_1	a_1	g_1	b_1	h_1	d_1	f_1

d_1	f_1	g_1	a_1	h_1	b_1	c_1	e_1
e_1	c_1	b_1	h_1	a_1	g_1	f_1	d_1
f_1	d_1	h_1	b_1	g_1	a_1	e_1	c_1
g_1	h_1	d_1	c_1	f_1	e_1	a_1	b_1
h_1	g_1	f_1	e_1	d_1	c_1	b_1	a_1

Here, it is interesting to note that A is a ***Latin square***.

Theorem 6.1: $\boldsymbol{G = \langle 1, x\rangle \times \langle 1, y\rangle \times \langle 1, z\rangle \times \langle 1, w\rangle}$, *where,* $\boldsymbol{x^2 = y^2 = z^2 = w^2 = 1}$
$\boldsymbol{xy = yx, xz = zx, xw = wx, yz = zy, yw = wy, zw = wz}$
i.e $\boldsymbol{G = C_2 \times C_2 \times C_2 \times C_2}$ ***= Direct Product***
if 4 copies of cyclic groups of order "2".
Let $(R, +, \bullet)$ *be given commutative ring with unity* $1 \neq 0$.
Consider the group algebra ***RG.***
$$\boldsymbol{RG = \{a + bx + cy + dz + ew + f(xy) + g(xz) + h(xw) + i(yz) + j(yw) + k(zw) + l(xyz) + m(xyw) + n(xzw) + o(yzw) + p(xyzw)\ ; a, b, c \cdots o, p \in R\}}$$
Let $\boldsymbol{f(x, y, z, w) = a + bx + cy + dz + ew + f(xy) + g(xz) + h(xw) + i(yw) + k(zw) + l(xyz) + m(xyw) + n(xzw) + o(yzw) + p(xyzw) \in RG}$
Then we can reconstruct $f(x, y, z, w)$ *from* $f(x, y, z, w) \cdot g(x, y, z, w)$, *where*
$$\boldsymbol{g(x, y, z, w) = a_1 + b_1x + c_1y + d_1z + e_1w + f_1xy + g_1xz + h_1xw + i_1yz + j_1yw + k_1zw + l_1xyz + m_1xyw + n_1xzw + o_1yzw + p_1xyzw}$$
If and only if

$$B = \begin{bmatrix}
a_1 & b_1 & c_1 & d_1 & e_1 & f_1 & g_1 & h_1 & i_1 & j_1 & k_1 & l_1 & m_1 & n_1 & o_1 & p_1 \\
b_1 & a_1 & f_1 & g_1 & h_1 & c_1 & d_1 & e_1 & l_1 & m_1 & n_1 & i_1 & j_1 & k_1 & p_1 & o_1 \\
c_1 & f_1 & a_1 & i_1 & j_1 & b_1 & l_1 & m_1 & d_1 & e_1 & o_1 & g_1 & h_1 & p_1 & k_1 & n_1 \\
d_1 & g_1 & i_1 & a_1 & k_1 & l_1 & b_1 & n_1 & c_1 & o_1 & e_1 & f_1 & p_1 & h_1 & j_1 & m_1 \\
e_1 & h_1 & j_1 & k_1 & a_1 & m_1 & n_1 & b_1 & o_1 & c_1 & d_1 & p_1 & f_1 & g_1 & i_1 & l_1 \\
f_1 & c_1 & b_1 & l_1 & m_1 & a_1 & i_1 & j_1 & g_1 & h_1 & p_1 & d_1 & e_1 & o_1 & n_1 & k_1 \\
g_1 & d_1 & l_1 & b_1 & n_1 & i_1 & a_1 & k_1 & f_1 & p_1 & h_1 & c_1 & o_1 & e_1 & m_1 & j_1 \\
h_1 & e_1 & m_1 & n_1 & b_1 & j_1 & k_1 & a_1 & p_1 & f_1 & g_1 & o_1 & c_1 & d_1 & l_1 & i_1 \\
i_1 & l_1 & d_1 & c_1 & o_1 & g_1 & f_1 & p_1 & a_1 & k_1 & j_1 & b_1 & n_1 & m_1 & e_1 & h_1 \\
j_1 & m_1 & e_1 & o_1 & c_1 & h_1 & p_1 & f_1 & k_1 & a_1 & i_1 & n_1 & b_1 & l_1 & d_1 & g_1 \\
k_1 & k_1 & k_1 & e_1 & d_1 & p_1 & h_1 & g_1 & j_1 & i_1 & a_1 & m_1 & l_1 & b_1 & c_1 & f_1 \\
l_1 & i_1 & g_1 & f_1 & p_1 & d_1 & c_1 & o_1 & b_1 & n_1 & m_1 & a_1 & k_1 & j_1 & h_1 & e_1 \\
m_1 & j_1 & h_1 & p_1 & f_1 & e_1 & o_1 & c_1 & n_1 & b_1 & l_1 & k_1 & a_1 & i_1 & g_1 & d_1 \\
n_1 & k_1 & p_1 & h_1 & g_1 & o_1 & e_1 & d_1 & m_1 & l_1 & b_1 & j_1 & i_1 & a_1 & f_1 & c_1 \\
o_1 & p_1 & k_1 & j_1 & i_1 & n_1 & m_1 & l_1 & e_1 & d_1 & c_1 & h_1 & g_1 & f_1 & a_1 & b_1 \\
p_1 & o_1 & n_1 & m_1 & l_1 & k_1 & j_1 & i_1 & h_1 & g_1 & f_1 & e_1 & d_1 & c_1 & b_1 & a_1
\end{bmatrix}$$

is invertible over R

Corollary 6.1: Let $\boldsymbol{R = (\mathcal{P}(X), +, \bullet; 1 = X, 0 = \{\})}$ be a ***Boolean Ring*** with $|X| < \infty$
$a_1, b_1, c_1, d_1, e_1, f_1, g_1, h_1, i_1, j_1, k_1, l_1, m_1, n_1, o_1, p_1$ forms a **partition of X.**
Then we can reconstruct $f(x, y, z, w)$ from $f(x, y, z, w) \cdot g(x, y, z, w)$

Example 6.1:
Group Algebra over Klein's 4 group
$\boldsymbol{G}$ has the following presentation:
$\boldsymbol{G = < x, y \mid x^2 = y^2 = (xy)^2 = 1 > = C_2 \times C_2}$
$RG = \{a + bx + cy + dxy \mid a, b, c, d \in R\}$
Let $g(x, y) = a_1 + b_1x + c_1y + d_1xy \in RG$ (given)
Now define a map ψ: $RG \rightarrow$ RG,

$\psi\ (\ f\ (\ x,y\ )\ ) = g(x,y)\cdot f(x,y) - g(x,y) - f(x,y)$
Then ψ is bijective if and only if the following matrix **A** is invertible over **R**

$$\boldsymbol{A} = \begin{bmatrix} a_1 - 1 & b_1 & c_1 & d_1 \\ b_1 & a_1 - 1 & d_1 & c_1 \\ c_1 & d_1 & a_1 - 1 & b_1 \\ d_1 & c_1 & b_1 & a_1 - 1 \end{bmatrix}$$

As a special case if $\boldsymbol{R} = (\boldsymbol{\mathcal{P}}(\boldsymbol{X}), +, \bullet; 1 = X, 0 = \{\})$ be a ***Boolean Ring*** with $|X| < \infty$
b_1, c_1, d_1 forms a **partition of $\boldsymbol{a_1}$.**

Theorem 6.2: *Let $R = (\mathbb{Z}_N, +_N, \times_N)$ be a ring of integers $mod N$, where N is a fixed large positive integer.*
Let $f(\boldsymbol{x},\boldsymbol{y}) = a + b\boldsymbol{x} + c\boldsymbol{y} + d\boldsymbol{xy}$ be a given polynomial over $(\mathbb{Z}_N, +_N, \times_N)$.
*We can **reconstruct $\boldsymbol{f}(\boldsymbol{x},\boldsymbol{y})$** from $f(\alpha_0\boldsymbol{x} + \beta_0, \alpha_1\boldsymbol{y} + \beta_1)$ if and only if $\boldsymbol{gcd}(\boldsymbol{\alpha_0}.\boldsymbol{\alpha_1}, \boldsymbol{N}) = \boldsymbol{1}$*
Proof:

$$f(\alpha_0\boldsymbol{x} + \beta_0, \alpha_1\boldsymbol{y} + \beta_1)$$
$$= (a + b\beta_0 + c\beta_1 + d\beta_0\beta_1) + (b\alpha_0 + d\alpha_0\beta_1)\boldsymbol{x} + (c\alpha_1 + d\beta_0\alpha_1)\boldsymbol{y} + d\alpha_0\alpha_1\boldsymbol{xy}$$

$$\begin{bmatrix} 1 & \beta_0 & \beta_1 & \beta_0\beta_1 \\ 0 & \alpha_0 & 0 & \alpha_0\beta_1 \\ 0 & 0 & \alpha_1 & \beta_0\alpha_1 \\ 0 & 0 & 0 & \alpha_0\alpha_1 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} a' \\ b' \\ c' \\ d' \end{bmatrix}$$

$\begin{bmatrix} 1 & \beta_0 & \beta_1 & \beta_0\beta_1 \\ 0 & \alpha_0 & 0 & \alpha_0\beta_1 \\ 0 & 0 & \alpha_1 & \beta_0\alpha_1 \\ 0 & 0 & 0 & \alpha_0\alpha_1 \end{bmatrix} \in M_4(\mathbb{Z}_N)$ is invertible iff $\boldsymbol{gcd}(\boldsymbol{\alpha_0}\cdot\boldsymbol{\alpha_1}, \boldsymbol{N}) = \boldsymbol{1}$
Determinant of this matrix = $(\alpha_0.\alpha_1)^2$
Similarly,
taking $f(x,y,z) = a' + b'\boldsymbol{x} + c'\boldsymbol{y} + d'\boldsymbol{z} + e'\boldsymbol{xy} + f'\boldsymbol{yz} + g'\boldsymbol{xz} + h'\boldsymbol{xyz}$
we define $f(\alpha_0\boldsymbol{x} + \beta_0, \alpha_1\boldsymbol{y} + \beta_1, \alpha_2\boldsymbol{z} + \beta_2)$ such that $\boldsymbol{gcd}(\boldsymbol{\alpha_0}\cdot\boldsymbol{\alpha_1}\cdot\boldsymbol{\alpha_1}, \boldsymbol{N}) = \boldsymbol{1}$

$$A = \begin{bmatrix} 1 & \beta_0 & \beta_1 & \beta_2 & \beta_0\beta_1 & \beta_1\beta_2 & \beta_0\beta_2 & \beta_0\beta_1\beta_2 \\ 0 & \alpha_0 & 0 & 0 & \alpha_0\beta_1 & 0 & \alpha_0\beta_2 & \alpha_0\beta_1\beta_2 \\ 0 & 0 & \alpha_1 & 0 & \alpha_1\beta_0 & \beta_1\beta_2 & 0 & \alpha_1\beta_0\beta_2 \\ 0 & 0 & 0 & \alpha_2 & 0 & \alpha_2\beta_1 & \alpha_2\beta_0 & \alpha_2\beta_0\beta_1 \\ 0 & 0 & 0 & 0 & \alpha_0\alpha_1 & 0 & 0 & \alpha_0\alpha_1\beta_2 \\ 0 & 0 & 0 & 0 & 0 & \alpha_1\alpha_2 & 0 & \alpha_1\alpha_2\beta_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha_0\alpha_2 & \alpha_0\beta_1\beta_2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_0\alpha_1\alpha_2 \end{bmatrix}$$

$\in M_8(\mathbb{Z}_N)$ is invertible iff $\boldsymbol{gcd}(\boldsymbol{\alpha_0}\cdot\boldsymbol{\alpha_1}\cdot\boldsymbol{\alpha_2}, \boldsymbol{N}) = \boldsymbol{1}$
Determinant of this matrix = $(\alpha_0.\alpha_1\cdot\alpha_2)^4$

Example 6.2: Let R be any given commutative ring with **identity**. Let G be the given group generated by $\{\boldsymbol{x},\boldsymbol{y}\}$ such that $\boldsymbol{x^2} = \boldsymbol{y^2} = \boldsymbol{1}, \boldsymbol{xy} = \boldsymbol{yx}$.
Consider the group algebra RG

$\bullet$	**1**	x	y	xy
1	**1**	$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{xy}$
x	$\boldsymbol{x}$	**1**	$\boldsymbol{xy}$	$\boldsymbol{y}$
y	$\boldsymbol{y}$	$\boldsymbol{xy}$	**1**	$\boldsymbol{x}$

xy	$\boldsymbol{xy}$	$\boldsymbol{y}$	$\boldsymbol{x}$	$\mathbf{1}$

Now our basic ring is ***RG***, where, we are considering polynomials over ***RG***.
Let $f(\boldsymbol{x},\boldsymbol{y}) = a + b\boldsymbol{x} + c\boldsymbol{y} + d\boldsymbol{xy}$ be the given polynomial in "$\boldsymbol{x}$" and "$\boldsymbol{y}$" over ***RG***.
We can reconstruct $f(\boldsymbol{x},\boldsymbol{y})$ from $f(\boldsymbol{x},\boldsymbol{y}) \cdot g(\boldsymbol{x},\boldsymbol{y})$, where $g(\boldsymbol{x},\boldsymbol{y}) = a_1 + b_1\boldsymbol{x} + c_1\boldsymbol{y} + d_1\boldsymbol{xy}$ iff
$\begin{bmatrix} a_1 & b_1 & c_1 & d_1 \\ b_1 & a_1 & d_1 & c_1 \\ c_1 & d_1 & a_1 & b_1 \\ d_1 & c_1 & b_1 & a_1 \end{bmatrix}$ is invertible over R.

References

[1] T.M. Apostol, (1976), Introduction to analytic number theory. Springer.

[2] Christof Paar, Jan Pelzl, (2010), Understanding Cryptography, Springer

[3] I.N. Herstein, (1975), Topics In Algebra (2nd ed.), John Wiley & Sons

[4] Inder Bir S. Passi, "Group algebras," Indian Journal of Pure and Applied Mathematics, Vol. 43, No. 2, (2012), pp. 89-106.

[5] K. Komaya, U. Maurer, T. Okamoto and S. Vanston, "New public-key schemes based on elliptic curves over the ring Zn," In J. Feigenbaum (Ed.): Crypto'91, LNCS 576, Springer-Verlag (1992), pp. 252-266.

[6] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, Vol. 48 (177), (1987), pp. 203-209.

[7] R.A. Mollin, C. Small, "On permutation polynomials over finite fields," International Journal of Mathematics and Mathematical Sciences, Vol. 10, No. 3, (1987), pp. 535-544.

[8] R.L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Communications of the ACM, Vol. 21, No. 2, (1978), pp. 120-126.

[9] W. Diffie, M.E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, Vol. 22, No. 6, (1976), pp. 644-654.