MODIFIED HILL- CIPHER AND CRT METHODS IN GALOIS FIELD GF(2^M) FOR CRYPTOGRAPHY

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Technology

in

Telematics and Signal Processing

By

JYOTIRMAYEE   MAJHI

207EC114

Department of Electronics and Communication Engineering

National Institute Of Technology

Rourkela

2007-2009

MODIFIED HILL- CIPHER AND CRT METHODS IN GALOIS FIELD GF(2^M) FOR CRYPTOGRAPHY

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Technology

in

Telematics and Signal Processing

By

JYOTIRMAYEE   MAJHI

207EC114

Under the Guidance of

Prof. G. S. RATH

Department of Electronics and Communication Engineering

National Institute Of Technology

Rourkela

2007-2009

NATIONAL INSTITUTE OF TECHNOLOGY
ROURKELA

CERTIFICATE

This is to certify that the thesis titled " **Modified Hill -Cipher and CRT Methods in Galois Field gf(2^m) for cryptography"** submitted by Miss. **Jyotirmayee majhi** in partial fulfillment of the requirements for the award of Master of Technology degree **Electronics & Communication Engineering** with specialization in "**Telematics and Signal Processing**" during session 2008-2009 at National Institute Of Technology, Rourkela (Deemed University) is an authentic work by him under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other university / institute for the award of any Degree or Diploma.

Date:

Prof. G. S.RATH

Dept. of E.C.E

National Institute of Technology

Rourkela-769008

Email: gsrath@nitrkl.ac.in

Acknowledgement

I would like to express my gratitude to my thesis guide **Prof. G. S. Rath** for his guidance, advice and constant support throughout my thesis work. I would like to thank him for being my advisor here at National Institute of Technology, Rourkela.

Next, I want to express my respects to **Prof. G. Panda, Prof. K. K. Mahapatra, Prof. S.K. Patra , Dr. S. Meher , Prof. S. k. Behera , Prof Poonam singh , Prof. U. C. Pati , Prof P. k. Sahoo and Prof D. P. Acharya** for teaching me and also helping me how to learn. They have been great sources of inspiration to me and I thank them from the bottom of my heart.

I would like to thank all faculty members and staff of the Department of Electronics and Communication Engineering, N.I.T. Rourkela for their generous help in various ways for the completion of this thesis.

I would also like to mention the names of **Vikas Baghel, Pyarimohan Pradhan and Naresh kumar koppala** for helping me a lot during the thesis period.

I would like to thank all my friends and especially my classmates for all the thoughtful and mind stimulating discussions we had, which prompted us to think beyond the obvious. I've enjoyed their companionship so much during my stay at NIT, Rourkela.

I am especially indebted to my parents for their love, sacrifice, and support. They are my first teachers after I came to this world and have set great examples for me about how to live, study, and work.

Jyotirmayee Majhi

Roll No: 207ec114

Dept of ECE, NIT, Rourkela

Contents

ABSTRACT

Security can only be as strong as the weakest link. In this world of Cryptography, it is now well established, that the weakest link lies in the implementation of cryptographic algorithms. Galois field is extensively used in coding. Recently Galois field particularly $GF(2^m)$ has been used for Cryptography. Hill-cipher is an old symmetric key Technique of Cryptography. In this project, a novel method of Hill-cipher has been introduced in Cryptography. This new type of cipher matrix utilizes. The polynomials as element in $GF(2^m)$. Simulation and results confirm the utility such a data security in a private network. In addition to this, encryption and decryption of data are implemented in $GF(2^m)$ using the principle of data Chinese Remainder Theorem.

List of Figures

List of Tables

List of symbol

CHAPTER - 1

1.1 Introduction

In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed needed to store the information securely. This, in turn, led to a heightened awareness to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks.[1] cryptography, the science of encryption, plays a central role in mobile phone communications, pay-tv, e-commerce, sending private emails, transmitting financial information, security of ATM cards, computer passwords, electronic commerce digital signature and touches on many aspects of our daily lives . Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message (plaintext) into one that is unintelligible (cipher text) and then retransforming that message back to its original form .In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering.

Although in the past cryptography referred only to the encryption and decryption of message using secret keys. Nowadays, cryptography generally classified into two categories, the symmetric and asymmetric. Conventional Encryption is referred to as symmetric encryption or single key encryption. The Hill cipher algorithm in Galois field GF(2^m)using polynomial is one of the symmetric key algorithms that have several advantages in data encryption. Galois field is used for one of error detecting code. But, the inverse of the key matrix used for decrypting of the cipher text does not always exist. If the key matrix is not invertible, then encrypted text cannot be decrypted. In the Self-invertible matrix generation method, the key matrix used for the encryption is self invertible. So, at the time of decryption we need not find the inverse of the key matrix.

In this thesis a modified method of Hill -cipher is developed by the principle of exponentiation operation on plain text in GF(2^m) polynomial form. In these method minimal polynomials is used in decryption to find out the original cipher -text. Minimal polynomial is one that the original polynomial will become one after some repeated multiplication by itself. In Cipher text-only cryptanalysis of this method is very difficult.

In the 3rd part of the thesis another method of Chinese Remainder Theorem in Galois field has been developed. Minimal polynomial are the basic part of this algorithm. This

algorithm is an asymmetric key cryptography. In asymmetric key cryptography there two key present, one is private key another one is public key. The security of the RSA cryptosystem is based on the widely believed difficulty of factoring large number. One of the useful features of the Chinese remainder theorem is that it provides a way to manipulate (potentially very large) numbers mod N in terms of tuples of smaller numbers. This can be useful when N is 150 digits or more. However, it is necessary to know beforehand the factorization of N.

1.2 Objectives

There are so many algorithms present to encrypt and decrypt the data for security purpose in cryptography. Hill cipher method is one of the monoalphabetic polygraphic substitution ciphers. The mathematician LESTER HILL in1929 first developed the Hill- cipher algorithm. But till now no one had done the Hill cipher method in Galois field using polynomial. In this algorithm, Galois is field is used to increase the speed of encryption in Hill cipher method. Also to avoid the wastage of bit pattern and for implementation efficiency, Galois field (2^m) is used. In novel modified hill cipher method an exponential polynomial is used which is quite robust as for as cryptanalysis is concerned. But it has some mathematical complexity to find exponential. The Chinese remainder theorem (CRT) allows for an efficient and faster algorithms for implementation of the RSA algorithm.CRT avoids the complexity of the RSA decryption $M = C^D \ mod \ N$, where D specifies the modular multiplications necessary to perform the exponentiation and N determines the size of the intermediate results. The objective of this algorithm is that to reduce the size of both D & N for that it increases the speed of the algorithm.

1.3 Layout of the Thesis

The remainder of the thesis is organized as follows. Chapter II gives a brief review literature. It also presents the recent developments of Hill cipher, R/B conversion, mathematical operation in Galois field & CRT theorem. Chapter III presents all the theorems and algorithms that are used in this thesis. Chapter IV contains the description of my whole project work i.e, modified Hill- cipher method in Galois field GF(2^m). A novel modified Hill- cipher method based on exponentiation value in GF(2^m) and Modified CRT method in Galois field.

Simulation result for both for Hill cipher method and Modified CRT method using in Galois field are present in chapter V. Last but not the least chapter 6 contents the conclusion, application and future work.

CHAPTER - 2

This chapter gives a review of existing literature about Hill cipher and CRT method. A small overview about Galois field and Meressen prime number in cryptography.

2.1 Cryptography

Cryptography, a word with Greek origins, means" secret writing". Crypto is secret and grapy is writing .Cryptography is the science of using mathematics to transform the contents of information in secure mode and also immunes to attack. . Some of the common terms that are used in cryptosystems are explained here. The original message is called as the **Plaintext**. The disguised message is called as the **Cipher text**. The method of producing cipher text from plaintext using the key is called as **Encryption.** The reverse procedure of producing the plaintext from cipher text using the key is called as **Decryption** [3]. The science of breaking cryptosystems is called the **Cryptanalysis.** Cryptanalysis plays an important role in the cryptography because; it attacks the encoded message to produce the relevant plaintext.

Virtually all encryption algorithms, both symmetric and public key, involve arithmetic operations on integers. For convenience and for implementation efficiency, Galois field is one that fit exactly into a given number of bits, with no wasted bit patterns. The high complexity of the arithmetic operations that are performed in these algorithms makes formal verification [4] of such circuits of utmost necessity. Galois field architectures are represented using modulo-2 sum-of products (SOP) canonical form and are thus better expressed. In this paper, an isomorphism property between GF(2^m) and $GF(2^m)^p$, where $m = np$ is used which decrease the time.

The technique that is proposed in [5] is briefly stated here.

Step 1) Simplify a given Galois field expression using well-known mathematical theorems in Galois field.

Step 2)

    a. Transform the expressions into SOP form.

    b. Evaluate all multiplication using exponential representation of the Galois elements.

    c. Convert all elements in the expressions from exponential representation to vector representation of the elements.

d. Evaluate all addition over GF(2^m) using vector representation.

Lehmer's algorithm is used to calculate the multiplicative inverse based on extended Euclidean algorithm in Galois field. Extended Euclidean algorithm is derived from the ancient GCD method which is not suitable for higher order bit. This is primarily because a multi precision division operation is relatively expensive. Lehmer [6] observed that many of these division steps can be avoided. His idea was to extract the leading digits r^ and s^ of the inputs r and s, and run the Euclidean GCD algorithm on these single precision approximations of the inputs. In this electronics Letter we use this approach to develop a Lehmer's 'fast' Euclidean algorithm for computing multiplicative inverses in Galois fields GF(2^m).

Algorithm. Lehmer-Based Inversion in GF(2^m)

Input: a.

Output: $u = a^{-1}$.

1. $r = g;\ s = a;\ u = 0;\ v = 1;$

2. $while\ (degree(s \geq k)\ \{Lehmer\ step(r, s, u, v);\}$

3. $while\ (s \neq 0)\ \{Euclidean\ step(r, s, u, v);\}$

Lehmer step- Inputs and outputs: $r, s, u, v.$

1. $n = k\ \lceil degree(r) = kc \rceil;\ r^\char`^ = r >> n;\ s^\char`^ = s >> n;$

2. $If\ (s^\char`^ = 0)\ \{Euclidean\ step(r, s, u, v)\}$

3. $Else\ \{\alpha = [1, 0, r^\char`^];\ b¼\ [0, 1, s^\char`^]\};$

4. $While\ (\beta2 \neq 0\{q = \alpha2/\beta2;\ [\alpha, \beta] = [\beta, \alpha + q\ b];\}$

5. $[r, s] = [\alpha0r + \alpha1s, \beta0r + \beta1s];$

6. $[u, v] = [\alpha0u + \alpha1v, \beta0u + \beta1v];$

7. $If\ (degree(r) < degree(s))\ \{r \leftrightarrow s;\ u \leftrightarrow v;\}$

Euclidean step- Inputs and outputs: $r, s, u, v.$

1. $[q, p] = [r = s, r\ mod\ s\ ];\ [r, s] = [s, p];\ [u, v] = [v, u \leftrightarrow qv];$

Where $a(x) = am_1 x_{m1} + \ldots\ldots + a_1 x + a_0$ be the polynomial representation of an element of $gf(2^m)$ and $(a_{m1}, \ldots, a_1, a_0)$ its canonical basis representation. $G =$ generator matrix.

In classical cryptography, the **Hill -cipher** is a polygraphic substitution cipher based on linear algebra, in which it was practical (though barely) to operate on more than three symbols at once. Each letter is first encoded as a number. A block of n letters is then considered as a vector of n dimensions, and multiplied by a $n \times n$ matrix, modulo 26. The key size is the binary logarithm of the number of possible keys. There are 26^{n^2} matrices of dimension $n \times n$. Thus $\log_2(26^{n^2})$ or about $4.7n^2$ is an upper bound on the key size of the Hill -cipher using $n \times n$ matrices. This is only an upper bound because not every matrix is invertible and thus usable as a key. The number of invertible matrices can be computed via the Chinese Remainder Theorem. i.e., a matrix is invertible modulo 26 if and only if it is invertible both $modulo\ 2$ and $modulo\ 13$. The number of invertible $n \times n$ matrices modulo 2 is equal to the order of the general linear group GF (n, Z^2) [7].

The hallmark of conventional encryption is that the cipher or key to the algorithm is shared, i.e., known by the parties involved in the secured communication. Substitution Cipher is one of the basic components of classical ciphers. A substitution cipher is a method of encryption by which units of plaintext are substituted with cipher text according to a regular system; the units may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution [3]. The units of the plaintext are retained in the same sequence in the cipher text, but the units themselves are altered. There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different times in the message— such as with homophones, where a unit from the plaintext is mapped to one of several possibilities in the cipher text. Hill cipher is a type of monoalphabetic polygraphic substitution cipher.

In the improved version of the hill cipher, a randomly generated non-singular matrix is used as encryption key, and the inverse of the matrix is used as the decryption key. But the inverse of the matrix is always not present which will make difficult in decryptions. The self invertible matrix of encryption key is created to overcome this drawback. In the self-invertible matrix generation method, the matrix used for the encryption is itself self-invertible. Moreover, this method eliminates the computational complexity involved in finding inverse of the matrix while decryption [8].

Matrix cryptosystem, like Hill cipher, are resistant to frequency analysis. The key is a non singular matrix, for example 3×3 matrix k . A modular non-singular key-matrix for matrix ciphers can be generated and these results are applied to cryptography and computer security. For example a mutual authentication protocol based on Hamiltonian cycle in directed weight graphs and modular matrix algebra has been purposed.

The residue-to-binary (R/B) conversion is the crucial step for any successful RNS application. The traditional technique of the (R/B) conversion is based on the Chinese Remainder Theorem (CRT). This method has a disadvantage of requiring a $modulo\ M$ operation, where the dynamic range M is a large-valued integer. The dynamic range of multiple integers that can be uniquely determined from their residue sets [9]. Recently, some new general R/B conversion algorithms, the New Chinese Remainder Theorems have been introduced, based on three conjunctive module, which improve the CRT in many aspects. These three conjunctive module sets, the converters based on the New CRT-I are consistently faster while requiring less hardware, compared to the previous residue-to-binary converters which are designed based on the traditional Chinese Remainder Theorem [10].

The two most important considerations when designing RNS systems are the choices of the module sets and the conversion from the residue to the weighted binary system. The Residue Number System (RNS) is an integer system capable of supporting parallel, carry-free, high-speed arithmetic. An important area of application of the RNS is Digital Signal Processing (DSP) whose Intensive computations such as digital filtering, convolutions, correlation, DFT and FFT are required.

CRT has various generalizations. A different generalization of CRT has recently purposed in, where (instead of single integer in CRT) multiple integers need to be determined from (not a sequence of remainders) but a sequence of sets, residue sets, of remainders. A

residue set consists of the remainders of multiple integers modulo. A modulus integer, the residue set and the multiple integers is not specified. The generalized CRT was motivated from the determination of multiple frequencies in super positioned signal of multiple sinusoids from its multiple under sample wave forms. As like as sensor network, the multiple sensors have low power and low transmission rates, and their sampling rates may be low and much lower than nyquist rate of a signal of interest in the field. CRT can also apply in multiple frequency determination from multiple under sampled waveforms, such as, from low functionality sensors.

In Chinese Remainder Theorem, if a codeword is corrupted in (2) coordinates, then there exists a unique integer whose corresponding codeword differs from the corrupted word in at most places. Furthermore, Mandelbaum shows how can be recovered efficiently given the corrupted word provided that these are very close to one another.[CRT10]. Many emerging network applications are based upon group communication models and are implemented with multicast communications. In a pair of key management schemes, the session key is distributed mathematically based upon the Euler-Fermat Theorem, such that upon receiving the broadcast keying material known as the rekey message, each member in the privileged multicast group can derive with a modular operation this group oriented common shared secret. The Chinese Remainder Theorem, present some unusual analysis results concerning the two novel rekey schemes. Both schemes are revealed to have failed to effectively protect the multicast session key[CRT11].

CHAPTER -3

3.1 Definition of Cryptography

"*Cryptography is the science of using mathematics to transform the contents of information in secure mode and also immunes to attack*".

3.2 Cryptographic Goals

However, there are other natural cryptographic problems to be solved and they can be equally if not more important depending on who is attacking you and what you are trying to secure against attackers. The cryptographic goals covered in this text (in order of appearance) are privacy, integrity, authentication, and no repudiation.
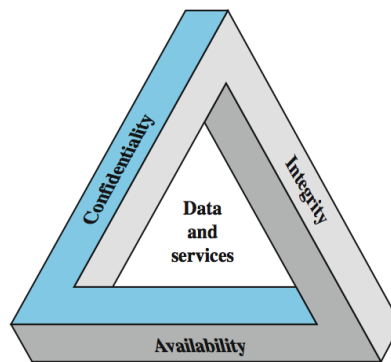
Fig. 1

These three concepts form what is often referred to as the **CIA triad**. The three concepts embody the fundamental security objectives for both data and for information and computing services. FIPS PUB 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are:

- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

Generally there are two types key present

1. Symmetric-key
2. Asymmetric-key

3.3 Symmetric key encryption

The universal technique for providing confidentiality for transmitted data is symmetric encryption. Symmetric encryption also referred to as conventional encryption or single-key encryption was the only type of encryption in use prior to the introduction of public-key encryption in the late 1970s. Countless individuals and groups, from Julius Caesar to the German U-boat force to present-day diplomatic, military, and commercial users, use symmetric encryption for secret communication. It remains by far the more widely used of the two types of encryption.

A symmetric encryption scheme has five ingredients

- **Plaintext:** This is the original message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
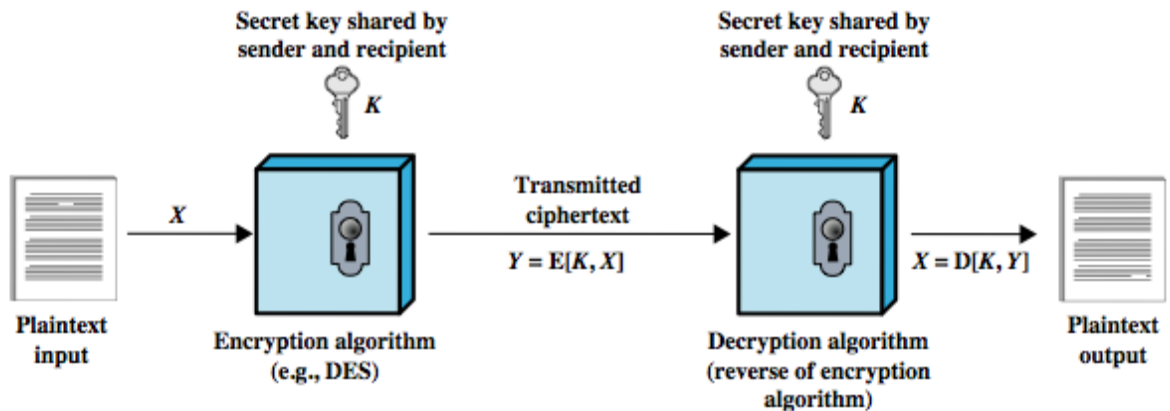
Fig. 2 Symmetric key encryption

- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.

- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

There are two requirements for secure use of symmetric encryption:

1. We need a strong encryption algorithm.

2. Sender and receiver must have secured obtained, & keep secure, the secret key.

3.4 Symmetric-key vs. Public-key Cryptography

Symmetric-key and public-key encryption schemes have various advantages and disadvantages, some of which are common to both. This section highlights a number of these and summarizes features pointed out in previous sections.

3.4.1 Advantages of symmetric-key cryptography

1. Symmetric-key ciphers can be designed to have high rates of data throughput. Some hardware implementations achieve encrypts rates of hundreds of megabytes per second,

while software implementations may attain throughput rates in the megabytes per second range.

2. Keys for symmetric-key ciphers are relatively short.

3. Symmetric-key ciphers can be employed as primitives to construct various cryptographic mechanisms including pseudorandom number generators, hash functions, and computationally efficient digital signature schemes, to name just a few.

4. Symmetric-key ciphers can be composed to produce stronger ciphers. Simple transformations which are easy to analyze, but on their own weak, can be used to construct strong product ciphers.

5. Symmetric-key encryption is perceived to have an extensive history, although it must be acknowledged that, notwithstanding the invention of rotor machines earlier, much of the knowledge in this area has been acquired subsequent to the invention of the digital computer, and, in particular, the design of the Data Encryption Standard in the early 1970s.

3.4.2 Disadvantages of symmetric-key cryptography

1. In a two-party communication, the key must remain secret at both ends.

2. In a large network, there are many key pairs to be managed. Consequently, effective key management requires the use of an unconditionally trusted TTP.

3. In a two-party communication between entities A and B, sound cryptographic practice dictates that the key be changed frequently and perhaps for each communication session.

4. Digital signature mechanisms arising from symmetric-key encryption typically require either large keys for the public verification function or the use of a TTP.

3.4.3 Advantages of public-key cryptography

1. Only the private key must be kept secret (authenticity of public keys must, however, be guaranteed).

2. The administration of keys on a network requires the presence of only a functionally trusted TTP as opposed to an unconditionally trusted TTP. Depending on the mode of usage, the TTP might only be required in an "off-line" manner, as opposed to in real time.

3. Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable periods of time, e.g., many sessions (even several years).

4. Many public-key schemes yield relatively efficient digital signature mechanisms. The key used to describe the public verification function is typically much smaller than for the symmetric-key counterpart.

5. In a large network, the number of keys necessary may be considerably smaller than in the symmetric-key scenario.

3.4.4 Disadvantages of public-key encryption

1. Throughput rates for the most popular public-key encryption methods are several orders of magnitude slower than the best known symmetric-key schemes.

2. Key sizes are typically much larger than those required for symmetric-key encryption, and the size of public-key signatures is larger than that of tags providing data origin authentication from symmetric-key techniques.

3. No public-key scheme has been proven to be secure (the same can be said for block ciphers). The most effective public-key encryption schemes found to date have their security based on the presumed difficulty of a small set of number-theoretic problems.

4. Public-key cryptography does not have as extensive a history as symmetric-key encryption, being discovered only in the mid 1970.

3.5 Number Theory

Number theory is the branch of pure mathematics concerned with the properties of numbers in general, and integers in particular which is essential in the design of cryptographic algorithms. Number theory may be subdivided into several fields, according to the methods used. This chapter provides an overview of the concepts along with the proofs of the theorems used in these algorithms. The various theorem have been elucidated which are further applied in Hill cipher and CRT in my work.

3.6 Modular Arithmetic

      Modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" after they reach a certain value—the modulus. The analysis presented here for generation of self repetitive matrix is valid for matrix of positive integers that are the residues of modulo arithmetic on a prime number. So in analysis the arithmetic operations presented here are addition, subtraction, Unary operation, Multiplication and division.

SR. No.	Property	Expression
1.	Commutative Law	$(w + x) \bmod p = (x + w) \bmod p$ $(w * x) \bmod p = (x * w) \bmod p$
2.	Associative Law	$[(w + x) + y] \bmod p = [w + (x + y)] \bmod p$
3.	Distributive Law	$[w * (x + y)] \bmod p = [w * x + w * y] \bmod p$ $[w * (x * y)] \bmod p = [\{w * x \bmod p\} * \{(w * y) \bmod p\}] \bmod p$
4.	Identities	$(0 + a) \bmod p = a \bmod p$ $and\ (1 * a) \bmod p = a \bmod p$
5.	Inverse	$For\ each\ X\ belongs\ to\ Zp\ ,there\ exists\ y\ such\ that$ $(x + y) \bmod p = 0\ then\ y = -x$ $For\ each\ X\ belongs\ to\ Zp, there\ exists\ y\ such\ that\ (x * y) \bmod p = 1$

Table-1 exhibits the properties of modulo arithmetic

The Modulo operator have the following properties:

1. $a = b \bmod p\ if\ n|\ (a - b)$

2. $(a \bmod p) = (b \bmod p) => a = b \bmod p$

3. $a = b \bmod p => b = a \bmod p$

4. $a = b \bmod p$ and $b = a \bmod p => a = c \bmod p$

The modulo arithmetic have the following properties:

Let $z = [0, 1, \ldots, p-1]$, the set residues modulo p. If modular arithmetic is performed within the set Z_n, the following equations present the arithmetic identities:

1. Addition: $(a+b) \bmod p = [(a \bmod p) + (b \bmod p)] \bmod p$

2. Subtraction: $(a-b) \bmod p = [(a \bmod p) - (b \bmod p)] \bmod p$

3. Multiplication: $(a*b) \bmod p = [(a \bmod p) * (b \bmod p)] \bmod p$

4. Negation: $-a \bmod p = p - (a \bmod p)$

5. Division: $(a/b) \bmod P = c$ when $a = (c*b) \bmod p$

6. Multiplicative inverse: $(a^{-1}) = c$ if there exists $(c*z) \bmod p = 1$

3.7 Galois Field

The arithmetic operations in the Galois field have several applications in coding theory, Computer algebra and cryptography. Galois field is the set of all positive integer from $0, 1 \ldots \ldots (P - 1)$ where P is a prime number .It is denoted by $GF(P^M)$ where m is any positive value. Many devices that perform functions such as error-control encoding, error detection, and error correction, operate by performing Galois field arithmetic over $GF(PM)$. In practice, most implementations take $p = 2$ and use binary digits (bits) to represent elements from the field. Performing Galois field arithmetic operations over $GF(P^M)$ requires addition and multiplication $modulo\ p$. With $p = 2$, addition and multiplication modulo 2 become the exclusive-OR and logical-AND function, respectively. For this reason, and the ease with which a symbol of size 2^mmay be handled in a binary system [e.g., a single byte may be represented as an element from $gf(2^8)$. Galois fields of size 2^m are widely used.

Virtually all encryption algorithms, both symmetric and public key, involve arithmetic operations on integers. If one of the operations that are used in the algorithm is division, then we need to work in arithmetic defined over a field. For convenience and for implementation efficiency, we would also like to work with integers that fit exactly into a given number of bits,

with no wasted bit patterns. That is, we wish to work with integers in the range 0 through $2^n - 1$, which fit into an n-bit word.

Suppose we wish to define a conventional encryption algorithm that operates on data 8 bits at a time and we wish to perform division. With 8 bits, we can represent integers in the range 0 through 255. However, 256 is not a prime number, so that if arithmetic is performed in Z_{256} (arithmetic modulo 256), this set of integers will not be a field. The closest prime number less than 256 is 251. Thus, the set Z_{251}, using arithmetic modulo 251, is a field. However, in this case the 8-bit patterns representing the integers 251 through 255 would not be used, resulting in inefficient use of storage.

To summarize, we are looking for a set consisting of 2^n elements, together with a definition of addition and multiplication over the set that define a field. We can assign a unique integer in the range 0 through $2^n - 1$ to each element of the set. Keep in mind that we will not use modular arithmetic, as we have seen that this does not result in a field. Instead, we will show how polynomial arithmetic provides a means for constructing the desired field. It obeys all   the properties of Modular Arithmetic.

An example of a $GF(2^2)$ Field:

	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Table-2 Addition & Multiplication

3.8 Irreducible Polynomials

A polynomial of degree n is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots \ldots \ldots \ldots \ldots + a_0 x^n$$

Before defining the operation on polynomials, it is required to know about the modulus polynomials. Addition of two polynomials never creates a polynomial out of the set. However, multiplication of two polynomials may create a polynomial with a degree more than n. This means it needs to divide the result by a modulus keep only the remainder. For the set of polynomials $GF(P^M)$ a group of polynomials of degree M is defined as the modulus. The

modulus in this case acts as a prime polynomial, which means that no polynomial in the set can divide this polynomial with degree less than n. Such polynomials are referred to as Irreducible polynomials.

For each, there is often more than one irreducible polynomial, which means when we define our $GF(P^M)$ we need to declare which irreducible polynomial we are using as the

modulus.

3.9 Primitive Polynomial

Primitive polynomial is an irreducible polynomial that divides $x^e + 1$, where e is least

integer in the form of $e = 2^k - 1$ and $k \geq 2$. It is not easy to generate a primitive polynomial.

This means that a primitive polynomial is necessarily an irreducible polynomial, but an irreducible polynomial is not necessarily a primitive polynomial.

3.10 Modular Polynomial Arithmetic

Consider the set S of all polynomials of degree $n - 1$ or less over the field Z_p. Thus,

each polynomial has the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots \ldots \ldots \ldots \ldots + a_0 x^n$$

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots \ldots \ldots \ldots \ldots \ldots \ldots \ldots + b_0 x^n$$

$$f(x) + g(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots \ldots \ldots \ldots \ldots \ldots + c_0 x^n$$

where $a_{i\varepsilon} \in (0,1),\ b_i \in (0,1),\ c_i \in (0,1)$

We have seen that addition of polynomials is performed by adding corresponding coefficients, and, in the case of polynomials over Z^2 addition is just the XOR operation. So, addition of two polynomials in $GF(2^N)$ corresponds to a bitwise XOR operation.

With the appropriate definition of arithmetic operations, each such set S is a finite field. The definition consists of the following elements:

1. Arithmetic follows the ordinary rules of polynomial arithmetic using the basic rules of algebra, with the following two refinements.
2. Arithmetic on the coefficients is performed modulo p. That is, we use the rules of arithmetic for the finite field Z_p.

3. If multiplication results in a polynomial of degree greater than $n-1$, then the polynomial is reduced modulo some irreducible polynomial $m(x)$ of degree n. That is, we divide by $m(x)$ and keep the remainder. For a polynomial $f(x)$, the remainder is expressed as $r(x) = f(x) \bmod m(x)$. Subtraction is done by addition of additive inverse.

3.11 Multiplication

21

Multiplication in polynomials is the sum of the multiplication of the each term of the 1st polynomial with each term of the 2nd polynomial.

1. The coefficient multiplication is done in GF(2^N)
2. The multiplying x^i by x^j results in x^{i+j}.

3. The multiplication may create terms with degree more than $n - 1$, which means results

    needs to reduced using a modulus polynomial.

Example: The Advanced Encryption Standard (AES) uses arithmetic in the finite field GF(2^8) with the irreducible polynomial $m(x) = x^8 + x^4 x^3 + x + 1$. Consider the two polynomials

$f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$. Then

$f(x) * g(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$

$f(x) * g(x) \bmod m(x) = x^7 + x^6 + 1$.

3.12 Division

The division of a polynomial is done like the ordinary division of polynomial but the coefficient are obey the GF(2). We have shown that the elements of GF(2^N) can be defined as the set of all polynomials of degree $n - 1$ or less with binary coefficients. Each such polynomial can be represented by a unique n-bit value. Arithmetic is defined as polynomial arithmetic modulo some irreducible polynomial of degree n.

3.13 Multiplicative Inverse

Just as the Euclidean algorithm can be adapted to find the greatest common divisor of two polynomials, the extended Euclidean algorithm can be adapted to find the multiplicative inverse of a polynomial. Specifically, the algorithm will find the multiplicative inverse of $b(x) \ modulo \ m(x)$ if the degree of $b(x)$ is less than the degree of $m(x)$ and $gcd[m(x), b(x)] = 1$. If $m(x)$ is an irreducible polynomial, then it has no factor other than itself or 1, so that $gcd[m(x), b(x)] = 1$. The algorithm is as follows:

Extended Euclid $[m(x), b(x)]$

1. $[a_1(x), a_2(x), a_3(x)] \quad [1, 0, m(x)]$;

   $[b_1(x), b_2(x), \ b_3(x)] \quad [0, 1, b(x)]$;

2. $if \ b_3(x) = 0 \ return \ a_3(x) = gcd[m(x), b(x)]$;

   $no \quad , \ Inverse$

3. $if \ b_3(x) = 1 \ return \ b3(x) = gcd[m(x), b(x)]$;

4. $b_2(x) = b_1(x) mod \ m(x)$

   $q(x) = quotient \left(\dfrac{a_3(x)}{b_3(x)} \right)$

5. $[t_1(x), t_2(x), t_3(x)] \quad [a_1(x) \ q(x)b_1(x), a_2(x)q(x)b_2(x), a_3(x)q(x)b_3(x)]$

6. $[a1(x), a2(x), a3(x)] \quad [b1(x), b2(x), b3(x)]$

7. $[b1(x), b2(x), b3(x)] \quad [t1(x), t2(x), t3(x)]$

8. goto 2

Although the Euler-Fermat Theorem is a well-studied component of the number theory and has contributed a lot to the cryptology, it should never be employed in a naive manner as observed in [13] [14].

3.14   Exponentiation

In cryptography, a common modular operation is exponentiation .That is, we often need to calculate

$$y = a^x \ mod \ n$$

This exponentiation is mostly required for both encryption and decryption in RSA cryptosystem with very large exponentiation. With the use of this exponentiation we purposed one Hill cipher method. It is very difficult to find out when it is very large. So there are two methods present to calculate the exponentiation of higher order.

3.15   Fast Exponentiation

Fast exponentiation is possible using the square-and-multiple method. In traditional algorithms only multiplication is used to simulate exponentiation but in fast exponentiation algorithm uses both squaring and multiplication. The main idea behind this method is to treat the exponent as a binary number n_b bits ($x_0 \ to \ x_{n_b -1}$).for example $x = 22 = [10110]$. In general

$$x = x_{n_h -1} \times 2^{k-1} + x_{n_h -2} \times 2^{k-2} + x_0 \times 2^0$$

Algorithm:

Square-and-multiply (a, x, n)

{

$Y \leftarrow 1$

  $For \ (I \leftarrow 0 \ to \ n_b - 1)$ //n_b is the number of bits in x

  {

     If $(x_i = 1)$ $\ y \leftarrow a \times y \ mod \ n$ //multiply only if the bit is 1

       $A \leftarrow a^2 \ mod \ n$

  }

$Return \ y$

}

i	x_i	Multiplication (Initialization $y = 1$)		Squaring (initialization: $a = 17$)
0	0	$\rightarrow$		$a = 17^2 mod\ 21 = 16$
1	1	$Y = 1 \times 16\ mod\ 21 = 16$	$\rightarrow$	$a = 16^2 mod\ 21 = 4$
2	1	$Y = 16 \times 4 mod\ 21 = 1$	$\rightarrow$	$a = 4^2 mod\ 21 = 16$
3	0	$\rightarrow$		$a = 16^2 mod\ 21 = 4$
4	1	$Y = 1 \times 4 mod\ 21 = 4$	$\rightarrow$	

Table-3: Calculation of $17^{22}\ mod\ 21$

3.16 Minimal Value Of Polynomial

Minimal value of a polynomial is one that the exponent power of the polynomial in Galois field at which the result will be 1 which means the original polynomial will become one after some repeated multiplication by itself. In mathematics, a Mersenne number is a positive integer that is one less than a power of two:

$$M_n = 2^n - 1$$

where n is the degree of the primitive polynomial.

In case of primitive polynomial it satisfies the above condition. But in case of irreducible polynomial it does not satisfy the condition. Minimal values of irreducible polynomials are the factor of minimal value of the primitive polynomial.(3).

Some examples are given in table which contains all the primitive polynomials and irreducible polynomials with respected minimal value. The star marks are not the primitive polynomial.

m	Primitive Polynomial	Minimal value
2	$x^2 + x + 1$	3
3	$x^3 + x + 1$	7
	$x^3 + x^2 + 1$	7
4	$x^4 + x + 1$	15
	$x^4 + x^3 + 1$	15
	$x^4 + x^3 + x^2 + x + 1(*)$	15(*)
5	$x^5 + x^2 + 1$	31
	$x^5 + x^3 + 1$	31
	$x^5 + x^3 + x^2 + x + 1$	31
	$x^5 + x^4 + x^2 + x + 1$	31
	$x^5 + x^4 + x^3 + x + 1$	31
	$x^5 + x^4 + x^3 + x^2 + 1$	31
6	$x^6 + x + 1$	63
	$x^6 + x^4 + x^3 + x + 1$	63
	$x^6 + x^5 + 1$	63
	$x^6 + x^5 + x^2 + x + 1$	63
	$x^6 + x^5 + x^3 + x^2 + 1$	63
	$x^6 + x^5 + x^4 + x + 1$	63
	$x^6 + x^2 + 1(*)$	14(*)
7	$x^7 + x + 1$	127
	$x^7 + x^3 + 1$	127
	$x^7 + x^3 + x^2 + x + 1$	127
	$x^7 + x^4 + 1$	127
	$x^7 + x^4 + x^3 + x^2 + 1$	127
	$x^7 + x^5 + x^2 + x + 1$	127
	$x^7 + x^5 + x^3 + x + 1$	127
	$x^7 + x^5 + x^4 + x^3 + 1$	127
	$x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$	127
	$x^7 + x^6 + 1$	127
	$x^7 + x^6 + x^3 + x + 1$	127
	$x^7 + x^6 + x^4 + x^2 + 1$	127
	$x^7 + x^6 + x^5 + x^2 + 1$	127
	$x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$	127
	$x^7 + x^6 + x^5 + x^4 + 1$	127
	$x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$	127
	$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$	127

Table - 4: List of primitive value and corresponding minimal value

3.17 Hill Cipher Encryption

The Hill cipher, developed by the mathematician Lester Hill in 1929. The encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters. The substitution is determined by m linear equations in which each character is assigned a numerical value $(a = 0, b = 1 \dots z = 25)$. Core of hill cipher is matrix manipulation. For $m = 3$, the system can be described as follows:

$$C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26$$
$$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26$$
$$C_3 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26$$

This can be expressed in terms of column vectors and matrices:

$$C = KP$$

where C and P are column vectors of length 3, representing the plaintext and the cipher text and K is a $3 * 3$ matrix, which is the encryption key. All operations are performed $\bmod 26$ here.

Decryption requires the inverse of matrix K. The inverse K-1 of a matrix K is defined by the equation.

$$K K^{-1} = I \text{ , where } I \text{ is the Identity matrix.}$$

NOTE: The inverse of a matrix doesn't always exist, but when it does it satisfies the proceeding equation.

K^{-1} is applied to the cipher text, and then the plain text is recovered. In general terms we can write as follows:

For encryption: $C = E\ k(P) = Kp$

For decryption: $P = D\ k(C) = K - 1C = K - 1Kp = P$

3.18   Traditional Chinese Remainder Theorem

The CRT is used to solve a set of congruate equation with one variable but different module which is relatively prime, means reconstruction of integers in a certain range of their residues modulo a set of pair wise relatively prime module.

27

The integers 0 through 9 in z_{10}, can be reconstructed from their two residues modulo 2 and 5 (the relative *prime factor of* 10).The known residues of a decimal digit $x \bmod 2 = 0$ and $X \bmod 5 = 3$.Therefore, x is an integer in z_{10} whose remainder on division by 5, is 3.The unique solution of $x = 8$.

Theorem 1:

Let m and n be integers with $gcd(m,n) = 1$, $M = mn$ and let b and c be any integers. Then simultaneous congruence's

$$X \equiv b \ (mod \ m \ ) \ and \ x \equiv c(mod \ n)$$

have a exactly one solution with $0 \leq x \leq M$

Proof:

We begin by solving the congruence's $x \equiv b \ (mod \ m \ )$.The solution consists of all numbers of the form $x = my + b$. We substitute this into second congruence, which yields $my \equiv c - b(mod \ n)$.

We are given that $gcd \ (m,n) = 1$, so the linear congruence theorem tells us that there is exactly one solution y_1 with $0 \leq y_1 < n$. Then the solution to the original is given by

$$x_1 = my_1 + b$$

This will be the only solution x_1 with $0 \leq x_1 < M$, since there is only y_1 between 0 and n, we multiply y_1 *by* m to get x_1.

Example:

For solution of three simultaneous congruence's

$$x \equiv 2(mod \ 3), \ x \equiv 2(mod \ 5), \ x \equiv 3(mod \ 7),$$

Solution:

Using the theorem, $M = 3 \times 5 \times 7 = 105$

Let $m_1 = 3, \ m_2 = 5$ and $m_3 = 7$;

Let $b_1 = 2, b_2 = 1, b_3 = 3$

The integers y_1, y_2, y_3 are found by congruence $\frac{M}{m_i} \ y_i \equiv (\ mod m_i)$

Thus we have $35y_1 \equiv 1(mod \ 3), \ 21y_2 \equiv 1(mod \ 5), \ 15y_3 \equiv 1(mod \ 7)$. So $y_1 = y_2 = y_3 = 1$ are possible values and

$$x = (35)(-1)(2) + (21)(1)(1) + (15)(1)(3) = (-4) \ mod \ 105 = 101.$$

This leads us define x as

$$x = \left(\sum_{i=1}^{a} \frac{M}{m_i} y_i b_i \right) (mod M)$$

Remarks: Notice that in the congruence's

$M/m_i \ y_i \equiv 1 \ (mod \ m_i)$, y_i is the multiplicative inverse of $\frac{M}{m_i}$ modulus m_i

3.19   Extension of the Theorem to Polynomials

When trying to extend the definition of CRT to polynomials we presented a problem of the following kind:

Example:

Find a polynomial that when it is divided by $(x-1)$ remainder is 3, when it is divided by $(x-2)$ remainder is 2, and when it is divided by $(x-3)$ remainder is -1.

Solution:

Using the theorem, we get $g(x) = (x-1)(x-2)(x-1)$ Notice that polynomial $p(x)$ can be a polynomial of degree at most 3.

Let $m_1 = (x-1), m_2 = (x-2), \ m_3 = (x-3).$

now let $b_1 = 3, b_2 = 2, b_3 = -1$

the polynomial y_1, y_2, y_3 (degree 0 in this particular case) are found by the congruence

$M/m_i \ y_i \equiv 1 \ (mod \ m_i),$

We now have $(x^2 - 5x + 6)y_1 \equiv 1[mod(x-1)]$

$$(x^2 - 4x + 3)y_2 \equiv 1[mod(x-2)]$$

$$(x^2 - 3x + 2)y_3 \equiv 1[mod(x-3)]$$

So $y_1 = \frac{1}{2}, y_2 = -1, y_3 = 1/2.$ are possible values and

$$p = (x-2)(x-3)\left(\frac{1}{2}\right)(3) + (x-1)(x-3)(-1)(2) + (x-1)(x-2)(-1)\left(\frac{1}{2}\right)$$

$$= -x^2 + 2x + 2$$

Thus in this way the theorem could be extended to polynomials as long as the module m_i are relatively prime to each other.

Theorem 2:

Let $m_1(x), m_2(x), m_3(x), \ldots \ldots \ldots \ldots , m_r(x),$ denote r prime polynomials of degree $p(p \geq 1)$ that are relatively prime in pairs, and let $b_1, b_2, b_3, \ldots \ldots \ldots \ldots , b_r,$ denote any r prime polynomials of degrees at most p-1.then the system of congruences

$x \equiv b_i \ (mod(m)_i\ (x)), \quad i = 1,2, \ldots \ldots \ldots \ldots \ldots r$ has a unique solution $modulo\ (x),$where

$$g(x) = \prod_{i=1}^{r} m_i\ (x)$$

Proof:

Let $g(x)$ denoted polynomial obtained by multiplying together all the $m_i(x)$, since $m_i(x)$ is a monic polynomial of degree one we can write it as $(x - a_1)$, where a_i is one of the x co-ordinate of our points. For each point (a_i, b_i) we can write expression $\dfrac{b_i}{g'(a_i)} * \dfrac{g(x)}{(x-a_i)}$

For which $\dfrac{g(x)}{(x-a_i)}$ is just $\dfrac{M}{m_i}$ and $\dfrac{1}{(g'\ a_i)}$ is the logarithm for finding y_i.We now have our familiar $x = \left(\sum_{i=1}^{a} \dfrac{M}{m_i} y_i b_i \right) (mod\ M)$ in the form of

$p(x) = \left(\sum_{i=1}^{a} \dfrac{g(x)}{(x-a_i)} \dfrac{b_i}{g'(a_i)} \right) (mod\ g(x))$ for polynomials. A note of remarkable importance is the fact that the algorithm for $p(x)$ is the familiar Lagrance interpolation formula found in numerical analysis.

CHAPTER 4

4.1 Hill Ciphers

Letter-by-letter substitution ciphers easily succumb to frequency analysis and so are notoriously unsecure. Polytrophic ciphers, by contrast, in which each list of n consecutive letters of the plaintext—an n-graph—is replaced by another n-graph according to some key, can be more challenging to break. The first systematic yet simple polygraphic ciphers using more than two letters per group are the Hill ciphers, first described by Lester Hill [4] in 1929. For a polygraphic substitution, changing just one or two plaintext letters can completely change the corresponding cipher text! That is one reason that Hill ciphers are so difficult to crack.

4.2 Traditional Hill Cipher

The Hill cipher algorithm takes m successive plaintext letters and substitute's m cipher text letters for them. The substitution is determined by m linear equations in which each character is assigned a numerical value $(a = 0, b = 1, \ldots, z = 25)$. Let m be a positive integer, the idea is to take m linear combinations of the m alphabetic characters in one plaintext element and produce m alphabetic characters in one cipher text element. Then, a $m \times m$ matrix A is used as a key of the system such that A is invertible modulo 26 [5]. Let a_{ij} be the entry of A. For the Plaintext block $(x_1, x_2, \ldots \ldots x_m)$ (the numerical equivalents of m letters) and a key matrix A, the corresponding cipher text block $(y_1, y_2, y_3 \ldots \ldots \ldots y_m)$ be computed as

Encryption

$$(y_1, y_2, y_3 \ldots \ldots \ldots y_m) = (x_1, x_2, \ldots \ldots \ldots x_m)(mod\ 26)$$

$$\text{where } A = \begin{bmatrix} a_{11} & a_{12} & \ldots \ldots \ldots \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots \ldots \ldots \ldots & a_{2m} \\ \ldots & \ldots & \ldots \ldots \ldots \ldots & \ldots \ldots \\ a_{m1} & a_{m2} & \ldots \ldots \ldots \ldots & a_{mm} \end{bmatrix}$$

The cipher text is obtained from the plaintext by means of a linear transformation.

Decryption

The reverse process, deciphering, is computed by

$$(x_1, x_2, \ldots \ldots \ldots x_m) = (y_1, y_2, y_3 \ldots \ldots \ldots y_m)^{-1}(mod\ 26)$$

Where $A^{-1} = \begin{bmatrix} a_{11} & a_{12} & \ldots\ldots\ldots\ldots & a_{1m} \\ a_{21} & a_{22} & \ldots\ldots\ldots\ldots & a_{2m} \\ \ldots. & \ldots. & \ldots\ldots\ldots\ldots. & \ldots\ldots. \\ a_{m1} & a_{m2} & \ldots\ldots\ldots\ldots & a_{mm} \end{bmatrix}^{-1} (mod26)$

Since the block length is m, there are 26^m different m letters blocks possible, each of them can be regarded as a letter in a 26^m - letter alphabet. Hill's method amounts to a monoalphabetic substitution on this alphabets [6].

We have not yet discussed one complication that exists in picking the encrypting matrix. Not all matrices have an inverse. The matrix will have an inverse if and only if its determinant is not zero, and does not have any common factors with the modular base. Thus, if we work $modulo\ 26$ as above, the determinant must be nonzero, and must not be divisible by 2 or 13. If the determinant is 0, or has common factors with the modular base, then the matrix cannot be used in the Hill cipher, and another matrix must be chosen (otherwise it will not be possible to decrypt). Fortunately, matrices which satisfy the conditions to be used in the Hill cipher are fairly common.

4.3 Modified Hill Cipher Method In Galois Field

This algorithm generates random key matrix each block encryption instead of keeping the key matrix constant in Galois field. So it increases secrecy of the data. As Galois field is on of the error detecting and correcting code it rectify the code. Randomly generated key matrix always generated the invertible key matrix in Galois matrix for encryption of the data. So that it avoids the drawback of the traditional method. As Galois field used the entire bit pattern, it increases the speed of the encryption.

4.3.1 Encryption

In this Hill cipher algorithm ASCII character is taken as the plaintext. Then each character is converted into corresponding nonnegative integers from the look up table. The lookup tables consist of all small alphabet, those are assigned as integers starting from $0, 1\ldots\ldots.25.\ (\ i.e.\ a = 0, b = 1\ldots\ldots z = 25)$. But this is not an essential feature of the cipher. A block of m letters is then considered as a vector of n dimensions. Chose the key as a

square matrix of size $m \times m$ in which m is the size of the block. Each element of key matrix express in Galois field. The whole matrix is considered the cipher key, and should be random provided that the matrix is invertible in modulo of an irreducible polynomial of degree m (to ensure decryption is possible). If the length of plain text is not an integral multiple *of* the key size m, then add $z = 25$ as needed. Partition plaintext into n column vectors $\boldsymbol{v_n}$. Each integer of the plaintext express in polynomial formats in Galois field. Then take the product of key matrix and each column vector $\boldsymbol{v_n}$, equivalently, form the matrix product $K[v_1|v_2| \ldots \ldots \ldots \ldots \ldots |v_n]$.All the operation should be done in Galois field of modulo of irreducible polynomial of degree m. Reassemble the consecutive columns of this product into a new vector w. Finally, decode w into the corresponding cipher text string of modulo 26.

Example:

In Hill cipher 3×3 , the key matrix

$$K = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} (mod\ p(x))$$

Where $p(x)$ = primitive polynomial of degree m.

The cipher text of this key matrix is in polynomial form

$$C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3)\ mod\ 26$$
$$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3)\ mod\ 26$$
$$C_3 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3)\ mod\ 26$$

This case can be expressed in term of column vectors and matrices:

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} E_{11} & E_{12} & E_{13} \\ E_{21} & E_{22} & E_{23} \\ E_{31} & E_{32} & E_{33} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} (mod\ p(x))$$

$C = EP\ mod\ p(x)$, where C and P are column vectors of length3, representing the Cipher text and Plaintext respectively and E is a 3×3 encryption matrix. All operations are performed $mod\ m$.

ALGORITHM FOR ENCRYPTION

1. P is taken as plain text string.

2. A is the integer vector, created from P vector with the help of the look up table.

3. m is the size of the block.

4. A1 is the integer matrix generated after addition of extra bit in A (if necessary).

5. N is the number of columns, which is a factor of m.

6. J is the no. of column vectors equal to ratio of length of (A) and N.

7. A_j is the equivalent set containing all the column vectors.

8. K is the random key matrix of size $m \times m$.

9. E is the key matrix generated from K, expressed in Galois field.

10. B_j is the equivalent polynomial set of A_j expressed in Galois field.

11. C is the vector equivalently generated by the multiplication of E with each column vector of B_j (i.e $E \ [b_1|b_2|b_3| \dots \dots b_j]$) with modulo of irreducible polynomial with degree m.

12. T is the string of character s generated from C by the help of lookup table with $modulo\ 26$.

4.3.2 Decryption

Decryption is the process of getting back the original message(plain text) from the encrypted message(cipher text). A Hill cipher is relatively immune from attack if its key size n is large enough to preclude frequency analysis of n-graphs. For decryption, first we have to convert the cipher text back into the vector with the same procedure that have taken in encryption. For decryption it require to calculate the modulo inverse of the key matrix . The inverse k^{-1} of matrix k is defined by the equation

$$k.\ k^{-1} = \ k^{-1}.k = I$$

where I is the matrix that is all zeros expect for ones along the main diagonal from upper left to lower right. Hence decryption matrix D is generated by multiplying the modulo inverse key matrix with the cipher text. All the operation in this process carried out in modulus of same

degree m irreducible polynomial in Galois field. Then the data is converted back into the integer form from the polynomial form then into the character string with the help of the lookup table. We can explain these as

$$P = D.C = E^{-1}.C$$

In general, the algorithm can be expressed as follows:

$$C = E.P \bmod p(x)$$

$$P = E^{-1}.C \bmod p(x) = E^{-1} E.P \bmod p(x) = P$$

The original message p (i.e plaintext).

ALGORITHM FOR DECRYPTION:

1. Initially T string is converted into C vector with the help of the lookup table.

2. m is the size of the block.

3. C_1 is the integer matrix generated after addition of extra bit in C (if necessary).

4. N is the number of columns taken, which is the factor of m.

5. j is no. of column vectors equal to ratio of length of (C_1) and N.

6. C_2 is the equivalent set containing all the column vectors.

7. V_j is the set of column vector generated from C_2 expressed in polynomial format in Galois field.

8. E^{-1} is the inverse matrix, generated from E with modulus of degree m irreducible polynomial .

9. R is the equivalent vector generated by the multiplication of E^{-1} with each column vector V_j (i.e $E^{-1}[b_1|b_2|b_3| \dots \dots .b_j]$) with modulo of irreducible polynomial with degree m.

10. R_1 is the integer vector generated from the R.

11. T is the string of characters generated from R_1 with the help of lookup table of modulo 26.

a	0	i	8	q	16	y	24
b	1	j	9	r	17	z	25
c	2	k	10	s	18		
d	3	l	11	t	19		
e	4	m	12	u	20		
f	5	n	13	v	21		
g	6	o	14	w	22		
h	7	p	15	x	23		

Table -5: Lookup Table

4.4 A Novel Modified Hill Cipher Method Based on Exponentiation Value in Gf (2)

4.4.1 Encryption

In this modified Hill cipher method encryption is done with another new operation which we can named as exponentiations .Exponentiation decreases the average number of multiplications required to compute x^e provided that x^{-1} is supplied along with X [12].

The novel modified Hill cipher method is defined as follows

$$\begin{bmatrix} a_{11} & a_{12} & \dots\dots\dots\dots & a_{1m} \\ a_{21} & a_{22} & \dots\dots\dots\dots & a_{2m} \\ \dots & \dots & \dots\dots\dots\dots & \dots\dots \\ a_{m1} & a_{m2} & \dots\dots\dots\dots & a_{mm} \end{bmatrix}_{m\times m} * \begin{bmatrix} b_1 \\ b_2 \\ \dots \\ b_m \end{bmatrix}_{m\times n} = \begin{bmatrix} c_1 \\ c_2 \\ \dots \\ c_m \end{bmatrix}_{m\times n}$$

where $c_{ij} = \prod_{k=1}^{m} a_{kj}{}^{b_{ik}}$

In case of polynomials in $gf(2^m)$ for encryption the matrix B is a vector of polynomials in $gf(2^m)$ which represent 'n' bit of data. This B vector is the plain text vector is generated as before expressed in encryption algorithm step 9.   Matrix A is the key matrix consist of numbers

37

in Galois field of $modulo\ M$ where M is equal to $2^m - 1$. C is the cipher text matrix exponentiation as defined above is evaluated in mod of primitive polynomial of degree m. This results the cipher text matrix.

For Hill cipher 2×2 matrix the encryption is as follows:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \qquad\qquad B = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$$

Each element of A matrix and B vector are expressed in Galois field of mod of degree m of prime polynomial. The exponentiation C matrix is calculated as bellow

$$c_1 = b_1{}^{a_{11}} \times b_2{}^{a_{21}} (mod\ p(x))$$
$$c_2 = b_1{}^{a_{12}} \times b_2{}^{a_{22}} (mod\ p(x))$$

Where $p(x)$ = primitive polynomial of degree m.

This C vector converted into ASCII char with the help of the lookup table.

ALGORITHM FOR ENCRYPTION:

1. P is taken as plain text string.
2. X is the integer vector created from P vector with the help of the look up table.
3. m is the size of the block.
4. $X1$ is the integer matrix generated after addition of extra bit in X if necessary.
5. N is the number of columns taken, which is the factor of m.
6. J is the no. of column vectors is equal to ratio of length of (X) and N.
7. X_j is the equivalent set containing all the column vectors.
8. K is the key matrix created of size $m \times m$.
9. A is the key matrix generated from k expressed   in Galois field.
10. b_j is the set has been generated from X_j which is expressed   in polynomial format in Galois field.

11. C is the vector equivalently generated by taking the exponentiation of each element of A with each element of column vector b_j. It is described bellow with modulo of irreducible polynomial of degree m.

$$c_{ij} = \prod_{k=1}^{m} b_{kj}{}^{a_{ik}} \ (mod \ p(x))$$

12. T is the string of character generated from the C with the help of lookup table with modulo 26.

4.4.2 Decryption

For decryption, first we have to convert the cipher text back into the string of integer vector with the same procedure that has taken in encryption. For decryption it require to calculate the modulo inverse of the key matrix with the help of multiplicative inverse of the matrix and the inverse of matrix with modulo m. After finding out the inverse of the matrix we take the exponentiation of the key matrix same that as described in encryption for generating the plaintext in Galois field $gf(2^m)$.

It is one of the secure and fast Hill cipher algorithm for encryption. For Hill cipher 2×2 matrix the decryption is as follows:

$$X = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \qquad\qquad C = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$$

Each element of X matrix and C vector are expressed in Galois field of mod of degree m of prime polynomial. X is the multiplicative inverse matrix of A. The exponentiation R matrix is calculated as below

$$R_1 = c_1{}^{x_{11}} \times c_2{}^{x_{21}} (mod \ p(x)) = (b_1{}^{a_{11}} \times b_2{}^{a_{21}})^{x_{11}} \times (b_1{}^{a_{12}} \times b_2{}^{a_{22}})^{x_{21}} (mod \ p(x))$$
$$= b_1{}^{a_{11}x_{11}+a_{12}x_{21}} \times b_2{}^{a_{21}x_{11}+a_{22}x_{21}} = b_1$$

As we know that

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} a_{11}x_{11}+a_{12}x_{21} & a_{11}x_{12}+a_{12}x_{22} \\ a_{21}x_{11}+a_{22}x_{21} & a_{21}x_{12}+a_{22}x_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$R_2 = c_1{}^{x_{12}} \times c_2{}^{x_{22}} (mod\ p(x)) = (b_1{}^{a_{11}} \times b_2{}^{a_{21}})^{x_{12}} \times (b_1{}^{a_{12}} \times b_2{}^{a_{22}\,x_{22}})(mod\ p(x))$$

$$= b_1{}^{a_{11}x_{12}+a_{12}x_{22}} \times b_2{}^{a_{21}x_{12}+a_{22}x_{22}} = b_2$$

Now we get plain text matrix $B = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$.

ALGORITHM FOR DECRYPTION:

1. Vector matrix T is converted into integer vector.

2. Inverse of key matrix is calculated.

3. Multiplicative inverse of the determinant of key matrix with modulo of m is found.

4. Multiplicative inverse of the key matrix is calculated by simple multiplication of Output of step 3 and step2 with modulo m. Output of this step is denoted as X.

5. R is the equivalent vector generated by taking the exponentiation of each element of X with each element of column vector c. It is described bellow with modulo of irreducible polynomial with degree m.

$$R_{ij} = \prod_{k=1}^{m} c_{kj}{}^{x_{ik}} \ (mod\ p(x))$$

6. W is the string of character generated from the R with the help of lookup table with $modulo\ 26$.

4.5 Modified CRT in Galois Field $gf(2^m)$

4.5.1 Encryption

The CRT is used to solve a set of congruate equation with one variable but different module, which is relatively prime, means reconstruction of integers in a certain range of their residues modulo, a set of pair wise relatively prime module. In this method two prime polynomial $p_1 \& p_2$ of different degree $m_1\ and\ m_2$ respectively have taken which is relatively

prime to each other. A is the vector matrix of plain text is expressed in polynomial form in Galois field $gf(2^m)$. Intermediated vector c_{int} is calculated as defined below:

$$c_{int} = (q_1 \times x^{m_1} + r_1)(\mathrm{mod}\,(\mathrm{p}(\mathrm{x})))$$

where q_1 = quotient of the p_1, when it is divided by the 1st element of the A vector

r_1 = remainder of the p_1, when it is divided by the 1st element of the A vector

$p(x)$ = Primitive polynomial of degree M, where $M = m_1 + m_2$

In this method another two prime polynomial R_1 and R_2 are also taken of same degree p_1, p_2, respectively. The cipher text C_A is the vector matrix in polynomial format is generated by taking the exponent of K where K is not the factor of product of k_1 and k_2 are the minimal polynomial of the R_1 and R_2 prime polynomial. Mathematically it express as below

$C_A = c\_int^k\,(mod\,m)$

where m is the product of R_1, R_2

All the calculation is done in Galois field.

ALGORITHM FOR ENCRYPTION:

1. p_1 and p_2 are two prime polynomials taken with degree of m_1 and m_2 respectively.

2. w is the plain text of string of ASCII characters.

3. w_1 is the integer vector created from w.

4. A matrix is the polynomial format of w_1 vector matrix in the Galois field of modulo M.

   where $M = m_1 + m_2$

5. The formula for calculation of c_{int} is given below:

$$c_{int} = (q_1 \times x^{m_1} + r_1)(\mathrm{mod}\,(\mathrm{p}(\mathrm{x})))$$

where q_1 = quotient of the p_1, when it is divided by the 1st element of the A vector

r_1 = remainder of the p_1, when it is divided by the 1st element of the A vector

$p(x)$ = Primitive polynomial of degree M, where $M = m_1 + m_2$

6. R_1 and R_2 another two primitive polynomial with degree of m_1 and m_2 respectively.

7. $k_1 and k_2$ the minimal polynomials calculated from $R_1 and R_2$ respectively.

8. K is the integer taken, which not the factor is of $k_1 and k_2$, where k_1 and k_2 are the minimal polynomials of the $R_1 and R_2$ prime polynomial.

9. C_A is the cipher text matrix calculated as below

$$C_A = c_{int}{}^k \ (mod \ m) \ \text{where} \ m = R_1 \times R_2,$$

10. C is the encrypted string generated by conversion of the C_A into ASCII code

4.5.2 Decryption

Cryptosystem of CRT is highly vulnerable to attacks. The Chinese Remainder Theorem can also be used in Secret sharing, which consists of distributing a set of shares among a group of people who, all together (but no one alone), can recover a certain secret from the given set of shares. Each of the shares is represented in congruence, and the solution of the system of congruence using the Chinese remainder theorem is the secret to be recovered. Secret Sharing using the Chinese Remainder Theorem, along with the Galois field with special sequences of integers that guarantee the impossibility of recovering the secret from a set of shares with less than certain cardinality.

For decryption of the CRT, initially it required to find out multiplicative inverse of exponent value of the cipher text with modulo of the product minimal value of the other two prime polynomial. Multiplicative inverse can be calculated with the help of extended Euclidean algorithm. This is the inter-mediate value. From this we can get the original message or plaintext. We can explain it in bellow

ALGORITHM FOR DECRYPTION:

1. Vector matrix C_A is converted into integer vector.

2. k^{-1}, Multiplicative inverse of K with modulo $k_1 \times k_2$ is calculated with the help of Extended Euclidean algorithm.

3. c_{int} is the exponentiation k^{-1} of C_A with modulo of primitive polynomial of degree M.

4. Original message or plain text is calculate as below

$$((c_{int} - r_1) \div x^{m_1}) \times p_{1,} + r_1 = w_1 (mod \ (p(x)))$$

42

Where w_1 = integer vector of plaintext

5. Plaintext is calculated from w1 matrix by conversion of corresponding ASCII code.

Chapter 5

Results:

5.1 Result of Modified CRT in Galois Field $gf(2^m)$

5.1.1 Encryption

W-plaintext=

Cryptographyistheartorscienceencompassingtheprinciplesandmethodsoftransforminganintelligib
lemessageintoonethatisunintelligibleciphertextandthenretransformingthatmessagebacktoitsorigin
alform

W1-integer=

  99 114 121 112 116 111 103 114 97 112 104 121 105 115 116 104 101 97 114
116 111 114 115 99 105 101 110 99 101 101 110 99 111 109 112 97 115 115
105 110 103 116 104 101 112 114 105 110 99 105 112 108 101 115 97 110 109
101 116 104 111 100 115 111 102 116 114 97 110 115 102 111 114 109 105 110
103 97 110 105 110 116 101 108 108 105 103 105 98 108 101 109 101 115 115
97 103 101 105 110 116 111 111 110 101 116 104 97 116 105 115 117 110 105
110 116 101 108 108 105 103 105 98 108 101 99 105 112 104 101 114 116 101
120 116
97 110 100 116 104 101 110 114 101 116 114 97 110 115 102 111 114 109 105 110
103 116 104 97 116 109 101 115 115 97 103 101 98 97 99 107 116 111 105 116
115 111 114 105 103 105 110 97 108 102 111 114 109

>>P1=1   0   1   1

>> P2=1   0   0   1   0   1

q1=1   1   0   1

>> q2=1   0   1   0   0   1

k=17

>> k1=7

> k2 =31

C=,üË±]ÄüdËîE±îÃdü±]ü,EÃþ,ÃÃþ,] ËdEþÄ±îÃËüEþ,EËûÃdþ Ã±î]]ô±üdþô]ü EþÄdþEþ±Ãû ûEÄEìûÃ ÃdÄÃEþ±]]bÃ±îd±EÁþEþ±ÃûûEÄEìûÃ,EËîÃü±Ãdþ±îÃþüÃ±üdþô]ü EþÄ±îd± Ãd ÄÃìd,÷±]E±]üEÄEþdûô]ü

5.1.2 Decryption

k^{-1}=166

c_{int} =113 102 110 100   96 126 117 102 115 100 121 110 120 103 96 121 19
115 102   96 126 102 103 113 120 119 127 113 119 119 127 113 126 124
100 115 103 103 120 127 117   96 121 119 100 102 120 127 113 120 100 125 119
103   115   97 118 124 119   96 121 126 118 103 126 116 96 102 115 127 103 116
126 102   124 121 127 117 115 121 120 127 96 119 125 125 120 117 120 112 125
119 124   119   103 103 115 117 119 120 127 96 126 126 127 119 96 121 115 96
120 103   97   127 120 127   96 119 125 125 120 117 120 112 125 119 113 120 100
121 119 102 96
119 111   96 115 127 118 96 121 119 127 102 119 96 102 115 127 103 116 126 102
124 120 127 117   96 121 115 96 124 119 103 103 115 117 119 112 115 113 122 96
126 120 96 103 26 102 120 117 120 127 115 125 116 126 102 124

>> w1=
Cryptographyistheartorscienceencompassingtheprinciplesandmethodsoftransforminganintelligib
lemessageintoonethatisunintelligiblecipertextandthenretransformingthatmessagebacktoitsorigin
alform

Elapsed time is 2048.046575 seconds.

5.2 Result of Modified Hill Cipher Method in Galois Field

5.2.1 Encryption

P =
Cryptographyistheartorscienceencompassingtheprinciplesandmethodsoftransforminganintelligib
lemessageintoonethatisunintelligibleciphertextandthenretransformingthatmessagebacktoitsorigin
alform

A =
   2 17 24 15 19 14   6 17 0 15 7 24 8 18 19 7 4 0 17 19 14 17 18 2   8 4 13 2   4
   4 13 2 14 12 15   0 18 18 8 13 6 19 7   4 15 17 8 13 2 8 15 11   4 18 0 13 3 12 4 19
   7 14 3 18 14 5 19 17   0 13 18 5 14 17 12 8 13 6 0 13 8 13 19 4 11 11 8 6   8 1 11
   4 12 4 18 18 0 6 4 8 13 19 14 14 13 4 19 7 0 19 8 18 20 13 8 13 19 4 11 11
   8 6 8 1 11 4 2 8 15 7 4 17 19 4 23 19 0 13 3 19 7   4 13 17 4 19 17   0 13 18 5
  14 17 12 8 13 6 19 7 0 19 12   4 18 18 0 6 4 1 0 2 10 19 14 8 19 18 14 17   8 6
   8   3 0 11 5 14 17 12
>>M=5

 N = 5

K =
  28   15   16   24   25
   6   2   10   16   21
   9   31   13   20   14
  21   18   7   6   18
   9   13   18   12   25

 C =

2 7 6 25 11 20 16 11 10 6 19 29 24 27 13 22 1 10 19 20 30 22 31 14 11
21 31 2 19 30 5 31 15 6 4 30 7 2 20 25 22 27 19 29 18 29 21 24 7 8 16 5 20 4 21
12 31 29 11 3 9 29 16 18 14 9 0 20 5 28 15 1 16 7 8 2 17 4 10 11 30 21 9
3 20 15 5 23 14 18 11 12 8 1 17 5 24 9 24 22 22 25 2 14 19 18 29 5 12 11
14 22 31 0 28 28 3 7 28 29 8 8 16 20 22 25 12 9 0 20 20 0 9 5 19 0 22 0
20 26 24 3 4 28 11 6 1 20 30 21 20 9 30 20 29 18 5 23 24 21 27 4 0 9 29 19
21 17 13 25 5 30 21 10 25 0 11 3 2 6 8 3 26 6 4 24 25 28 1 7

>>T

Gzluqlkgtynwbktuwolvctfpgehcuzwtsvyhiqfuevmldjqsojaufpqhicreklvjdupfxoslmsbrfyjywwzco
tsfmlowadhsiquwzmjauuajptawauydelgbuvujusfxyveattvrnzfvkzaldcgidgeyzbhcbhrtdkcletdcgid
geyzbhc

5.2.2 Decryption

$E^{-1} =$

27	2	8	29	12
16	5	24	6	7
8	11	15	5	22
0	17	15	7	30
2	4	17	28	15

R1=

2 17 24 15 19 14 6 17 0 15 7 24 8 18 19 7 4 0 17 19 14 17 18 2 8 4
13 2 4 4 13 2 14 12 15 0 18 18 8 13 6 19 7 4 15 17 8 13 2 8 15 11 4 18
0 13 3 12 4 19 7 14 3 18 14 5 19 17 0 13 8 5 14 17 12 8 13 6 0 13 8 13
19 4 11 11 8 6 8 1 11 4 12 4 18 18 0 6 4 8 13 19 14 14 13 4 19 7 0
19 8 18 20 13 8 13 19 4 11 11 8 6 8 1 11 4 2 8 15 7 4 17 19 4 23 19 0 13
3 19 7 4 13 17 4 19 17 0 13 18 5 14 17 12 8 13 6 19 7 0 19 12 4 18 18 0
6 4 1 0 2 10 19 14 8 19 18 14 17 8 6 8 13 0 11 5 14 17 12

T =

Cryptographyistheartorscienceencompassingtheprinciplesandmethodsoftransforminganintelligib
lemessageintoonethatisunintelligibleciphertextandthenretransformingthatmessagebacktoitsorigin
alform.

Elapsed time is 4.057650 seconds.

5.3 Result of Novel Method of Hill Cipher using Exponentiation in $gf(2^M)$

5.3.1   Encryption

Please enter a sentence −

'cryptographyistheartorscienceencompassingtheprincipleandmethodsoftransforminganintelligibl
emessageplaintextintoonethatisunintelligibleciphertextandthenretransformingthatmessagebackto
itsoriginalform'

int_word =

 3 18 25 16 20 15   7 18   1 16   8 25   9 19 20   8   5   1 18 20 15 18 19   3   9   5 14
 3   5   5 14   3 15 13 16   1 19 19   9 14   7 20   8   5 16 18   9 14   3   9 16 12   5   1 14
 4 13   5 20   8 15   4 19 15   6 20 18   1 14 19   6 15 18 13   9 14   7   1 14   9 14 20
 5 12   2   9   7   9   2 12   5 13   5 19 19   1   7   5 16 12   1   9 14 20   5 24 20   9 14 20
15 15 14   5 20   8   1 20   9 19 21 14   9 14 20   5 12 12   9   7   9   2 12   5   3   9 16   8
 5 18 20   5 24 20   1 14   4 20   8   5 14 18   5 20 18   1 14 19   6 15 18 13   9 14   7
20   8   1 20 13   5 19 19   1   7   5   2   1   3 11 20 15   9 20 19 15 18   9   7   9 14   1
12   6 15 18 13

the number of row you want = 2

input no. of bits u want = 7

ket_word=

```
 3   5   11   13
17   19  23   29
31   37  41   43
47   53  59   61
```

tran_dec_mat = GF(2^7) array. Primitive polynomial = D^7+D^3+1 (137 decimal)

Array elements =

```
 52  103  24  73  106   3   7  10  50  16  54 114  76  11  72  82  17  85  84  89  66  12  84 100
125  66  58  59  95  19  58 59  55  91  18  50 121   7 122  34  44  98  40  61   6   114 122
34  66 119 112  74  17  85 104  35 119  35  72  82  40 93 100 111   4  12  22  94  10
62  59   5  65 105 122  34  21 107  71  40  57  38  120  67 104  56 119   5  103  96 38
22  56 124  23  91 25  92 112  74 109   9  57  38 127   5  83 122  57  38  13  49 100  77
72  82  40  20  76  11  59 104 122  34  35   1  27  32  45  17  44  83  34   24  66 119  44
11 109  41 35   1 64 54 110   14  45  90  40  61  28  80  5 76  22  94  10  62  59  5  65
105 122  34  44  98  64  36  68  83  56 124  23  91  25  92   4  8 112  105 106   3  21
26 100  111 73   3  119   5  84  110  48  16  66  12  43  66
```

tran_char =

Çx©ÊcgjpÒ¬k¨²qµ´¹¢l´ÄÝ¢¿s»rÙgÚÂ • fÒÚ¢×Ðªqµ È ×¨²½ÄÏdlv¾je¡ÉÚuË§Ø£È×eÇÀvÜw»y
¼Ðª Íißo³ÚmÄ-¨²t¬kÈÚa{ • q³x¢×kÍa În • º • |°e¬v¾je¡ÉÚÂ ¤³Üw»y¼dhÐÉÊcuzÄÏ©c×eÍ • p¢l
¢

5.3.2 Decryption

exp_value = 127

Inverse key martrix

```
77   122   35    30
65    33   10    80
35    12   95   101
121   76   64    82
```

>> res1_dec_mat

3 18 25 16 20 15   7 18 1 16 8 25   9 19   20   8 5 1 18   20 15   18 19 3 9 5   14 3
5   5 14 3 15 13 16 1 19 19   9 14 7 20   8   5 16 18 9 14 3   9 16 12   5 1   14   4
13 5 20 8 15 4   19 15   6 20 18 1 14 19 6 15 18 13 9 14 7 1 14   9 14 20 5 12
12 9 7   9 2 12   5   13 5 19 19   1 7 5 16 12 1 9 14   20 5 24   20 9 14 20 15 15
14   5 20   8   1 20 9 19 21 14   9 14   20   5 12   12 9 7 9 2 12 5 3 9 16 8 5 18
20 5 24 20 1 14 4 20   8   5 14   18   5   20 18 1 14   19   6 15 18 13   9 14 7   20
8 1 20 13 5 19 19   1 7 5 2 1   3 11 20 15   9 20 19 15   18   9   7   9 14 1 12
6 15 18 13 26

res_char =

cryptographyistheartorscienceencompassingtheprincipleandmethodsoftransforminganintelligible
messageplaintextintoonethatisunintelligibleciphertextandthenretransformingthatmessagebacktoit
soriginalform

Elapsed time is 14.143951 seconds.

Chapter 6

6.1 Conclusion

Arithmetic operations in Galois Fields GF(2^M) play an essential role in the area of communications including error-correcting codes, cryptography, and digital signal processing. In these applications, area and speed requirements are essential. Therefore, an efficient hardware structure for such operations is desirable. The efficiency of these applications heavily depends on the efficiency of the arithmetic operations in Galois fields like addition (sum), multiplication (product), inversion, and exponentiation. So all the work done in this project related to Galois field. With extensive simulation studies, it is shown that modified Hill cipher method is one of the secure method of encryption in Galois field as compared to any other encryption method, because the bit pattern of the message and higher order key size matrix is difficult to crack the message. As this algorithm uses a different key for each block encryption thereby significantly increases its resistance to various attacks. In this method, the exponentiation of data represented in Galois field which is computationally quite efficient compare to normal exponentiation. It is very tedious and computationally very intense to crack the code. Cipher text-only cryptanalysis of Hill cipher is very difficult. Cryptosystem of CRT is highly vulnerable to attacks. Secret Sharing using the Chinese Remainder Theorem, along with the Galois field with special sequences of integers that guarantee the impossibility of recovering the secret form a set of shares with less than a certain cardinality.

6.2   Future Work

- Though it is very complicated to find out the inverse of higher order matrix in polynomial modular arithmetic, It is proposed to developed an self invertible matrix in Galois field which will provide the robustness of the Hill cipher method with the higher order of the key size. For finding out, the self invertible matrix 1st we have to find out the Eigen values of the matrix of higher order key size which is very mathematically complicated one in polynomial Galois field.

- Among basic arithmetic operations in $GF(2^M)$multiplicative inversion specially in extended Euclidean algorithm and exponentiation using square-and multiply algorithm is the most time consuming which increases cost .Recently one paper is published on

finding out the Inversion in $GF(2^M)$ suitable for Implementation Using a Polynomial Multiply Instruction on $gf(2)$ [15]. So it is proposed to apply this algorithm in the 2nd Hill cipher method and modified CRT method reduction of computation time [16].

REFERENCE

1. W. Stallings, "*Cryptography and Network Security*", 4th edition, Prentice Hall, 2005.

2. Imai H., Hanaoka G., Shikata J., Otsuka A., Nascimento A.C., "*Cyptography with Information Theoretic Security*", Information Theory Workshop, 2002, Proceedings of the IEEE, 20-25 Oct 2002.

3. Behrouz A.Forouzan , *"Cryptography and network security",* Special Indian edition 27,Tata McGraw-Hill, 2006

4. Debdeep Mukhopadhyay, Gaurav Sengar, and Dipanwita Roy Chowdhury, "*Hierarchical Verification of Galois Field Circuits"*, IEEE transactions on computer-aided design of integrated circuits and systems, Vol. 26, No. 10, October 2007.

5. S. Morioka, Y. Katayama, and T. Yamane, "*Towards efficient verification of arithmetic algorithms over Galois fields GF(2^m),"* in *Proc. CAV*, 2001, vol. 2102, pp. 465–477.

6. F. Argu¨ello , "*Lehmer-based algorithm for computing inverses in Galois fields GF(2^m)",* ELECTRONICS LETTERS 2nd March 2006 Vol. 42 No. 5

7. *"Hill-cipher"*. wikipidea, The free encyclopedia

8. Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, and Saroj Kumar Panigrahy, "*Novel methods of generating self-invertible matrix for hill cipher algorithm*" International Journal of Security, Volume 1 : Issue (1)2007

9. Huiyong Liao and Xiang-Gen Xia, "*A Sharpened Dynamic Range of a Generalized Chinese Remainder Theorem for Multiple Integers*" Ieee Transactions On Information Theory, Vol. 53, No. 1, January 2007.

10. Wei Wang, M.N.S. Swamy, M.O. Ahmad and Yuke Wang, "*A Comprehensive Study Of Three Moduli Sets For Residue Arithmetic",* Proceedings of the 1999 IEEE Canadian Conference on Electrical and Computer Engineering Shaw Conference Center, Edmonton, Alberta, Canada May 9-12,1999

11. Wen Tao Zhu , "*Analyzing Euler-Fermat Theorem Based Multicast Key Distribution Schemes with Chinese Remainder Theorem",* IFIP International Conference on Network and Parallel Computing , 2008

12. O. E_gecio_glu, *"Exponentiation using Canonical Recoding"*, Department of Computer Science University of California Santa Barbara, California , Theoretical Computer Science, 129(2):407-417, 1994.

13. J. Pegueroles and F. Rico-Novella, *"Rekeying de grupo en multicast seguro usando el Teorema de Fermat,"* Proceedings of URSI 2002 (ISBN: 84-8138- 517-4), pp. 477–478, Sept. 2002.

14. K.-H. Chi, J.-H. Jiang, Y.-C. Hsu, *"Multigroup rekeying for a wireless network,"* NBIS 2007, Lecture Notes in Computer Science, vol. 4658, pp. 147–156, Sept. 2007.

15. Katsuki Kobayashi, Naofumi Takagi, and Kazuyoshi Takagi , *"An Algorithm for Inversion in GF(2m) Suitable for Implementation Using a Polynomial Multiply Instruction on GF(2)"*, 18th IEEE Symposium on Computer Arithmetic(ARITH'07) Department of Information Engineering, Graduate School of Information Science, Nagoya University.

16. Xiang-Gen Xia and Kejing Liu, *"A Generalized CRT for residue sets with errors and its application in frequency determination from multiple sensors with low sampling rates"*, IEEE Signal Processing Letters, Vol. 12, No. 11, November 2005

17. Yi Shiung Yeh,Tzong-chen wu,Chin-ChenChang, *"A new cryptosystem using Matrix transformation"*, 25th Annual 1991 IEEE International Carnahan Conference on Security Technology, 1991.

18. Bao Ngoc Tran,Thus Dinh Nguyen, *"Modular Matrix Cipher and its application in authentication protocol"*, Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing , 2008