Algebraic Structural Application of Finite Field $GF(p^m)$ in Cryptography

Ramachandran S
Research Scholar
Department of Mathematics and Actuarial Sciences
B. S. Abdur Rahman Crescent Institute of Science & Technology
Tamil Nadu India

Dr. Sindhu J Kumaar
Associate Professor
Department of Mathematics and Actuarial Science
B. S. Abdur Rahman Crescent Institute of Science \& Technology
Tamil Nadu India

Dr. Jayakumar C V
Principal
St. Peter's College of Engineering & Technology
Tamil Nadu India

Abstract:- Cryptography is the science which associates with the process of converting plain text information into cipher text and vice- versa. Data security concerned cryptography plays vital role in confidentiality, reliability and authenticity in data transmission through public network. Cryptography is one of the most important application areas of the finite field arithmetic. Almost all public key cryptography depends on finite field arithmetic including the recent algorithms like Elliptic curve and Pairing based cryptography. While considering the objectives execution speed and design space constraint of algorithms constitute enormous challenges, which necessitate interdisciplinary research effort towards the best algorithmic structure and solid data security. This paper proposes to provide concise designing architecture and high level of security in communication network.

Keywords:- Finite field, Multiplicative inverse, Polynomial, Cipher digital sequence

1. INTRODUCTION

Cryptography is where data security meets mathematical theory. At present the whole world depends on internet and its applications on every part of life. Organizations around the world generate a large number of data and transmit through public network every day. Information and data security concern cryptography plays a vital role in preventing private data from unauthorized usage. Also cryptography provides secure transmission of data through social network. There are two types of ciphers, stream cipher and block cipher. The stream cipher is data encoding according to the stream of the position of plaintext symbols but several plaintext symbols are encoded in the block cipher at once. Modern cryptography relays various mathematical applications and techniques to keep cores droppers away from using the content of encrypted data [3] [7].

Finite field arithmetic is one of the principal application areas of cryptography. Finite field is a field in which there exist only finitely many elements, which is also known as Galois Fields. Computer data consists of combination of two numbers 0 and 1, which are elements of finite field GF(2). Since there is one-to-one correspondence between ASCII Code of 256 characters and the elements of finite field $GF(2^8)$, [3] [6], there is a function from the characters with Unicode 13.0 to $GF(2^{18})$ and also computer data can be represented as combination of vectors in finite field, which admits mathematical operations to scramble data effectively. This work

provides **concise** cryptosystem based on the algebraic structure of general finite field GF(p^m) with the combination of both types of ciphers.

2. ALGEBRAIC STRUCTURE 0F FINITE FIELD

Finite field has several interesting structures in various directions. We here present few of them. If p is a prime and the set $Z_p = \{0,1,2,3, \ldots \ldots \ldots, p-1\}$ then $(Z_p, +_p, *_p)$ is a finite field of order p, If the set $Z_p(x)$ is the ring of polynomials over Z_p and $a(x)$ is an n^{th} degree irreducible polynomial over Z_p then $F = {Z_p(x)}/{< a(x) >}$ is a finite quotient field. The field F has p^n elements, each of the form $a_k x^k + a_{k-1}x^{k-1} + \ldots + a_1 x + a_0$ where $k < n$ and $a_0, a_1, \ldots, a_k$ are elements in Z_p. Galois field $GF(p^m)$ is the set of all roots of the *polynomial* $g(x) = x^{p^m} - x$ and the roots are 0, 1, ω^1, $\omega^2, \ldots, \omega^{p^m-2}$ where $\omega^{p^m-1} = 1$. Clearly

$$GF(p^m) \approx {Z_p(x)}/{< f(x) >} \approx \underbrace{Z_p \oplus Z_p \oplus \ldots. \oplus Z_p}_{m \ times} \quad (1)$$

With the correspondence $x^l \rightarrow [a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_l x^l + \cdots + a_1 x + a_0] \rightarrow (a_{m-1}, a_{m-2}, \ldots, a_l, \ldots, a_1, a_0)$, where $a_i \epsilon Z_p$ and $f(x)$ is an m^{th} degree irreducible polynomial over Z_p. [5], [6].

For example if $Z_2 = \{0,1\}$, then roots of the polynomial $h(x) = x^{2^3} - x$ are elements in the finite field $GF(2^3) = \{ 0, 1, \omega^1, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6\}$. By considering an irreducible polynomial $q(x) = x^3 + x + 1$ over Z_2 we have $GF(2^3) \approx {Z_2(x)}/{< q(x) >} \approx Z_2 \oplus Z_2 \oplus Z_2$. Representation of elements in isomorphic sets $GF(2^3)$, ${Z_2(x)}/{< q(x) >}$ and $Z_2 \oplus Z_2 \oplus Z_2$ are as in the table (1).

Elements			
$GF(2^3)$	${Z_2(x)}/{< q(x) >}$ $(\omega^3 + \omega + 1 = 0 \Rightarrow \omega^3 = \omega + 1)$	$Z_2 \oplus Z_2 \oplus Z_2$ (Binary)	Regular (Digital)
0	$0\omega^2 + 0\omega + 0$	(000)	0
1	$0\omega^2 + 0\omega + 1$	(001)	1
ω^1	$0\omega^2 + 1\omega + 0$	(010)	2
ω^2	$1\omega^2 + 0\omega + 0$	(100)	4
ω^3	$0\omega^2 + 1\omega + 1$	(011)	3
ω^4	$1\omega^2 + 1\omega + 0$	(110)	6
ω^5	$1\omega^2 + 1\omega + 1$	(111)	7
ω^6	$1\omega^2 + 0\omega + 1$	(101)	5

Table 1. Representation of elements

By considering 8^{th} degree irreducible polynomial over Z_2, a unique element in $GF(2^8)$ can be identified for each ASCII code of 256 characters and its 8 bits binary representation. This one -to - one correspondence allows mathematical operations to scramble binary data effectively.

3. MULTIPLICATIVE INVERSE

Proposed cryptosystem strongly depend on the concept of irreducible polynomial and multiplicative inverse of polynomials. There are two method for finding multiplicative inverse, namely Extended Euclidian Algorithm (EEA) and Arithmetic method. Since EEA fails to find multiplicative inverse of all non zero polynomials arithmetic method is used to obtain multiplicative inverse of polynomial and the following theorem is used to construct irreducible polynomial in this work.

Theorem 1. If $p = 3\ (mod\ 4)$ is a prime and $p + 1 = 2^{\Upsilon}$. with s odd then for any integer $k \geq 1$, the polynomial $x^{2^k} - 2ax^{2^{k-1}} - 1$ is irreducible polynomial over F_p, and hence irreducible over F_{p^m}. For any odd integer m where $a = a_{\Upsilon}$ is recursively obtained as follows $(i)\ a_1 = 0$ $(ii)\ set\ a_j = (\frac{a_{j-1}+1}{2})(p+1)/4$, for j from 2 to $\Upsilon - 1$ and (iii) $a_{\Upsilon} = (\frac{a_{\Upsilon-1}-1}{2})\ (p+1)/4$.

4. PROPOSED WORK

The work Algebraic structural cryptosystem is a symmetric key cryptography, which enables almost all type of computer data. The work as follows, suppose that $uvwxyz$ ... ... , is the data to encrypt and corresponding binary string is 011101010111011001110111….. We first split binary string as a sequence $\{a_n\}$ of sub binary strings, each a_n of size M bits. Digital value of each substring a_n ranges from 0 to $2^M - 1$. Let p be a prime such that $p > 2^M - 1$ and let k be the number of bits in the binary representation of p. Then we form the digital sequence $\{b_n\}$ according to the digital value of each element in the sequence $\{a_n\}$ of sub binary strings, split digital sequence $\{b_n\}$ into sequence $\{c_n\}$ of digital sub string such that c_n of size m, then convert each $c_n = (c_{n_1}, c_{n_2}, \dots, c_{n_m})$ as a polynomial $c_n(x) = c_{n_1}x^{m-1} + c_{n_2}x^{m-2}$ ... $+c_{n_m}$ and then we construct the sequence of polynomials $\{c_n(x)\}$ each of degree $m - 1$.

By considering m^{th} degree irreducible polynomial $a(x) = x^m + a_{m-1}x^{m-1} + a_{m-2}x^{m-2}$ ... $+ a_2x^2 + a_1x + a_0$ over $GF(p)$, we form the sequence $\{d_n(x)\}$ of multiplicative inverse of polynomials in the sequence $\{c_n(x)\}$ such that $d_n(x) = \begin{cases} 0 & if\ \ c_n(x) = 0 \\ d_n(x)c_n(x) = 1\ mod\ a(x) & if\ \ c_n(x) \neq 0 \end{cases}$ over the field $GF(p)$. Suppose that $d_n(x) = d_{n_1}x^{m-1} + d_{n_2}x^{m-2}$ ... $+d_{n_m}$, we form cipher digital sequence $\{d_n\}$ where $d_n = (d_{n_1}, d_{n_2}, \dots, d_{n_m})$, also called vector representation in $Z_p \oplus Z_p \oplus$ .... $\oplus Z_p$. We now express each component d_{n_i} of d_n in the sequence $\{d_n\}$ into k bits binary expression and thus form cipher binary string. We finally split cipher binary string into sequence $\{s_n\}$ of sub cipher binary strings each s_n of size 6 bits. By using radix-64 representation we translate each sub s_n which results the required encrypted data (cipher text) for given data (plain text). Decryption process is in reverse order since the polynomial of degree less than m is a unique element in $GF(p^m)$. Symmetric key of this cryptosystem are irreducible polynomial $a(x)$ and prime p.

This work allows to encrypt the plain text file with minimum of N characters, where N is the multiple of L and the value of L and L is obtained by the equation

$$L = \frac{lcm(M,m,n)}{n} \qquad (2)$$

M is size each element in sequence $\{a_n\}$ of sub binary string, m is degree of irreducible polynomial $a(x)$ and n is number of bits in the representation of character. If given data do not meet the constraint of minimum number of characters, we add space character in minimum number at the end of data for requirement. [3] [5].

5. PROPOSED ALGORITHM

1) Plain text $uvwxyz$ .... and its binary string 01110101….
2) Split into sub strings, each of size M
3) Choose prime $p > 2^M - 1$ (symmetric key)
4) Form sequence of digital value of sub strings from step 2.
5) Choose an irreducible polynomial $a(x)$ of degree m over $GF(p)$
6) Split sequence of digital value into digital substring, each of size m, from step 4.
7) Construct polynomial $c_n(x)$ of degree $m - 1$ for each digital substring

8) Form sequence of polynomials $\{c_n(x)\}$ }
9) Construct sequence $\{d_n(x)\}$ }, the multiplicative inverse of each element in $\{c_n(x)\}$ } under modulo $a(x)$ over $GF(p)$ such that
if $c_n(x) = 0$ then
$d_n(x) = c_n(x)$
else
$d_n(x)\, c_n(x) \equiv 1 \ mod\ a(x)$
end
10) Form sequence of coefficients of polynomials in $\{ d_n(x)\}$, called cipher digital string
11) Express each member of cipher digital sequence as k bits binary representation, results cipher binary string.
12) Convert cipher binary string into radix - 64 representation
13) Cipher text
14) Exit.

6. EXAMPLE

We illustrate the proposed cryptosystem by considering plain text SUPER CIPHER, The ASCII code representation of characters of plain text are 83 85 80 69 82 32 67 73 80 72 69 82 and corresponding binary string is 01010011 01010101 01010000 01000101 01010010 00100000 01000011 01001001 01010000 01001000 01000101 01010010. Split binary string into a sequence $\{a_n\}$ of sub binary strings, each a_n of size 3 $(= M)$. That is {(010) (100) (110) (101) (010) (101) (010) (000) (010) (001) (010) (101) (001) (000) (100) (000) (010) (000) (110) (100) (100) (101) (010) (000) (010) (010) (000) (100) (010) (101) (010) (010)}. Digital value of each sub binary string ranges from 0 to 7 $(= 2^3 - 1)$. If we choose prime $p = 11$, binary representation of $11 = 1011$ therefore the number of bits in binary representation of 11 is $k = 4$. Clearly $p > 7$ and $p = 3\ (mod\ 4)$. By theorem (1) the polynomial $a(x) = x^4 + 3x^2 - 1\ (= x^4 + 3x^2 + 10)$ under modulo 11 is an irreducible polynomial over $GF(11)$ and $\deg a(x) = 4(= m)$ .By equation (2), the value of $L = \frac{lcm(3,4,8)}{8} = 3$. Since number of characters in the plain text is 12 which is multiple of $L = 3$ thus required condition holds.

The sequence $\{b_n\}$ of digital value of sub binary string is { 2 4 6 5 2 5 2 0 2 1 2 5 1 0 4 0 2 0 6 4 4 5 2 0 2 2 0 4 2 5 2 2}. We now split digital sequence $\{b_n\}$ into a sequence $\{c_n\}$ of digital substrings, each substring of size $4(= m)$, that is { (2 4 6 5) (2 5 2 0) (2 1 2 5) (1 0 4 0) (2 0 6 4) (4 5 2 0) (2 2 0 4) (2 5 2 2)}. The sequence $\{c_n(x)\}$ is { $2x^3 + 4x^2 + 6x + 5$, $2x^3 + 5x^2 + 2x + 0$, $2x^3 + 1x^2 + 2x + 5$, $x^3 + 0x^2 + 4x + 0$, $2x^3 + 0x^2 + 6x + 4$, $4x^3 + 5x^2 + 2x + 0$, $2x^3 + 2x^2 + 0x + 4$, $2x^3 + 5x^2 + 2x + 2$} .

Using arithmetic method the sequence $\{d_n(x)\}$ is multiplicative inverse of the above sequence $\{c_n(x)\}$ of polynomials under modulo $a(x) = x^4 + 3x^2 + 10$ over the finite field $GF(11)$. that is $\{d_n(x)\}$ = { $8x^3 + 0x^2 + 5x + 7$, $4x^3 + 6x^2 + 10x + 6$, $10x^3 + 2x^2 + 5x + 8$, $4x^3 + 0x^2 + 8x + 0$, $3x^3 + 4x^2 + 7x + 5$, $6x^3 + 10x^2 + 0x + 9$, $7x^3 + 2x^2 + 1x + 1$, $10x^3 + 1x^2 + 7x + 0$ }. Thus the cipher digital sequence $\{d_n\}$ is {8 0 5 7 4 6 10 6 10 2 5 8 4 0 8 0 3 4 7 5 6 10 0 9 7 2 1 1 10 1 7 0}. Expressing each element of cipher digital sequence into $4(= k)$ bits binary expression, we have {(1000) (0000) (0101) (0111) (0100) (0110) (1010) (0110) (1010) (0010) (0101) (1000) (0100) (0000) (1000) (0000) (0011) (0100) (0111) (0101) (0110) (1010) (0000) (1001) (0111) (0010) (0001) (0001) (1010) (0001) (0111) (0000)}. Which results the cipher binary string 1000000001010111010001101010011010100010010110000100000010000000001101000111010101101010000010010111001000010001101000010111000 0.

Splitting cipher binary string into sequence $\{s_n\}$ of binary substrings, each of size 6 bits, that is {(100000) (000101) (011101) (000110) (101001) (101010) (001001) (011000) (010000) (001000) (000000) (110100) (011101) (010110) (101000) (001001) (011100) (100001) (000110) (100001) (011100) (000000)}. By translating it into a radix-64 representation we have cipher text ***gFdGpqJYQIA0dWoJchGhcA==*** [3] corresponding to plain text SUPER CIPHER. Decryption of cipher text in reverse order with the symmetric key p and irreducible polynomial $a(x) = x^4 + 3x^2 + 10$ over the finite field $GF(11)$.

7. CONCLUSION AND FUTURE WORK

Algebraic Structure of Finite field is utilized in multi directions. Proposed cryptosystem strongly extracts properties of finite field in new direction. Security of data purely depends on the value of prime p and degree of key polynomial in this cryptosystem. Since proposed method is designed in multi stage security which provides high level security in data security and information system. The important feature of proposed cryptosystem is that it can adobe the part of AES method in any of three stages where binary string formed. In future, comparison of proposed technique with famous exiting cryptosystem will be studied. And the work will be carried to develop the cryptosystems with the properties of NSPPL.

Acknowledgement

The author is deeply indebted to the Management, Sri Ganesh college of Engineering and Technology, Pondicherry for allowing to do research work in the field of Mathematics. Author is very much grateful to Dr. S. Rajasekaran, Head, Department of Mathematics & Actuarial Sciences, B. S. Abdur Rahman Crescent Institute of Science & Technology, Chennai for the valuable suggestions and encouragement. Author is also takes this opportunity to express sincere thanks to R. Dhanalakshmi, Manager, Agriculture market committee, Cuddalore for the financial support.

REFERENCE

[1] Prof. Mukund, R.Joshi, Renuka Avinash Karkade, *"Network Security with Cryptography"*, International Journal of Computer Science and Mobile Computing, Vol.4, pp.201-204, (**2015).**

[2] Sindhu J Kumaar, P. J Abisha, D. G. Thomas, Nor Haniza Sarmin, K. G. Subramaniam, *"Languages defined by pure patterns"*, International journal of applied mathematics and computer intelligence, vol.2, pp.195-203, (**2013**).

[3] Ramachandran S, Dr. Sindhu J Kumaar, Dr. Jayakumar C V, *" Embedded Cryptosystem in Analitical Geometry"*, Gis Science Journal, Vol.7, pp.60-65, (**2020**).

[4] Krishna Kumar Pandey, Vigas Rangari, Siresh Kumar Sinha, "An Enhanced Symmetric Key Cryptography algorithm Improve Data Security", International Journal of Computer Application, Vol.74, pp.29-33, (**2013**).

[5] Ramachandran S, Dr.Sindhu J Kumaar, Dr. Jayakumar C V, " Application of Cryptosystem Using NSPP"L, Bulletin Monumental Journal, Vol.21, pp 31-36, (**2020**)

[6] Atul Kahate, *"Cryptography and Network Security"*, Mc Graw Hill Education (India) Private Limited, (**2013**).

[7] I. N. Herstein, *"Topics in Algebra"*, pp.207-256, pp.356-371, JOHN WILEY SONS, New York (**2007**).