International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 10 (2015) pp. 25075-25080

http://www.ripublication.com

Construction of A New Cryptosystem From An Arithmetic Group

Chandradeo Prasad
Assistant Professor, RGIT, Koderma, India
E-mail :cpsindri@gmail.com

Abstract

In symmetric key cryptosystem, a single key is used for both encryption and decryption. It is the most widely used cryptosystem in which the sender and receiver parties share a single key . In this paper a new symmetric key cryptosystem is constructed with the help of an arithmetic group of 3- tupples. Properties of circulant matrix and Galois field of prime order are applied for the construction of this new cryptosystem.

Key words: key, cryptosystem, abelian group, symmetric key, circulant matrix, congruence.

Introduction

Cryptosystem:
A cryptosystem is a security mechanism. It eliminates the need to trust the network. It is based on secrets called keys that are selectively distributed to the computers in a network and used to process messages. Cryptography enables a recipient to verify that the message was created by some computer possessing a certain key and this key is the source of the message , Similarly for a sender, this key become the the destination. Keys are designed in such a way that it is not computationally feasible to derive them from the messages they were used to generate. These keys provide a much more trustworthy means of constraining senders and receivers of the message.

Symmetric Key Cryptosystem:
A symmetric key cryptosystem is a collection of encryption algorithm, all types of plain texts, secret key, cipher texts and decryption algorithms where the sending and receiving parties know each other and have disclosed the information about private keys toeach other.

Circulant Matrix

A n * n matrix of the following form

$a_1\ a_2\ a_3\ a_4$ ... a_n
$a_n a_1\ a_2\ a_3$ ... a_{n-1}
$a_{n-1}\ a_n\ a_1\ a_2$ ... a_{n-2}
.....
.....
$a_2\ a_3\ a_4\ a_5$ ... a_1

is called a circulant matrix.

A circulant matrix has the following properties :

- Sum of two circulant matrices is a circulant matrix.
- Product of two circulant matrices is a circulant matrix.
- Inverse of a circulant matrix is a circulant matrix.

Galois Fields:

If the set F has the finite numbers of elements, the F is called a finite field or a Galois Field. If F=(F,+,.) is Galois Field , then $|F|=p^n$ where p is prime and n is a positive integer.

Arithmetic Group:

An arithmetic group is a non-empty set G of numbers together with a law of binary composition which is associative and has an identity element, and such that every element of G has an inverse.

Abelian Group:

An abelian group is a group whose law of composition is commutative.

Linear Congruence:

A number a is said to be linear congruent to b modulus m if (a-b) is divisible by m. This is represented as

$a \equiv b \pmod m$

In this paper, a symmetric key cryptosystem is constructed with the help of a new arithmetic group.

Properties of circulant matrix and Galois field of prime order are used here.

General Algorithms

Algorithm I

Input: Given a finite abelian group G of order m and k is prime to m

Output: $a \neq b \Rightarrow a^k \neq b^k$

Step I:Let us assume that $a^k=b^k$

Step II: Since $a^k=b^k$

$\Rightarrow a^k(b^{-1})^k=e$

$\Rightarrow(ab^{-1})^k=e$
$\Rightarrow o(ab^{-1})|k$ ……. ….. [1]
Also $o(ab^{-1})|o(G)=m$ …… …… [2]
Since $o(ab^{-1})\neq 1$, (1)$\Rightarrow$k is not prime to m, which is a contradiction.
Therefore, $a^k\neq b^k$
This proves the algorithm.

Algorithm II

Input: Given the expression
$a_1x_1+a_2x_2+\ldots+a_nx_n\equiv b(\text{mod } m)$
Output: The expression has solutions if
$d=G.C.D.(a_1,a_2,a_3,\ldots.a_n,m)$ divides b. (The results are known vide [1] and [2]).
Also the number of solutions$=d*m^{n-1}$.

Symmetric Cryptosystem Algorithm

The construction of the symmetric cryptosystem is based on the following algorithm III :

Algorithm III

Input : $Z_p^3=Z_p*Z_p*Z_p$, and
$X=\{(a,b,c,)\in Z^3 : Det(circ(abc)\}=a^3+b^3+c^3-3abc\equiv 0(modp)\}$.
Output :An abelian group $G_p= Z_p^3-X$

Step I: We have
$(a_1,b_1,c_1)(a_2,b_2,c_2)=(A,B,C)$ iff $circ(a_1,b_1,c_1)circ(a_2,b_2,c_2)=circ(A,B,C)$

Step II: Let us assume that

- $(a_1,b_1,c_1),(a_2,b_2,c_2),(a_3,b_3,c_3),\ldots..\in G_p$,
- '$\equiv 0(\text{mod } p)$' be denoted by '=0',
- Also addition and multiplication mod p be denoted by juxtaposition.

Step III: Now let us check the properties of a group forG_p

1. Closure

$(a_1,b_1,c_1).(a_2,b_2,c_2)=(A,B,C)\Rightarrow circ(a_1,b_1,c_1)circ(a_2,b_2,c_2)=circ(A\ B\ C)$
$\Rightarrow$det $circ(a\ a_1,b_1,c_1)$det $circ(a_2,b_2,c_2)$=det circ(A B C)
Hence
det $circ(a\ a_1,b_1,c_1)\neq 0$ and det $circ(a_2,b_2,c_2)\neq 0$
$\Rightarrow$det $circ(a_1,b_1,c_1)$det $circ(a_2,b_2,c_2)\neq 0$ (since Z_p is an integral domain, so it is without zero divisors)
$\Rightarrow$det circ(A B C)$\neq 0$
$\Rightarrow(A,B,C)\in G_p$

2. Assocativity

$[circ(a_1,b_1,c_1)circ(a_2,b_2,c_2)circ(a_3,b_3,c_3)= circ(a_1,b_1,c_1)circ(a_2,b_2,c_2)circ(a_3,b_3,c_3)]$

$\Rightarrow circ[(a_1,b_1,c_1) . (a_2,b_2,c_2)] \; circ \; (a_3,b_3,c_3)= circ(a_1,b_1,c_1)circ[(a_2,b_2,c_2) . (a_3,b_3,c_3)]$

$\Rightarrow [(a_1,b_1,c_1)(a_2,b_2,c_2)](a_3,b_3,c_3)= (a_1,b_1,c_1)[(a_2,b_2,c_2)(a_3,b_3,c_3)]$

3. Identity

It can be easily shown that (1,0,0) is an identity.

4. Existence of inverse

We have $(a,b,c)) \in G_p \Rightarrow$ det circ(a b c)$\neq 0$

Let $(a,b,c)^{-1} = (a',b',c')$

Here $circ(a',b',c')=[circ(a,b,c)]^{-1}$

5. Commutative : Obviously the product is commutative.

$(a_1,b_1,c_1) . (a,b,c) = (a,b,c). (a_1,b_1,c_1)$

Since G contains all the properties of an abelian group,

So it is established that G_p is an abelian group.

Counting The Order of The Group

We have

$G_p = Z_p^3 - X \Rightarrow o(G_p)= o(Z_p^3) - o(X)=p^3 - o(X)$ ---------- [3]

Also o(X)= the number of solutions of the congruence $a^3+b^3+c^3-3abc \equiv 0(mod p)$

= the number of solutions of $a+b+c\equiv 0(\text{mod } p)$

And $\alpha+\alpha^2 b+\alpha c \equiv 0(\text{mod } p)$, $\alpha+\alpha b+\alpha^2 c \equiv 0(\text{mod } p)$

$\alpha+\alpha^2 b+\alpha c \equiv 0(\text{mod } p)$, where α is a primitive root of $\alpha 3\equiv 1(\text{mod } p)$

$=p^2+p^2+p^2-1-p-1+1=3p^2-p-1$

From (1), $o(G_p) = p^3 - 3p^2 + p + 1 = (p - 1)(p^2 - 2p - 1)$

Remarks

The number of solution of $a + b + c = 0$ is p^2.

The number of solution of $\alpha + \alpha b + \alpha^2 c = 0$ is p^2.

The number of solutions of $\alpha + \alpha^2 b + \alpha c = 0$ is p^2.

Order of the group $G_p = o(G_p) = (p - 1)(p^2 - 2* p - 1)$, where p is a prime, there exists an abelian group of order $3k(9k^2 - 2)$.

A symmetric key cryptosystem is obtained by choosing a number prime to $o(G_p)$.

If p_1 is one of the number prime to $o(G_p)$, the map $f : G_p \rightarrow G_p$ given by $f(x) = x^{p1}$ is an injection. This gives a symmetric key cryptosystem.

Example 1: If from $Z_7 \times Z_7 \times Z_7$, the following triplets are removed, it is a group.

(1) (a,b,c), where a=b=c.

(2) (a,b,c) where $a+b+c\equiv 0(\text{mod } 7)$.

(3) (a,b,c) where

$\alpha + \alpha b + \alpha^2 c = 0(\text{mod } 7)$

$\alpha+\alpha^2b + \alpha c = 0(\text{mod } 7)$ where $\alpha^3 \equiv 1(\text{mod } 7)$ and α is not congruent to 1 mod 7.

Here $\alpha = 2$, we proceed to find solutions of the following equations:
$\alpha+2b+4c=0$
$\alpha+4b+2c=0$
The solutions for $\alpha+2b+4c = 0$ are (1,3,0), (1,1,1), (3,2,0), (3,0,1), (5,1,0).
These are vectors orthogonal to (1,2,4) in Z_7^3 . However there are more such vectors.

Our aim is to find all the vectors orthogonal to (1,2,4) in Z_7^3 . We have that if (1,3,0) is a solution of $\alpha +2b+4c \equiv 0(\text{mod } p)$, then k(1,3,0), k= 1,2,3,4,5,6 is also a solution. All solutions are
(1,1,1), (2,2,2), (3,3,3), (4,4,4), (5,5,5), (6,6,6), (1,2,4),
(2,4,1), (3,6,5), (4,1,2), (5,3,6), (6,5,3), (1,3,0), (2,6,0),
(3,2,0), (4,5,0), (5,1,0), (6,4,0), (1,0,5), (2,0,3), (3,0,1),
(4,0,6), (5,0,4), (6,0,2), (1,4,3), (2,1,6), (3,5,2), (4,2,5),
(5,6,1), (6,3,4), (1,5,6), (2,3,5), (3,1,4), (4,6,3), (5,4,2),
(6,2,1), (1,6,2), (2,5,4), (3,4,6), (4,3,1), (5,2,3), (6,1,5),
(0,1,3), (0,2,6), (0,3,2), (0,4,5), (0,5,1), (0,6,4) and (0,0,0).
The base is given by
{(1,1,1), (1,2,4), (1,3,0), (1,0,5), (1,4,3), (1,5,6), (1,6,2), (0,1,3)}
All solutions are obtained by multiplying each solution by 0,1,2,3,4,5,6. There are in all 49 solutions.
The number of solutions of $a+b+c=0$ is $7^2 = 49$.
The number of solutions of $\alpha+2b+4c=0$ is $7^2 = 49$.
The number of solutions of $\alpha +4b+2c=0$ is $7^2 = 49$.

The order of the group $G_7 = (7 – 1)(7^2 – 2.7 – 1) = 204$.
A symmetric key cryptosystem is obtained by choosing a number prime to 204 (e.g. 13). The map $f : G_7 \rightarrow G_7$ given by $f(x) = x^{13}$ is an injection.
This gives a symmetric key cryptosystem.

Example 2: We consider the following group :
$G_{13} = \{(a,b,c) \in Z_{13}^3 : \text{detcirc}(a,b,c) \text{ is not congruent to } 0 \text{ mod } 13 \}$.
The number of solutions of $a+b+c=0$ is $13^2 = 169$.
The number of solutions of $\alpha +2b+4c=0$ is $13^2 = 169$
The number of solutions of $\alpha +4b+2c=0$ is $13^2 = 169$
The order of the group $G_{13} = (13 – 1)(13^2 – 213 – 1) = 1704$.
A symmetric key cryptosystem is obtained by choosing a number prime to 1704 (e.g. 13). The map $f : G_{13} \rightarrow G_{13}$ given by $f(x) = x^{13}$ is an injection.
This gives a symmetric key cryptosystem.

Example 3: We consider the following group :
$G_{19} = \{(a,b,c) \in Z_{19}^3 : \text{detcirc}(a,b,c) \text{ is not congruent to } 0 \text{ mod } 1 \}$.
The number of solutions of $a+b+c=0$ is $19^2 = 361$.
The number of solutions of $\alpha +2b+4c=0$ is $19^2 = 361$.

The number of solutions ofα +4b+2c=0 is $19^2 = 361$.

The order of the group $G_{19} = (19 – 1)(19^2 – 2.19 – 1) = 5796$.

A symmetric key cryptosystem is obtained by choosing a number prime to 5796 (e.g. 13). The map $f : G_{19} \rightarrow G_{19}$given by$f(x) = x^{13}$ is an injection.

This gives a symmetric key cryptosystem.

Conclusion

A new symmetric key cryptosystem is constructed with the help of an arithmetic group of 3- tupples. Properties of circulant matrix and Galois field of prime order are applied for the construction of this new cryptosystem. It can be made more complex by extending the group to the arithmetic group of n-tupples.

References

[1] David E Goldberg,,, Genetic algorithms in search, optimization and machine learning", Addision- Wesley Pub.Co.1989.

[2] C. E. Shannon, "Communication Theory of Security System", Bell, System Technical Journal, 28, 1949

[3] A. J. Bagnall, "The Applications of Genetic Algorithms in Cryptanalysis", School of Information Systems, University Of East Anglia, 1996.

[4] N. Koblitz , ,,A Course in Number Theory and Cryptography", Springer-Verlag, New York, Inc., 1994.

[5] Menzes A. J., Paul, C., Van Dorschot, V., Vanstone, S. A., "Handbook of Applied Cryptography", CRS Press 5th Printing; 2001.

[6] National Bureau Standards, "Data Encryption Standard (DES)," FIPS Publication 46; 1977

[7] Tragha A., Omary F., Mouloudi A.,"ICIGA: Improved Cryptography Inspired by Genetic Algorithms", Proceedings of the International Conference on Hybrid Information Technology (ICHIT'06), pp. 335-341, 2006.

[8] Spillman R, Janssen M, Nelson B and Kepner N, "Use of Genetic Algorithm in Cryptanalysis of Simple Substitution Cipher" Cryptologia, Vol.17, No.4, pp. 367- 377, 1993.

[9] SpillmanR," Cryptanalysis of Knapsack Ciphers using Genetic Algorithms", Cryptologia, Vol.17, No.4, pp. 367-377, 1993.

[10] Garg Poonam, Genetic algorithm Attack on Simplified Data Encryption Standard Algorithm, International journal Research in Computing Science, ISSN1870-4069, 2006.

[11] Nalini, Cryptanalysis of Simplified data encryption standard via Optimization heuristics, International Journal of Computer Sciences and network security, vol 6, No 1B,Jan 2006. 2nd National Conference in Intelligent Computing & Communication Organized by Dept. of IT, GCET, Greater Noida, INDIA. ISBN: 9788175157538