INTERNATIONAL JOURNAL OF PURE MATHEMATICS
DOI: 10.46300/91019.2022.9.13 Volume 9, 2022

Finite Semi-group Modulo and Its Application to Symmetric Cryptography

Frank Emmanuel Akpan
Department of Mathematics/Statistics, University of Port Harcourt,
Rivers State, Nigeria

Udoaka Otobong Gabriel
Department of Mathematics, Akwa Ibom state University,
Akwa Ibom State, Nigeria

Abstract: In this paper, the application of finite semi-group structure S is studied. In particular, the study uses finite semi-group modulo n $FS(n)=(Z_p,\ +)\langle\theta\rangle$ to generate Mutually Orthogonal Latin Squares (MOLS) and applied same to symmetric cryptography. It is shown in the study that for any $n>1$, the maximum number of mutually orthogonal Latin squares in a finite semi-group modulo n $FS(n)=(Z_p,\ +)\langle\theta\rangle = \{0,\ 1,\ 2,3,\ .....p-1,$ $\phi,\phi^2,\phi^3\ .....nth\ \ element\ \ \}\ is\ n-1.$ Finally, the study shows manual Algorithm for the generation of mutually orthogonal Latin squares from a finite semi-group modulo and its application to symmetric cryptography which has been seen to be an effective coding technique for hiding sensitive information and suitable for reducing crime rate if not totally eradicated.

Keywords: Cryptography, Finite Semi-group, Semi-group modulo n, Latin Square.

I. INTRODUCTION

This section contains basic definitions of some important concepts needed in this study. Some theorems related to the investigation are of importance. Hence, such theorems are stated and proved appropriately where necessary.

A non-empty set S equipped with a binary operation * which is required only to be associative is known as a Semi-group. Any element e of S is called an identity element if $\forall\ x\in S,\ ex = xe = x$, such a semi-group is called monoid. Thus, a semi-group with identity is a monoid.

An identity may be adjourned to S by first of all choosing an element $1\notin S$. We denote such a semi-group by $S^1 = S \cup \{1\}$, we call such a semi-group "a monoid". We further define a multiplication on S^1 to be a multiplication on S so that $\forall\ x\in(S\cup\{1\}),\quad x1 = 1x = x$. Hence, it is correct to write this conventionally as

$$S^1 = \begin{cases} S\cup\ \{1\},\ \ if\ \ S\ \ has\ no\ identity\ \ element \\ \\ S\ ,\ Otherwise. \end{cases} \qquad (1)$$

Many algebraic structures are semi-groups [2], few among the semi-group structures related to this work are listed below:

Let A and B be two non-empty sets such that S = A×B. Define a binary operation on S such that $\forall(i,j),(k,l)\in S$ (i, j) (k,l) = (i, l). Then, $\forall\ (m,n)\in S$,

((i,j)(k,l))(m,n) = (i,l)(m,n) = (i,n) (2)

Also,(i,j)((k,l)(m,n))=(i,j)(k,n)=(i,n) (3)

Comparing (2) and (3), we see that ((i,j)(k,l))(m,n) = (i,j)((k,l)(m,n))

Hence, S is a semi-group since the operation is associative.

The set S defined by the operation (i,j)(k,l) = (i,l) is a semi-group called the rectangular band on A×B.

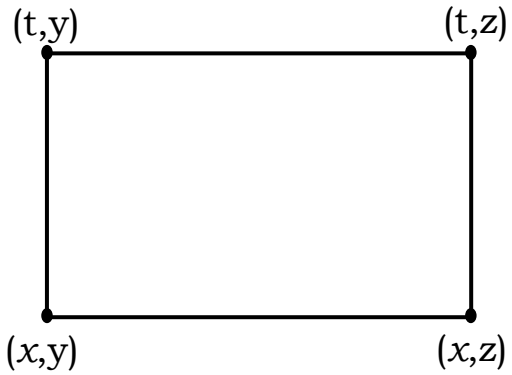
Any element $k\in S$ is called the zero of S if $\forall x\in S,\ kx = xk = k$. We may also adjourn a zero to S by first choosing an element $k\notin S$ such that the multiplication on $S^k = S\cup\{k\}$ implies the multiplication on S. In practice, we denote such construction thus:

$$S^k = \begin{cases} S\cup\{k\},\ if\ \ S\ \ has\ no\ zero\ element \\ \\ S,\ \ otherwise \end{cases} \qquad (4)$$

Irrespective of our choice of notation, a semi-group cannot have more than one zero. If S has a zero, conventionally we write $S = S^0 = S \cup \{0\}$ and the partial multiplication given by $S^o \times S^o \to S^o$ is defined only for pairs $(x, y) \in S^o \times S^o$ where $xy \neq 0$. Now, if S has a zero and all product are equal to zero. Then, S is an empty or null semi-group.

Let S denote a semi-group, an element $e \in S$ is said to be idempotent if $e^2 = e$.

If each element in a semi-group S is idempotent then S is called an idempotent semi-group (or a band). Again, if $\forall\ x, y \in S,\ xy = yx$ then S is a commutative semi-group.This shows that the rectangular band S = A×B on S is an idempotent semi-group. Notice that $(i,j)^2 = (i,j)(i,j) = (i,j)$, $(k,l)^2 = (k,l)$ etc. The term "rectangular" is evident. If (x,y) and (t, z) are regarded as coordinates in the Cartesian plane, then the product $(x, y)(t, z)$ and $(t, z)(x, y)$ can be written at each vertex of the rectangle as shown below



The Semi-group $(Z_n, *)$.

Let $S = (Z_{n,} *)$ denote an algebraic structure. This structure is known as the residue classes modulo n. For all $a, b, c \in S,\ n \in N,\ a*(b*c) = (a*b)*c.$ Hence, S is a semi-group. In fact, the idempodent element in $(Z_{n,} *)$ commute.

This particular semi-group structure $(Z_n, *)$. forms the core of this work .

Finite semi-group [4]

Let S be a semi-group with n-elements. Then, S is known as a finite semi-group of order n.

Homomorphism of a Finite Semi-group [3]

Let S_1 and S_2 denote two finite semi-groups. Suppose that $\theta: S_1 \to S_2$ defines a mapping from S_1 to S_2 such that θ preserves multiplication of the form $(ab)\theta = (a\theta)(b\theta) \quad \forall a, b \in S_1$ Then, θ is called a homomorphism. If θ is injective, θ is called monomorphism. If θ is surjective, it is called epimorphism. A bijective morphism (homomorphism) is called an isomorphism.

A bijective homomorphism from S_1 onto S_2 is anti-isomorphism if θ reverses the multiplication, such that $(ab)\theta = (b\theta)(a\theta)$, $\forall a, b \in S_1$. In such case, θ : $S_2 \to S_1$ as a monomorphism is also called a faithful representation or an imbedding of S_1 onto S_2 [3].

To apply the idea of finite semi-group to cryptography, we must choose a finite semigroup structure. In this work, the finite semi-group structure $(Z_n, *)$ will be used for construction of latin squares which will be applied in the encryption and decryption of a crypto system [7]. Obviously, the semi-group structure $(Z_n, *)$ is a finite semi-group.

The finite semi-group $(Z_n, *)$ will be denoted by *FS*(*n*) so that $FS(n) = (Z_p, +)\langle\theta\rangle$. This finite semi-group structure is called the residue classes modulo *n*. It will be used for prime and even p. Of course, residue classes modulo *n* are modulo groups and what is known today as semi-group is a generalized group.

Proposition 1.

Let $FS(n) = (Z_p, +)\langle\theta\rangle$ denote a finite semi-group. Then every element of $(Z_P, *)$ has an inverse.

Proof

Let $[a] \in FS(n) = (Z_P, +)\langle\theta\rangle,\ a \neq 0$ so that n does not divide " a". Then, (*a*, n) = 1 (*a* and n are relatively prime) clearly, p*a* + qn = 1 for some $p, q \ Z_n$ $. \Rightarrow pa = 1 \pmod n \Rightarrow [p][a] = 1.$ Therefore, [*a*] is invertible. Thus, $FS(n) = (Z_p, +)\langle\theta\rangle$ is a finite semi-group with each element having its inverse. Consequently, $FS(n) = (Z_p, +)\langle\theta\rangle$ is a regular semi-group.

Definition 1.

Let $FS(n) = (Z_p, +)\langle\theta\rangle$ denote a finite semi-group. Suppose that there exists a positive number p such that $pa = 0$, $\forall a \in FS(n)$. Then, the least of such p is called the characteristic of $FS(n)$. If the relation p*a* = 0 only holds for p = 0, then $FS(n)$ is said to be of characteristic 0. Generally, if n is a finite prime, then $FS(n) = (Z_p, +)\langle\theta\rangle$ is a finite semi-group of order n with characteristic n. **Note:** That if n is the characteristic of $FS(n) = (Z_p, +)\langle\theta\rangle$ then $n \notin Z_P$.

Proposition 2

Let $FS(n)=(Z_n, +)\langle\theta\rangle$ denote a finite semi-group. Then the characteristic of Z_n is either 0 or prime.

Proof

Let n be the characteristic of a finite semi-group $FS(n)=(Z_n, +)\langle\theta\rangle$, n > 0. Suppose n is not a prime number, then there exist $n_1\ n_2 \in Z_n$ such that n = n_1 n_2. Now, if n_1 n_2 are the characteristic of $FS(n)=(Z_n, +)\langle\theta\rangle$. It implies that $\forall a \in FS(n), (n_1 n_2)\, a = 0$ $\Rightarrow (n_1 n_2) = 0\ or\ a = 0$. Again, if n is prime, by the characteristic property, $\forall a \in FS(n), \quad n.a = 0$ but $a \neq 0$. this implies that FS(n) has a finite order n. Hence, the characteristic of FS(n) is either 0 or n.

Proposition 3

Let $FS(n)=(Z_n, +)\langle\theta\rangle$ denote a finite semi-group of characteristic n, then the order of $(Z_n, *)$ is n.

Proof

Let $\phi : Z \to Z_n$ be a semi-group homomorphism defined by ϕ(n) = n.1. Since the characteristic of Z_n is n, the kernel of ϕ must be nZ and the image of ϕ must be a subsemi-group denoted by K. Since Z_n is a finite semi-group, it must be an algebraic extension of K. Suppose that $|Z_n : k| = n$ is the dimension of Z_n where Z_n is a k vector space, there exist elements $a_1,\ a_2,\ a_3, \cdots\cdots a_n \in Z_n$ such that any element $a \in Z_n$ can be written uniquely in the form $X = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$ where the a_i's are in K. Since there are n elements in K, there are n possible linear combinations of the a_i's. Hence, the order of Z_n must be n.

Proposition 3

Let $FS(n)=(Z_n, +)\langle\theta\rangle$ denote a finite semi-group of order n. Then, the cayley semi-group table for $FS(n)=(Z_n, +)\langle\theta\rangle$ is a Latin square of order n.

Proof

Consider the case of $(Z_n,+)$, let a,b,c$\in FS(n)$. Then $a+(b+c)=(a+b)+c$. Now, since $(Z_n,+)$ satisfies the properties of a semi-group coupled with the fact that a semi-group (In particular, inverse semi-group) is a group, it follows that *a*+b = *a*+c. It further means that $\forall a \in (Z_n,+)$, there is $-a \in (Z_n,+)$ and *a*+(-*a*) = 0.

Therefore, (-*a*)+(*a*+b)= (-*a*+a) + c (5)

Observe that (5) is associative, this implies that b = c. Hence, an element cannot appear twice in the row. Also, an element cannot appear twice in any column. Therefore, the Cayley semi-group table must be a Latin square.

Proposition 4

Let $L_k = (a_{ij}^k)$ denote a Latin square formed from a finite semi-group $FS(n)=(Z_n, +)\langle\theta\rangle$ of order n. Then, there are $L_1, L_2, L_3 \ldots L_{n-1}$ r-mutually orthogonal set of Latin squares of order n and the total coordinates is p^n for some p= n∈N.

Proof

Let $L_k = (a_{ij}^k)$ denote a Latin square from the finite semi-group $FS(n)=(Z_n, +)\langle\theta\rangle$ suppose that $L_r = (a_{mn}^r)$ and $L_s = (a_{u\,v}^s)$ are two Latin squares such that when superimposed, the pair of elements in the (m,n)th and the (u,v)th positions are the same. Then $a_{m\,n}^r = a_{u\,v}^s$ and $a_{m\,n}^s = a_{u\,v}^s$. Therefore

$$\forall\, x \in (a_{k1}^q),\ x_k \circ x_m + x_n = x_k . x_u + x_v \quad (6)$$

Also,

$$x_1 \cdot x_m + x = x_L \cdot x_u + x_v \quad (7)$$

subtracting (6) and (7), we have

$$(x_k - x_L)x_m = (x_k - x_L)x_u$$
$$\Rightarrow x_k x_m - x_L x_m - x_k x_u + x_L x_v = 0$$
$$\Rightarrow (x_k - x_L)(x_m - x_n) = 0 \quad (8)$$

Since $L_k = (a_{ij}^k) \in FS(n)=(Z_n, +)\langle\theta\rangle$ has no zero divisor, it implies from (8) that , $x_k = x_L$ or $x_m = x_v$. Hence, either k = l or m = u. but k≠l and m≠u since $L_r = (a_{m\,n}^r)$ and $L_s = (a_{u\,r}^s)$ are mutually orthogonal to each other. This contradiction shows that for any two or more orthogonal Latin squares, the pairs of coordinate are all different. Each element of the first Latin square appears n times and must occur with all n different elements when compared to the second Latin square. Thus, each of the Latin square must be of order n. So, the total coordinates must be p^n.

Proposition 5

Let $FS(n)=(Z_n, +)\langle\theta\rangle$ denote a finite semi-group of order n. Then, there are n – 1 mutually orthogonal Latin squares $(a_{i\,j}^k) \in (Z_n, *),\ 1 \le k \le n-1$.

Proof

Let $\left(a_{ij}^{k}\right)$ denote a Latin square formed from the carley semi-group table. Let a permutation be defined for $1 \le k \le n-1$ by $a_{i\,j}^{k} = x_k\ x_i + x_j$ where 0≤ i ≤ n – 1 and 0 ≤ j ≤ n – 1 are the n – 1 elements of the set of Latin squares. Then, the difference between any two elements in the ith row is

$a_{i\,j}^{k} - a_{i\,m}^{k} = \left(x_k\ x_i + x_j\right) - \left(x_k x_i + x_m\right)$

$= x_j - x_m \neq 0_i \ \ if \ \ j \neq m$ this shows that each row is a permutation of the n - elements of the finite semi-group $FS(n) = (Z_n, +)\langle\theta\rangle$. Similarly, the difference between any two elements in the jth column is

$a_{i\,j}^{k} - a_{n\,j}^{k} = \left(x_k\ x_i + x_j\right) - \left(x_k x_i + x_n\right)$

$= x_i - x_n \neq 0_i \ \ if \ \ i \neq n$. Hence, each column is a permutation of n- elements of the finite semi-group. So, there must be n–1 mutually orthogonal Latin squares L_k, k = 1,2, 3 .. n –1, each of order n.

Finite semi-group modulo n and semi-groups in general together with their structures have been studied by many researchers. However, there are several classifications and theories of construction of finite semi-group that have not been extensively studied. Hence, the present study intends to contribute to this area of knowledge. The problem of this study is how to apply finite semi-group structures, specifically the residue classes integer modulo n to symmetric cryptography in order to hide sensitive and confidential information from unauthorized person(s) and be sure that such sensitive and confidential information only get to the authorized person(s). This will help in fighting crime in our society.

The ever increasing and challenging security situations all over the world has given many well meaning citizens sleepless nights as well as researchers. This has called for indebt application based research in providing solutions to this overwhelming situations. The purpose of this study is to use the idea of finite semi-group modulo n for the construction of Latin squares and apply same to symmetric cryptography thereby hiding sensitive information from bandits and kidnappers which can leads to their arrest and prosecutions. Hence, reducing crime rate if not totally eradicated.

This study has many significant dimensions. It serves as a guide and reference point for other researchers and computer programmers on how to solve related problems of data security using the idea of mutually orthogonal Latin squares constructed from finite semi-group modulo of order n. The study is also of immense benefit to network security providers. In general, it creates awareness to anyone who is security conscious of his/her intellectual properties both electronically and otherwise on how such properties can be secured using the idea of finite semi-group modulo n. The section 2 discusses some related works. Section 3-4, is on Mutually orthogonal Latin squares (MOLS**)** and Cryptography. The construction, examples and application of this work is in section 5-7 and finally the conclusion in section 8.

II REVIEW OF RELATED WORK

Finite semi-group modulo n and semi-groups in general together with their structures have been studied by many researchers. In the history of mathematics, the area of knowledge called “theory of semi-group” or semi-group theory” is relatively new. This aspect of knowledge in mathematics started developing in the twentieth century. Although much ground work was laid by researchers in the direction of both group and ring theory which metamorphous to what is now known as semi-group, it is of importance to state that many researchers have tried their best to invoke the concept of finite semi-group for solution to human problems.

Jayshre and Gaji, in 2014 carried out investigation on Lagrange’s property for finite semi-groups. From their study, non abstract finite semi-groups which satisfy weak lagrange’s property and anti Langrange’s property were analyzed. Such study leads us to visualized finite semi-groups to be analogue with finite groups and compare them.

In another study conducted in [2], the concept of semi-group closure of finite rank symmetric inverse semi-groups was studied. The notion of semi-group with tight ideal series and semi-topological semi-group particularly inverse semi-groups with continuous inversion were investigated. The result of the study showed that the symmetric inverse semi-group of finite transformation of rank ≤ n is algebraically closed in the class of semi-topological inverse semi-group with continuous inversion.

Nagy, in [3] conducted a study on finite semi-groups of degree $|S|$ over the fields. The result shows the dimension of the sub-algebra of $M_n(f)$ generated by $\phi(s)$, where S is an n –1 element semi-group (ie finite semi-group) and ϕ is a faithful representation of S for degree n over a field F, $M_n(f)$ denote all n×n matrices with entries from a field F specifically for a case where S is the left reductive and ϕ is the right regular representation of S.

Olexandr and Volodymyr in 2005 investigated the full finite inverse symmetric semi-group. The combination results of full finite symmetric inverse semi-group were presented including the description of automorphisims and endomorphism, Green’s relations and the description of some classes of sub-semigroups. Such as isolated, completely isolated and nilpotent.

Joao, Wolfram and Janusz in [4] carried out a research on the commuting graph of a finite non-commutative semi-group. In the study, the clique number of a finite non-commutative semi-group was calculated, the diameter of the commuting graphs of the proper ideals of the symmetric inverse semi-group I(x) and that of the non-commutative semi-group G(I(x)) were also calculated when |×| is even or a power of an odd prime. It was also shown that when |×| is odd and divisible by at least two

primes, then the diameter of G(I(x)) is either 4 or 5. Several results on semi-groups such as a description of all commutative sub-semigroups of inverse symmetric semi-groups of maximum order and analogous results for commutative inverse and commutative nilpotent sub-semigroups of symmetric semi-group were presented.

A study conducted in [6] on permutation presentation of non-abelian simple semigroups shows that free band of inverse semi-groups on a set and the free perfect band of inverse monoids could be represented as a quotient of suitable free unary semi-group. Consequently, it was shown that every band of inverse semi-group may be embedded in a perfect band of inverse monoids and that the free band of inverse semi-groups on a set X may be embedded in a natural way in the free perfect band of inverse monoids on X. A modified version of Rasin's representation of the free completely simple semi-group on a set was discussed [6]

Dustin in 2015 also involved in investigating the structure of a regular semi-group through maximum congruence ρ with the property that each ρ-classes for $e = e^2 \in S$ is a rectangular subband of S. A construction of all biordered sets was provided and this was specialized to provide a construction of all solid biodered sets. The result was used to construct all regular idempotent a regular idempotent-generated semi-group by rectangular bands.

Wanless in [7] carried out a study on Latin squares that attracted promptly the attention of many mathematicians. He investigated the transversals in latin squares and the quasigroup of related system. Based on his investigations, a concern in Latin squares was awoken by significant results which were achieved in different areas of mathematics.

In [8], the multiplication tables of groups was investigated and was found that the multiplication tables of groups are as a matter of fact special Latin squares.

Datta and Touba in [9] investigated a class of groups which are associated with Latin squares for the generation of burst-error correcting code. He Showed that a Latin square need not be a multiplicative table of group.

Similar concept was proved in [10] that each Latin square is a multiplicative table of a quasi-group. In addition, she found that there exists a close connection between dessurguesian projective planes and non associative quasi-groups. Owing to this fact, a great deal of papers were written devoted to the investigation of the finite projective planes.

Gallego in [11] wrote on generation of random latin squares , and some results of the theory of Latin squares from the study were also used by [12] for the construction of quantum latin squares and unitary error bases. Quite recently, the application of Latin squares was found in Genetics in [13]. Also, an investigation on the generalized Latin squares was made by katrnoska in [13], He investigated the Algebraic structure of set of all Latin squares over a commutative ring with identity.

III. MUTUALLY ORTHOGONAL LATIN SQUARES (MOLS)

Mutually orthogonal latin squares and their applications in finding solution to real life problem have been investigated by many mathematics researchers, to mention but few and notable among them are Musto in 2016 who was able to proved that more than two latin squares of order n each, may be mutually orthogonal.
In [14] , it was proved that if n is a positive integer, and if N(n) is the maximum number of MOLS of order n, then $N(n) \le n-1,$ for all $n > 1.$
Jordan in [15] tactically published a paper that has several influential results on MOLS. One of such results is that for any prime n, there exists a class of n-1 MOLS of order n. This result was same as that of [10]. The method of construction used in [14] though different from Jordan's paper in [15] gave the same result.

IV. CRYPTOGRAPHY

Vikas, Shruti and Rajesh in 2014 defined Cryptography as the practice and the study of methods of protecting or securing communication from third party.
More generally, Cryptography is concerned with the practice of setting out protocols for secure communication without the influence or interference of third party. Cryptography is related to various aspect of information security. Symmetric cryptography is all about the sender and the receiver of a message using the same key for encryption and decryption respectively.

A new algorithm was also Suggested in [15] which should be used for encryption and decryption of messages and images where one sends an encrypted message to another party without the interference of a third party.

V. CONSTRUCTION OR FORMATION OF "MUTUALLY ORTHOGONAL LATIN SQUARES" (MOLS) USING FINITE SEMI-GROUP OF ORDER N.

The major concern of this section is to show the procedures involved in the construction of MOLS from a finite semi-group $FS\ (n) = (Z_p, +)\langle\theta\rangle$ where n is the order of the semi-group and the algebraic structure $(Z_p, +)$ defines a residue classes modulo p. This formation or construction is done for prime p. The said procedures require the knowledge of finite semi-group theory [4], and the formation of the Carley semi-group table for finite semi-group. It also requires the knowledge of the mappings of the n–1 elements of the finite semi-group $FS\ (n) = (Z_p, +)\langle\theta\rangle$.

Let a finite semi-group $FS\ (n) = (Z_p, +)\langle\theta\rangle$ be given, where p =3 and n=5 so that

$$FS\ (n) = (Z_p, +) < \phi > = FS\,(5) = (Z_3, +)\langle\theta\rangle$$

$\Rightarrow FS(5) = \{0,\ 1,\ 2,\ \phi,\ \phi^2\}$ .Consider Table 1 with the operation of addition (+) as shown below. Notice that $\forall\ a, b, c \in [(Z_p,\ +)\langle\theta\rangle]$, $a+(b+c) = (a+b)+c$ Hence, $FS\ (n) = (Z_3,\ +)\langle\theta\rangle$ is a finite semi-group of n order. For the purpose of cryptography, let e=0+0=1+ϕ^2=ϕ^2+1 = ϕ+2 = 2+ϕ, f = 1+ϕ = ϕ^2+2 = 2+ϕ^2 = ϕ+ϕ, g = 2+0 = 0+2 = 1+1 = ϕ+ϕ^2 = ϕ^2+ϕ.

Table 1. Cayley Table of Finite Semigroup Modulo 5.

(+)	e	f	g	ϕ	ϕ^2
e	e	f	g	ϕ	ϕ^2
f	f	g	ϕ	ϕ^2	e
g	g	ϕ	ϕ^2	e	f
ϕ	ϕ	ϕ^2	e	f	g
ϕ^2	ϕ^2	e	f	g	ϕ

Obviously, Table 1 is a Latin square of n×n size of the form

$$L_1 = \begin{matrix} e & f & g & \phi & \phi^2 \\ f & g & \phi & \phi^2 & e \\ g & \phi & \phi^2 & e & f \\ \phi & \phi^2 & e & f & g \\ \phi^2 & e & f & g & \phi \end{matrix}$$

Observe that L_1 is a Latin square of the n-elements of $FS\ (n) = (Z_3,\ +)\langle\theta\rangle$ such that no element occurs twice in any row or column. By proposition 5, since $FS\ (n) = (Z_3,\ +)\langle\theta\rangle$ is a finite semi-group, we expect n–1 MOLS $(a_{ij}^k) \in (Z_3,\ +)\langle\theta\rangle$, $1 \le k \le n-1$. To construct the second latin square L_2 we substitute row 2 of L_1 with the bottom row of L_1 , so that row 2 of L_1 now becomes row 3 of L_2, row 3 of L_1 become row 4 of L_2 and so on while the first row of any L_i (i=1, 2…4) remains fixed. Thus, L_2 from the finite semi-group modulo $FS\ (5) = (Z_3,\ +)\langle\theta\rangle$ becomes

$$L_2 = \begin{matrix} e & f & g & \phi & \phi^2 \\ \phi^2 & e & f & g & \phi \\ f & g & \phi & \phi^2 & e \\ g & \phi & \phi^2 & e & f \\ \phi & \phi^2 & e & f & g \end{matrix}$$

Next, we form L_3 and L_4 using same construction processes . Hence,

$$L_3 = \begin{matrix} e & f & g & \phi & \phi^2 \\ \phi & \phi^2 & e & f & g \\ \phi^2 & e & f & g & \phi \\ f & g & \phi & \phi & e \\ g & \phi & \phi^2 & e & f \end{matrix},$$

$$L_4 = \begin{matrix} e & f & g & \phi & \phi^2 \\ g & \phi & \phi^2 & e & g \\ \phi & \phi^2 & e & f & g \\ \phi^2 & e & f & g & \phi \\ f & g & \phi & \phi^2 & e \end{matrix}$$

These are (n-1) mutually orthogonal Latin squares constructed from the finite semi-group modulo $FS\ (5) = (Z_3,\ +)\langle\theta\rangle$.

Again, consider the finite semi-group modulo $FS\ (n) = (Z_p,\ +)\langle\theta\rangle$ for even p and n is prime. In particular, let n = 7, p = 4 so that $FS\ (7) = (Z_4,\ +)\langle\theta\rangle = \{0,\ 1,\ 2, 3,\ \theta,\ \theta^2,\ \theta^3\}$. The table for the finite semi-group modulo is shown in Table 2 below, by letting e = 0+0 = θ^3+1 = 2+2 = 1+3 = 3+θ = θ^2+θ^2 = θ+θ^3 · f = 1+0 = 0+1 = θ^2+2 = 2+3 = θ+θ = 3+θ^2 = θ^3+θ^3 · g = 2+0 = 1+1 = 0+2 = θ+3 = θ^2+θ = θ^3+θ^2 = 3+θ^3 · h = 3+0 = 2+1 = 1+2 = 0+3 = θ^3+θ = θ+θ^2 = θ^2+θ^3· Notice that $\forall\ a,b,c \in FS(n),\ a+(b+c) = (a+b)+c$.

Table 2. Cayley Table of Finite Semigroup Modulo 7.

+	e	f	g	h	ϕ	ϕ^2	ϕ^3
e	e	f	g	h	ϕ	ϕ^2	ϕ^3
f	f	g	h	e	ϕ^2	ϕ^3	ϕ
g	g	h	e	F	ϕ^3	ϕ	ϕ^2
h	h	ϕ	ϕ^2	ϕ^3	e	F	g
ϕ	ϕ	ϕ^2	ϕ^3	g	f	h	e
ϕ^2	ϕ^2	ϕ^3	f	θ	g	e	h
ϕ^3	ϕ^3	e	θ	θ^2	h	g	f

Take notice that Table 2 is a Latin square of 7×7 size. From Proposition 5 we expect n-1 MOLS L_1, L_2 …L_{n-1}. L_1 is the Latin square formed from Table 2.

$$L_1 = \begin{matrix} e & f & g & h & \theta & \theta^2 & \theta^3 \\ f & g & h & e & \theta^2 & \theta^3 & \theta \\ g & h & e & f & \theta^3 & \theta & \theta^2 \\ h & \theta & \theta^2 & \theta^3 & e & f & g \\ \theta & \theta^2 & \theta^3 & g & f & h & e \\ \theta^2 & \theta^3 & f & \theta & g & e & h \\ \theta^3 & e & \theta & \theta^2 & h & g & f \end{matrix}$$

To construct L_2, we permute the objects of $FS(7)=(Z_4,\ +)<\theta>$ such that for any L_{ij} and L_{kl} when superimposed (i,j) ≠, (k,l).

$$L_2 = \begin{matrix} e & f & g & h & \theta & \theta^2 & \theta^3 \\ \theta^3 & e & \theta & \theta^2 & h & g & f \\ f & g & h & e & \theta^2 & \theta^3 & \theta \\ g & h & e & f & \theta^3 & \theta & \theta^2 \\ h & \theta & \theta^2 & \theta^3 & e & f & g \\ \theta & \theta^2 & \theta^3 & g & f & h & e \\ \theta^2 & \theta^3 & f & \theta & g & e & h \end{matrix}$$

Next, L_3 is constructed by the same process of forming L_2 making sure that no two coordinates are equal when superimposed except the first row of any L_{ij}.

$$L_3 = \begin{matrix} e & f & g & h & \theta & \theta^2 & \theta^3 \\ \theta^2 & \theta^3 & f & \theta & g & e & h \\ \theta^3 & e & \theta & \theta^2 & h & g & f \\ f & g & h & e & \theta^2 & \theta^3 & \theta \\ g & h & e & g & \theta^3 & \theta & \theta^2 \\ h & \theta & \theta^2 & \theta^3 & e & f & g \\ \theta & \theta^2 & \theta^3 & g & f & h & e \end{matrix}$$

Again, we construct L_4 as follows:

$$L_4 = \begin{matrix} e & f & g & h & \theta & \theta^2 & \theta^3 \\ \theta & \theta^2 & \theta^3 & g & f & h & e \\ \theta^2 & \theta^3 & f & \theta & g & e & h \\ \theta^3 & e & \theta & \theta^2 & h & g & f \\ f & g & h & e & \theta^2 & \theta^3 & \theta \\ g & h & e & f & \theta^3 & \theta & \theta^2 \\ h & \theta & \theta^2 & \theta^3 & e & f & g \end{matrix}$$

Again, L_5 is constructed thus:

$$L_5 = \begin{matrix} e & f & g & h & \theta & \theta^2 & \theta^3 \\ h & \theta & \theta^2 & \theta^3 & e & f & g \\ \theta & \theta^2 & \theta^3 & g & f & h & e \\ \theta^2 & \theta^3 & f & \theta & g & e & h \\ \theta^3 & e & \theta & \theta^2 & h & g & f \\ f & g & h & e & \theta^2 & \theta^3 & \theta \\ g & h & e & f & \theta^3 & \theta & \theta^2 \end{matrix}$$

The next Latin square is $L_{n-1} = L_6$. Thus,

$$L_6 = \begin{matrix} e & f & g & h & \theta & \theta^2 & \theta^3 \\ g & h & e & f & \theta^3 & \theta & \theta^2 \\ h & \theta & \theta^2 & \theta^3 & e & f & g \\ \theta & \theta^2 & \theta^3 & g & f & h & e \\ \theta^2 & \theta^3 & f & \theta & g & e & h \\ \theta^3 & e & \theta & \theta^2 & h & g & f \\ g & g & h & e & \theta^2 & \theta^3 & \theta \end{matrix}$$

The above Latin squares are constructed from the finite semi-group modulo n $FS(7)=(Z_4,\ +)\langle\theta\rangle$. Recall that proposition 5 , there are n-1 Latin squares in any finite semi-group modulo of n order .

VI. SYMMETRIC CRYPTOGRAPHY AND MUTUALLY ORTHOGONAL LATIN SQUARES

Symmetric cryptography involves the use of same key for encryption and decryption of cipher text so that no third party can read it. When a sender sends a message, he first encrypts it, then send the encrypted form to the receiver of the message. The receiver decrypts the message using same key of the sender which is made known only to the receiver by the sender. Mutually orthogonal Latin squares could be used in the creation of codes, one way to do this is :

Take any two or more MOLS formed from a finite semi-group modulo. Assign every coordinates, a letter or symbols on which of the L_i (i = 1,2 …n-1) MOLS to be used. The sender encrypts the message by substituting each letter or symbol to the corresponding coordinates, sends it. The receiver then decrypts the message by using same key (i.e same MOLS). Since every coordinate occurs only once, unless a third party knows the two or more mutually orthogonal Latin squares used and which letter or symbol corresponds to which coordinates, it is difficult and impossible to decrypt it, making it an effective coding system. When n is larger, the construction of Carley table which turns out to be a Latin square satisfying semi-group conditions is complex. Hence, below is a proposed claim that could be used as a guide to construction of Latin square from a finite semi-group modulo of any order n.

VII. APPLICATION OF MUTUALLY ORTHOGONAL LATIN SQUARES CONSTRUCTED FROM FINITE SEMI-GROUP MODULO N TO SYMMETRIC CRYPTOGRAPHY.

The basic aim of symmetric cryptography is that when a sender wants to sends a message, he/she first encrypts it before sending, so that no third party can read the message. The receiver then accepts the message, decrypts it using same code used for the encryption of the message.

Mutually orthogonal Latin squares can be applied to creation of codes, this is done thus :- Take any two or more (MOLS) L_i (i = 1,2,3, …n-1) of n order, assign each coordinates, a letter or symbol. Here, the sender and receiver must agree before hand on the L_i (i = 1,2,3 n-1) mutually orthogonal Latin squares constructed from a finite semi-group $FS(n)=(Z_p,\ +)<\theta>$ to be used.

The sender then encrypts the message by substituting each letter or symbol with corresponding coordinates, and sends it. The receiver then decrypts the message by using same MOLS. Since every coordinate occurs only once and distinct, unless a third party knows the two or more mutually orthogonal Latin squares used and which letter corresponds to which coordinates, it is difficult and impossible to decrypt it, making it an effective coding system for hiding sensitive and confidential materials or information.

Consider the six MOLS constructed from the finite semi-group modulo n=7 and p=4 , $FS(7)=(Z_4,\ +)\langle\theta\rangle$ with L_1 formed from the semi-group table (Table 2) and $L_1, L_2\ldots\ldots L_{n-1}\in L^n$ are the set of the n-1 MOLS. Choose any two MOLS say L_2 and L_3. Then, form a corresponding Latin square of alphabets together with elements or symbols as shown below :

e	f	g	h	θ	θ^2	θ^3	e	f	g	h	θ	θ^2	θ^3
θ^3	e	θ	θ^2	h	g	f	θ^2	θ^3	f	θ	g	e	h
f	g	h	e	θ^2	θ^3	θ	θ^3	e	θ	θ^2	h	g	f
g	h	e	f	θ^3	θ	θ^2	f	g	h	e	θ^2	θ^3	θ
h	θ	θ^2	θ^3	e	f	g	g	h	e	f	θ^3	θ	θ^2
θ	θ^2	θ^3	g	f	h	e	h	θ	θ^2	θ^3	e	f	g
θ^2	θ^3	f	θ	g	e	h	θ	θ^2	θ^3	g	f	h	e

P	V	Q	M	R	T	L
A	K	N	U	S	J	W
Y	B	I	X	O	C	F
D	G	Z	H	E	?	!
%	)	"	(	:	,	/
.	=	+	−	9	0	1
2	8	3	6	4	7	5

Worthy of note is that the position of any alphabet of the n×n grid of alphabets and symbols are immaterial, with the two mutually orthogonal latin squares above (ie L_2 and L_3) combining with the n×n grid of alphabets and symbols, any length of text could be sent since the whole twenty-six alphabets are involved including some symbols. It then follows that if n>7 in the finite semi-group $SF(n)=(Z_p,\ +)\langle\theta\rangle$, more symbols will be accommodated in the n×n grid of alphabets and characters.

The good thing about the use of finite semi-group modulo $FS(n)=(Z_p,\ +)\langle\theta\rangle$ to symmetric cryptography is that, it is very difficult for a third party to have access to the encrypted text. Hence, the sender must let the receiver know the mutually orthogonal latin squares with n×n grid of alphabets and symbols selected for the encryption, so that the receiver will use the same for decryption.

Now, consider a message sent by the commissioner of police of a state command to a Divisional Police Officer (DPO) ordering the invading of kidnappers hideout and arrest in a particular location of the DPO's jurisdiction on a scheduled date. The message read thus:-

"Due to intelligent report reaching me, I write to get you informed of a certain group of kidnappers in your domain whose criminal activities have caused lost of lives and properties of innocent citizens. Consequently the said kidnappers usually hold meetings for concoction every tenth day of the month at a forest adjacent to the blue sea at JIMUDU in OTOBO village by ten pm prompt. I hereby order the invading of the hideout and arrest of these kidnappers.

Below is an extract of the encrypted form of the above message.

$(g,f)(\theta^2,\theta)(\theta^3,\theta^2)\quad(\theta^2,\theta^2)(\theta^3,h)$
$(h,\theta)(\theta,f)(\theta^2,\theta^2)(\theta^3,\theta^2)(\theta^3,\theta^3)(\theta^3,\theta^3)(h,\theta)(h,g)(\theta^3,\theta^2)(\theta,f)(\theta^2,\theta^2)$
$(\theta,\theta)(\theta^3,\theta^2)(\theta,\theta)(\theta^2,h)(\theta,\theta)(\theta^2,\theta^2)$
$(\theta,\theta)(\theta^3,\theta^2)(\theta^2,\theta^3)(f,\theta^2)(\theta^3,g)(f,\theta)(h,f)(\theta,f)(h,g)$
$(h,h)(\theta^3,\theta^2)\quad(h,\theta)$
$(f,h)(\theta,\theta)(h,\theta)(\theta^2,\theta^2)(\theta^3,\theta^2)$
$(\theta^2,\theta^2)(\theta^3,h)$
$(h,g)(\theta^3,\theta^2)(\theta^2,\theta^2)\quad(f,\theta^3)(\theta^2,h)(\theta^2,\theta)$
$(h,f)(\theta,f)(\theta,f)(\theta^2,h)(\theta,\theta)(h,h)(\theta^3,\theta^2)(g,f)$
$(\theta^2,h)(\theta,f)(\theta^3,\theta^2)(\theta^3,\theta^2)$
$(\theta,\theta)(\theta^2,\theta^2)(\theta^3,\theta^2)(h,f)(\theta,f)$
$(h,g)(\theta,\theta)(\theta^2,h)(\theta^2,\theta)(\theta,\theta)\quad(\theta^2,h)(\theta,f)$
$(\theta,\theta^3)(h,\theta)(g,f)(\theta,f)(\theta^3,\theta^2)$
$(\theta,\theta)(\theta,\theta)(\theta^3,\theta^2)(\theta,\theta)(h,g)$

$(h,\theta)(\theta,f)\quad(f,\theta^3)(\theta^2,h)(\theta^2,\theta)(\theta,\theta)$
$(g,f)(\theta^2,h)(h,h)(\theta^3,\theta^2)(h,f)(\theta,f)$
$(f,h)(f,\theta)(\theta^2,h)(h,g)(\theta^3,\theta^2)$
$(\theta^3,g)(\theta,\theta)(h,\theta)(h,h)(h,\theta)(\theta,f)(\theta^3,\theta^2)(\theta^3,\theta^3)$

VIII. CONCLUSION

From investigations of this study, it is concluded that the application of mutually orthogonal Latin Squares constructed from a finite semi-group modulo n to symmetric cryptography remains an effective coding technique for hiding sensitive and confidential information from unauthorized person(s) and be sure that such sensitive and confidential information only get to the authorized person(s) thereby reducing crime rate if not eliminated totally.

References

[1] K. Jayshire and V. Gaji (2014). Lagrange *Property for Finite Semigroups.* Ultra Scientist Journal. Vol. 26, 283-289, (2014).

[2] G. Oleg , J. Lawson, and R. Duson). *Semigroup Closure of Finite Rank Symmetric Inverse Semigroup*. Semigroup Forum,(2009).

[3] A. Nagy. *On Faithful Representation of Finite Semigroup of degree /S/ Over the Fields.* International Journal of Algebra Vol. 7. no. 3,115 – 125, (2013).

[4] G. Olexandr, and M. Volodymyer. *On The Irreducible Representation of Finite Semigroup.* Proc. Timier. Maths Society 137, no 11, 35 -85 - 3592, (2005).

[5] A. Joao, B. Wolfram and K. Janusz. *The Commutative Graph of The Finite Non-commutative semigroup*. Journal of Mathematics. Dol: 10, 1007S11 856 – 015 - 1173 – 9, (2012*).*

[6] J. G. Dustin. *Permutation presentation of Non-abelion Simple groups.* University Press Oxford, (2015).

[7] I. Wanless . *Transversals in Latin Squares.* Quasigroup Related System. 15: 169-190, (2007).

[8] A. D. Keedwell and J. Denes *Latin Squares and their Applications*. Elsevier, (2015).

[9] R. Dalta and A. Touba. *Generating Burst-error Correcting Codes From OrthogonalLatinSquares*.International Symposium, (2011).

[10] J. Egan. *Latin Squares With Large Indivisible Plexes* . Journal of Combinatorial Theory. Series A. 118 (3): 796- 807, (2011).

[11] I. Gallego . *Generation of Random Latin Squares.* Congreso Argentino (BuenusAircs), (2014).

[12] B. Musto and J. Vicary. Quantum Latin Square and Unitary Error Bases, Elsevier, (2016).

[13] F. Katmoska. *On Algebras of Generalized latin Squares.* Mathematica , Bohemica, 91-103, (2009).

[14] J. Egan and M. Wanless. *Latin Squares with Restricted Transversals.* Journal of Combinatorials Designs: 20(2) : 124-141, (2012*).*

[15] B. Jordan . *On Magic Squares* Preprint maths /0408230, (2004).

[16] A. Vikas, A. Shruti, and D. Rajesh . *Analysis and review of Encryption/Decryption for Secure Communication.* Int'l Journal of scientific Engineering and research. Vol. 2 Issue 5, (2014).