JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CRYPTOGRAPHIC METHODS: SSC-KT AND SSC-MT TO ENHANCE DATA SECURITY OF COMMUNICATION

Dr. Akash Thakkar
Department of Cyber Security and Digital Forensics
Narnarayan Shastri Institute of Technology - Institute of Forensic Sciences & Cyber Security (NSIT-IFSCS)
Affiliated to National Forensic Sciences University (NFSU)
Ahmedabad, Gujarat, India
akash.thakkar@nsitifscs.ac.in

Abstract : Encryption and decryption are the two primary stages of cryptography, which uses mathematical concepts to secure data. To prevent unauthorized access, readable data has been converted into an unreadable format through encryption, which can be recovered by decryption. Kamal and Mellin Transform-based encryption and decryption techniques provide only a limited level of security when utilized individually. The public-key Schmidt-Samoa Cryptosystem (SSC) depends on the complexity of large integer factorization to ensure security. This paper presents cryptographic techniques that improve security by combining SSC with Kamal and Mellin Transforms. Furthermore, correlation analysis and frequency tests were performed to examine these techniques.

IndexTerms - Cryptography, Encryption, Decryption, SSC, Kamal Transform, Mellin Transform

I. INTRODUCTION

Cryptography is the art and science of achieving security by encoding messages to make them non-readable. [5] Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. [7] Two crucial cryptographic functions are encryption and decryption. Normal data is transformed into an unreadable form through encryption and the reverse is accomplished through decryption.

In symmetric key cryptography (also known as private key cryptography) same key is shared, i.e., the one key is used in both encryption and decryption. [3] It also requires a secure method for parties to share the key. Symmetric key cryptography algorithms, such as AES, DES, RC4, Blowfish and others, are known for their simplicity and efficiency, requiring less execution time.

In asymmetric key cryptography (also known as public key cryptography) different keys are used for encryption and decryption. The two keys are public key and private key. [3] Public key is used encryption and private key is used for decryption. Asymmetric key algorithms are more secure than the symmetric key algorithms but the working process is slower than symmetric key algorithms. Examples of asymmetric key algorithms: Rabin, RSA, ElGamal, ECC etc.

1.1 Schmidt-Samoa Cryptosystem (SSC)

Schmidt-Samoa Cryptosystem is an asymmetric cryptographic technique; whose security depends on the difficulty of integer factorization problem. [1]

SSC is divided into three stages.

1. Key Generation
2. Encryption process
3. Decryption process

Stage 1: key Generation [1]

1. Choose two large prime numbers p and q
2. Compute $N = p^2 q$
3. Compute $d \equiv N^{-1} \, mod \, (lcm(p-1, q-1))$

Public key: (N) and Private key: (d)

Stage 2: Encryption process [1]
Message $M < N$ can be encrypted as: $C \equiv M^N \ mod \ N$
Stage 3: Decryption process [1]
Ciphertext C can be decrypted as: $M \equiv C^d \ mod \ pq$

Integral transformations are important for cryptographic procedures. By using these transformations' characteristics to develop encryption and decryption methods, cryptographic systems become more secure and effective.

1.2 Kamal Transform (KT)

Kamal Transform was introduced by Kamal and Sedeeg in 2016. Kamal Transform is derived from the Fourier integral and is widely utilized in applied mathematics and engineering. [6][8]
Over the set of functions

$$A = \{ f(t) / \exists M, k_1, k_2 > 0 , |\{f(t)\}| < M e^{|t|/k_j}, \text{if } t \in (-1)^j \times [0, \infty)\}$$

For a given function in the set A, the constant M must be finite number, k_1, k_2 may be finite or infinite. [8]
Kamal Transform is defined by [8]

$$K[f(t)] = G(v) = \int_0^\infty f(t) e^{-t/v} \, dt, t \geq 0, \ k_1 \leq v \leq k_2 \quad \ldots (1)$$

The variable v in this transform is used to factor the variable t in the argument of the function f.

Some standard functions: [8]
For any function $f(t)$, we assume that the integral equation (1) exists.
1. Let $f(t) = 1$ then $K[1] = v$
2. Let $f(t) = t$ then $K[t] = v^2$
3. Let $f(t) = t^2$ then $K[t^2] = 2v^3 = 2!\, v^3$
4. In general case, if $n > 0$, then $K[t^n] = n!\, v^{n+1}$

Inverse Kamal Transform: [8]
1. $K^{-1}[v] = 1$
2. $K^{-1}[v^2] = t$
3. $K^{-1}[v^3] = \frac{t^2}{2!}$
4. In general case, if $n > 0$, then $K^{-1}[v^{n+1}] = \frac{t^n}{n!}$

1.3 Mellin Transform (MT)

The integral transform known as the Mellin Transform carries the name of the mathematician Hjalmar Mellin (1854-1933). [2][12]

Let $F(x)$ be a function defined for all positive values of t, then the Mellin Transform of $f(x)$ is defined by [12]

$$f(x)^*(s) = \int_0^\infty f(x) x^{s-1} \, dx \quad \ldots (2)$$

Properties of Mellin Transform: [12]
1. Scaling: $f^*(at)(s) = a^{-s} f^*(s)$
2. Inverse of independent variable: $(x^{-1} f(x^{-1}))^* = f^*(1 - s)$
3. Multiplication by Power of $ln\ x$: $((\ln x)^k (f(x)))^* = \frac{d^k}{ds^k} f*(s)$
4. Derivative: $(\frac{d^k}{dx^k} f(x))^* = (-1)^k (s-k)_k f^*(s-k)$

where: $(s-k)_k = (s-k)(s-j+1) \ldots (s-1) = \frac{\Gamma(s)}{\Gamma(s-k)}$

5. Convolution: $(f(x)g(x))^* = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} F(z) G(s-z) dz$

II. LITERATURE REVIEW

Santana (2014) developed a scheme in cryptography whose construction is based on the application of the Mellin Transform. This paper presented the key generation, encryption and decryption processes using the properties of the Mellin Transform. [12]

Kamal and Sedeeg (2016) introduce the Kamal transform as a new integral transform. They presented the definition and application of the Kamal transform. This paper provided a comprehensive introduction to the Kamal transform and its potential contributions to the field of information security. [6]

Thangavel and Varalakshmi (2016) proposed Enhanced Schmidt-Samoa cryptosystem (ESS). When compared to SSC, the ESS cryptosystem is composed of four prime numbers, which increases the complexity of breaking the cryptosystem. The experimental results with variable file size and key size also proved that the time required to perform the data encryption and decryption in ESS is lower and the time required to perform cryptanalysis in ESS is higher compared with SSC. Thus, the ESS cryptosystem is highly secured, and improves data confidentiality. [22]

Tayal et al. (2017) provided a comprehensive review of network security and cryptography. This paper covered various aspects of network security, including authentication, encryption, secure communication protocols and emerging trends in the field. [14]

Al-Haija et al. (2018) conducted a systematic expository review of the Schmidt-Samoa cryptosystem. Also, the cryptosystem's design issues have been methodologically analyzed and investigated in this paper. [1]

Johar (2019) provided a comprehensive overview of the Mellin transform. This paper introduced the basic concepts and properties of the Mellin transform, discussing its applications in various fields. [2]

Mittal and Gupta (2019) developed new cryptographic scheme using Kamal transform with congruence modulo operator involving ASCII value for encryption and decryption of message. [8]

Nagalakshmi et al. (2019) proposed an enhancement to data security by combining the RSA algorithm with the application of Laplace Transform Cryptosystem. The proposed algorithm was implemented using a high-level programme and its time complexity was tested using RSA cryptosystem algorithms. The comparison showed that the proposed algorithm improves data security when compared to RSA cryptosystem algorithms and the use of the Laplace transform in cryptosystem schemes. [9]

Nagalakshmi et al. (2020) proposed an implementation of ElGamal scheme for Laplace transform cryptosystem. The time analysis is compared with existing algorithms and comparison reveals that the proposed cryptosystem enhances the data security. [10]

Thakkar and Gor (2021) presented a review of literature concerned with cryptographic algorithms and mathematical transformations. The review of RSA and ElGamal algorithms aids readers in better understanding the differences between the two asymmetric key cryptographic algorithms and how they work. The review of mathematical transformations helps the reader to understand how mathematical transformations are used in cryptography. [15]

Thakkar and Gor (2022) introduced cryptographic methods integrating:

- RSA algorithm with Kamal Transform. [22]
- ElGamal algorithm with Kamal Transform. [23]
- ElGamal algorithm with Mellin Transform. [24]

Thakkar and Gor (2023) introduced cryptographic methods integrating:

- RSA algorithm with Mellin Transform. [25]
- RSA algorithm with Sumudu Transform. [26]
- ElGamal algorithm with Sumudu Transform. [27]

III. METHODOLOGY

The key generation, encryption and decryption procedures for the proposed SSC-KT and SSC-MT methods are provided in this section.

3.1 PROPOSED METHOD SSC-KT

The proposed method is SSC with application of Kamal Transform (SSC-KT). In this proposed method SSC-KT, polynomial will be generated using the Euler's phi function to apply the properties of Kamal Transform. The proposed work is to improve security of communication. When two parties want to transfer the data, they will follow the given steps for encryption and decryption. The following method gives an idea of how the proposed cryptographic scheme works.

3.1.1 Method of Key Generation

Steps involved in Key Generation as follows.

Step 1: Generate any two large prime numbers p and q

Step 2: Compute the public key as $N = p^2q$

Step 3: Find the private key as $d = N^{-1}\ mod\ lcm(p-1, q-1)$

Step 4: Calculate $n = pq$ and $\phi(n) = (p-1)\cdot(q-1)$

Step 5: Generate polynomial $p(t)$ using $\phi(n)$. i.e., $p(t) = \sum_{i=0}^{m} \phi(n)\ t^i$

3.1.2 Method of Encryption

Steps involved in Encryption as follows.

Step 1: Select the plaintext $P_0, P_1, \dots, P_m$, convert into ASCII code integer $M_0, M_1, \dots, M_m$

Step 2: Compute $R_i \equiv M_i^N\ mod\ N$

Step 3: Calculate $R_i\ (p(t)) = R_i \sum_{i=0}^{m} \phi(n)\ t^i = \sum_{i=0}^{m} G_i\ t^i$

Step 4: Apply Kamal Transform of a polynomial, i.e., $K\ [\sum_{i=0}^{m} G_i\ t^i] = \sum_{i=0}^{m} b_i\ v^{i+1}$

Step 5: Compute ciphertext C such that $C_i \equiv b_i\ mod\ N$

Step 6: Find $k_i = (b_i - C_i)/N$

Step 7: Each integer of ciphertext $C_0, C_1, \dots, C_m$ is converted to its construct by ASCII character is stored as the ciphertext C

3.1.3 Method of Decryption

Steps involved in Decryption as follows.

Step 1: Consider the ciphertext C and key k_i received from the sender

Step 2: Ciphertext C converted to ASCII values of $C_0, C_1, \dots, C_m$

Step 3: Compute $b_i = C_i + (N \cdot k_i)$

Step 4: Find the polynomial assuming b_i as a coefficient

Step 5: Apply inverse Kamal Transform, i.e., $K^{-1}[\sum_{i=0}^{m} b_i v^{i+1}] = \sum_{i=0}^{m} G_i\ t^i$ and find R_i as $\frac{G_i}{\phi(n)}$

Step 6: Each integer of R_i is converted into $M_i = R_i^d\ mod\ pq$

Step 7: Each integer M_i are converted to their corresponding ASCII Code values and hence get the original plaintext $P_0, P_1, \dots, P_m$

Public key: $\{p(t), N, k_i\}$
Private key: $\{d\}$

3.2 PROPOSED METHOD SSC-MT

The proposed method is SSC with application of Mellin Transform (SSC-MT). In this proposed method SSC-MT, polynomial will be generated using the value of $lcm(p-1, q-1)$ to apply the properties of Mellin Transform, where p and q are prime numbers. The proposed work is to improve security of communication. When two parties want to transfer the data, they will follow the given steps for encryption and decryption. The following method gives an idea of how the proposed cryptographic scheme works.

3.2.1 Method of Key Generation

Steps involved in Key Generation as follows.
Step 1: Generate any two large prime numbers p and q
Step 2: Compute the public key as $N = p^2 q$
Step 3: Find the private key as $d = N^{-1} \ mod \ lcm(p-1, q-1)$
Step 4: Generate polynomial $p(x)$ using $L = lcm(p-1, q-1)$ i.e., $p(x) = \sum_{i=1}^{m} L \ x^i$

3.2.2 Method of Encryption

Steps involved in Encryption as follows.
Step 1: Select the plaintext $P_1, P_2, \dots, P_m$, convert into ASCII code integer $M_1, M_2, \dots, M_m$
Step 2: Compute $R_i \equiv M_i^N \ mod \ N$
Step 3: Generating function $L(x) = e^{-x}[R_i \ p(x)] = \ \sum_{i=1}^{m} e^{-x}[R_i \ L \ x^i] \ = \sum_{i=1}^{m} e^{-x} \ G_i \ x^i$
Step 4: Apply Mellin Transform on $L(x)$ i.e., $L(x)^* = \sum_{i=1}^{m} G_i \ (s+i-1)!$
Step 5: Choose s and get $\sum_{i=1}^{m} B_i$
Step 6: Compute ciphertext C such that $C_i \equiv B_i \ mod \ N$
Step 7: Find k_i such that $k_i = (B_i - C_i)/N$ and $k_0 =$ (value of s)
Step 8: Each integer of ciphertext $C_1, C_2, \dots, C_m$ is converted to its construct by ASCII character is stored as the ciphertext C

3.2.3 Method of Decryption

Steps involved in Decryption as follows.
Step 1: Consider the ciphertext C and key k_i received from the sender
Step 2: Ciphertext C converted to ASCII values of $C_1, C_2, \dots, C_m$
Step 3: Compute $B_i = C_i + (N \cdot k_i)$
Step 4: Find the polynomial assuming B_i as a coefficient
Step 5: Apply inverse Mellin Transform i.e., $L^*(x) = e^{-x} \sum_{i=1}^{m} B_i \ x^i = \ \sum_{i=1}^{m} \frac{B_i}{(s+i-1)!} = \sum_{i=1}^{m} G_i$ and find R_i as $\frac{G_i}{L}$
Step 6: Each integer of R_i is converted into $M_i = R_i^d \ mod \ pq$
Step 7: Each integer M_i are converted to their corresponding ASCII Code values and hence get the original plaintext $P_1, P_2, \dots, P_m$

Public key: $\{p(x), N, k_i\}$
Private key: $\{d\}$

IV. NUMERICAL EXAMPLE

This section provides a numerical example of the proposed encryption and decryption methods, SSC-KT and SSC-MT.

4.1 NUMERICAL EXAMPLE OF SSC-KT METHOD

In SSC-KT method parameters are chosen to make computation easier, however they are not in the useable range for secure transmission.

If Alice (sender) wants to send an encrypted message to Bob (receiver).
Bob first computes his parameters using steps as given in method of Key Generation.
Step 1: Primes $p = 37$ and $q = 41$
Step 2: $N = p^2 q = (37)^2(41) = 56129$
Step 3: $d \ = \ N^{-1} \ mod \ lcm(p-1, q-1) = 56129^{-1} \ mod \ 360 = 209$
Step 4: $n = pq = 1517$ and $\phi(n) = (p-1) \cdot (q-1) = 1440$
Step 5: Polynomial $p(t)$ using $\phi(n)$. i.e., $p(t) = \sum_{i=0}^{m} 1440 \cdot t^i$

Bob then sends his public key $(p(t), N)$ to Alice.
Alice computes his parameters to encrypt the message using steps as given in method of Encryption.

Step 1: Plaintext = "**In$pire**", $P_0 = I, P_1 = n, P_2 = \$, P_3 = p, P_4 = i, P_5 = r, P_6 = e$
Convert into ASCII Code integer $M_0 = 73, M_1 = 110, M_2 = 36, M_3 = 112, M_4 = 105, M_5 = 114, M_6 = 101$
Step 2: Compute $R_i \equiv M_i^{56129} \ mod \ 56129$
we get, $R_0 = 27379, R_1 = 20534, \ R_2 = 52021, R_3 = 16429, R_4 = 19049, R_5 = 35948, R_6 = 39120$

Step 3: $R_i\left(p(t)\right) = \sum_{i=0}^{6} R_i \cdot \phi(n) \cdot t^i = \sum_{i=0}^{6} R_i \cdot 1440 \cdot t^i$
$= 39425760 + 29568960 \cdot t + 74910240 \cdot t^2 + 23657760 \cdot t^3 + 27430560 \cdot t^4 + 51765120 \cdot t^5 + 56332800 \cdot t^6$
$= \sum_{i=0}^{6} G_i\, t^i$
Step 4: $K\left[\sum_{i=0}^{6} G_i\, t^i\right] = K[39425760 + 29568960 \cdot t + 74910240 \cdot t^2 + 23657760 \cdot t^3 + 27430560 \cdot t^4 + 51765120 \cdot t^5 + 56332800 \cdot t^6]$
$= 39425760 \cdot v + 1! \cdot 29568960 \cdot v^2 + 2! \cdot 74910240 \cdot v^3 + 3! \cdot 23657760 \cdot v^4 + 4! \cdot 27430560 \cdot v^5 + 5! \cdot 51765120 \cdot v^6 + 6! \cdot 56332800 \cdot v^7$
$= 39425760 \cdot v + 29568960 \cdot v^2 + 149820480 \cdot v^3 + 141946560 \cdot v^4 + 658333440 \cdot v^5 + 6211814400 \cdot v^6 + 40559616000 \cdot v^7$
$= \sum_{i=0}^{6} b_i\, v^{i+1}$
we get, $b_0 = 39425760, b_1 = 29568960, b_2 = 149820480, b_3 = 141946560, b_4 = 658333440, b_5 = 6211814400, b_6 = 40559616000$
Step 5: Compute ciphertext C such that $C_i \equiv B_i \; mod\; 56129$
we get, $C_0 = 23202, C_1 = 45106, C_2 = 12179, C_3 = 52448, C_4 = 52528, C_5 = 17970, C_6 = 14794$
Step 6: Find $k_i = (b_i - C_i)/56129$
we get, $k_0 = 702, k_1 = 526, k_2 = 2669, k_3 = 2528, k_4 = 11728, k_5 = 110670, k_6 = 722614$
Step 8: Each integer of ciphertext $C_0 = 23202, C_1 = 45106, C_2 = 12179, C_3 = 52448, C_4 = 52528, C_5 = 17970, C_6 = 14794$ is converted to its construct by ASCII character C_0 =媚, C_1 =姦 , C_2 =角, C_3 =첨, C_4 =歃, C_5 =襯, C_6 =抪 and stored as the ciphertext C = " **媚姦角첨歃襯抪** "

Alice then sends (k_i, ciphertext C) to Bob.
Bob decrypts the ciphertext using steps as given in method of Decryption.

Step 1: Consider the ciphertext C and key k_i received from the sender
Step 2: Ciphertext C = " **媚姦角첨歃襯抪** " converted to ASCII values of
$C_0 = 23202, C_1 = 45106, C_2 = 12179, C_3 = 52448, C_4 = 52528, C_5 = 17970, C_6 = 14794$
Step 3: Compute $b_i = C_i + (N \cdot k_i)$
we have, $k_0 = 702, k_1 = 526, k_2 = 2669, k_3 = 2528, k_4 = 11728, k_5 = 110670, k_6 = 722614$
we get, $b_0 = 39425760, b_1 = 29568960, b_2 = 149820480, b_3 = 141946560, b_4 = 658333440, b_5 = 6211814400, b_6 = 40559616000$
Step 4: Find the polynomial assuming b_i as a coefficient
$39425760 \cdot v + 29568960 \cdot v^2 + 149820480 \cdot v^3 + 141946560 \cdot v^4 + 658333440 \cdot v^5 + 6211814400 \cdot v^6 + 40559616000 \cdot v^7$
Step 5: Apply inverse Kamal Transform
$K^{-1}[\sum_{i=0}^{6} b_i v^{i+1}] =$
$K^{-1}[39425760 \cdot v + 29568960 \cdot v^2 + 149820480 \cdot v^3 + 141946560 \cdot v^4 + 658333440 \cdot v^5 + 6211814400 \cdot v^6 + 40559616000 \cdot v^7]$
$= 39425760 + (29568960 \cdot t)/1! + (149820480 \cdot t^2)/2! + (141946560 \cdot t^3)/3! + (658333440 \cdot t^4)/4! + (6211814400 \cdot t^5)/5! + (40559616000 \cdot t^6)/6!$
$= 39425760 + 29568960 \cdot t + 74910240 \cdot t^2 + 23657760 \cdot t^3 + 27430560 \cdot t^4 + 51765120 \cdot t^5 + 56332800 \cdot t^6$
$= \sum_{i=0}^{6} G_i\, t^i$
Compute $\frac{G_i}{\phi(n)}$ and get integer $R_0, R_1, \ldots, R_6$
we get, $R_0 = 27379, R_1 = 20534, R_2 = 52021, R_3 = 16429, R_4 = 19049, R_5 = 35948, R_6 = 39120$
Step 6: Each integer of R_i is converted into $M_i = R_i^{209}\; mod\; 1517$
we get, $M_0 = 73, M_1 = 110, M_2 = 36, M_3 = 112, M_4 = 105, M_5 = 114, M_6 = 101$
Step 7: Each integer M_i are converted to their corresponding ASCII Code values$P_0 = I, P_1 = n, P_2 = \$, P_3 = p, P_4 = i, P_5 = r, P_6 = e$ and hence get the original plaintext = **"In$pire"**

4.2 NUMERICAL EXAMPLE OF SSC-MT METHOD

In SSC-MT method parameters are chosen to make computation easier, however they are not in the useable range for secure transmission.

If Alice (sender) wants to send an encrypted message to Bob (receiver).
Bob first computes his parameters using steps as given in method of Key Generation.
Step 1: Primes $p = 31$ and $q = 37$
Step 2: $N = p^2 q = (31)^2(37) = 35557$
Step 3: $d = N^{-1}\; mod\; lcm(p-1, q-1) = 35557^{-1}\; mod\; 180 = 13$
Step 4: Polynomial $p(x)$ using $L = lcm(p-1, q-1) = 180$ i.e., $p(x) = \sum_{i=1}^{m}(180)\, x^i$

Bob then sends his public key $(p(x), N)$ to Alice.
Alice computes his parameters to encrypt the message using steps as given in method of Encryption.

Step 1: Plaintext = "**Inf!n!ty**",
$P_1 = I, P_2 = n, P_3 = f, P_4 = !, P_5 = n, P_6 = !, P_7 = t, P_8 = y$

Convert into ASCII Code integer
$M_1 = 73, M_2 = 110, M_3 = 102, M_4 = 33,$
$M_5 = 110, M_6 = 33, M_7 = 116, M_8 = 121$

Step 2: Compute $R_i = M_i^{35557} \, mod \, 35557$
we get, $R_1 = 23790, R_2 = 7917, R_3 = 18114, R_4 = 6297, R_5 = 7917, R_6 = 6297, R_7 = 13080, R_8 = 30239$

Step 3: $L(x) = e^{-x}[R_i \, p(x)]$
$= \sum_{i=1}^{8} e^{-x} \, [R_i \cdot 180 \cdot x^i]$
$= e^{-x}[4282200 \cdot x + 1425060 \cdot x^2 + 3260520 \cdot x^3 + 1133460 \cdot x^4 + 1425060 \cdot x^5 + 1133460 \cdot x^6 + 2354400 \cdot x^7 + 5443020 \cdot x^8]$
$= \sum_{i=1}^{8} e^{-x} \, G_i \, x^i$

Step 4: Apply Mellin Transform on $L(x)$ i.e., $L(x)^* = \sum_{i=1}^{8} G_i \, (s + i - 1)!$

Step 5: Choose $s = 3$ and
we get, $B_1 = 25693200, B_2 = 34201440, B_3 = 391262400, B_4 = 816091200,$
$B_5 = 7182302400, B_6 = 45701107200, B_7 = 854364672000, B_8 = 19751630976000$

Step 6: Compute ciphertext C such that $C_i \equiv B_i \, mod \, 35557$
we get, $C_1 = 21046, C_2 = 31163, C_3 = 28729, C_4 = 22493, C_5 = 1742, C_6 = 15113, C_7 = 9290, C_8 = 11922$

Step 7: Find k_i such that $k_i = (B_i - C_i)/35557$ and $k_0 = 3$ (value of s)
we get, $k_1 = 722, k_2 = 961, k_3 = 11003, k_4 = 22951, k_5 = 201994, k_6 = 1285291, k_7 = 24028030, k_8 = 555492054$

Step 8: Each integer of ciphertext $C_1 = 21046, C_2 = 31163, C_3 = 28729, C_4 = 22493, C_5 = 1742, C_6 = 15113, C_7 = 9290,$ $C_8 = 11922$ is converted to its construct by ASCII character C_1 = 制, C_2 =离, C_3 =瀹, C_4 =埝, C_5 =ぶ, C_6 =瞁, C_7 =口 C_8 =巳 and stored as the ciphertext C = " **制离瀹埝ぶ瞁口巳** "

Alice then sends (k_i, ciphertext C) to Bob.
Bob decrypts the ciphertext using steps as given in method of Decryption.

Step 1: Consider the ciphertext C and key k_i received from the sender

Step 2: Ciphertext C = " **制离瀹埝ぶ瞁口巳** " converted to ASCII values of $C_1 = 21046, C_2 = 31163, C_3 = 28729, C_4 = 22493, C_5 = 1742, C_6 = 15113, C_7 = 9290, C_8 = 11922$

Step 3: Compute $B_i = C_i + (N \cdot k_i)$
we have, $k_1 = 722, k_2 = 961, k_3 = 11003, k_4 = 22951, k_5 = 201994, k_6 = 1285291, k_7 = 24028030, k_8 = 555492054$
we get, $B_1 = 25693200, B_2 = 34201440, B_3 = 391262400, B_4 = 816091200,$
$B_5 = 7182302400, B_6 = 45701107200, B_7 = 854364672000, B_8 = 19751630976000$

Step 4: The polynomial assuming B_i as a coefficient
$25693200 \cdot x + 34201440 \cdot x^2 + 391262400 \cdot x^3 + 816091200 \cdot x^4 + 7182302400 \cdot x^5 + 45701107200 \cdot x^6 + 854364672000 \cdot x^7 + 19751630976000 \cdot x^8$

Step 5: Apply inverse Mellin Transform i.e., $L^*(x) = e^{-x} \sum_{i=1}^{8} B_i \, x^i$
we have, $k_0 = 3$ (value of s)
compute $\sum_{i=1}^{8} \frac{B_i}{(s+i-1)!} = \sum_{i=1}^{8} G_i$ and find R_i as $\frac{G_i}{L}$
we get, $R_1 = 23790, R_2 = 7917, R_3 = 18114, R_4 = 6297, R_5 = 7917, R_6 = 6297, R_7 = 13080, R_8 = 30239$

Step 6: Each integer of R_i is converted into $M_i = R_i^{13} \, mod \, 1147$
we get, $M_1 = 73, M_2 = 110, M_3 = 102, M_4 = 33, M_5 = 110, M_6 = 33, M_7 = 116, M_8 = 121$

Step 7: Each integer M_i are converted to their corresponding ASCII Code values $P_1 = I, P_2 = n, P_3 = f, P_4 = !, P_5 = n, P_6 = !, P_7 = t, P_8 = y$ and hence get the original plaintext = "**Inf!n!ty**"

V. TESTING AND ANALYSIS

Frequency testing and correlation analysis for the proposed SSC-KT and SSC-MT methods are presented in this section.

5.1 Frequency Test

The graphical representation of the frequency distribution for SSC, SSC-KT and SSC-MT is presented, comparing their performance. The x-axis represents plaintext, while the y-axis denotes the frequency level of ciphertext values.

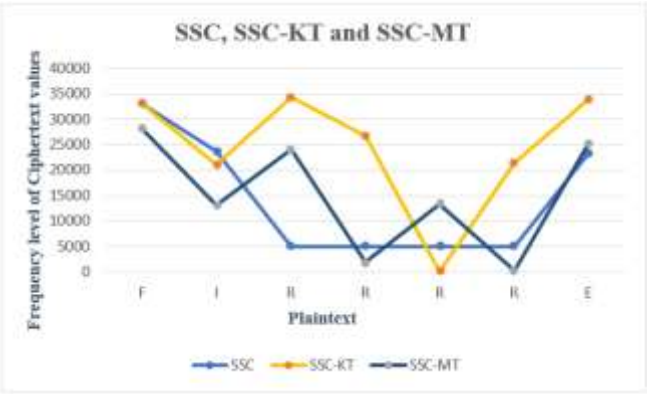

Figure 5.1: Ciphertext frequency distribution of SSC, SSC-KT and SSC-MT

5.2 Correlation Analysis

Correlation coefficients in statistics measure how strongly two variables are related to one another. The plaintext and its encryption are almost the same if the correlation coefficient is approaching 1. Strong encryption is indicated by a number around 0, which indicates that the ciphertext and plaintext are completely different. As a result, smaller correlation coefficient values indicate more effective encryption.

Table 5.1 presents the experimental results of correlation coefficient values for SSC, KT method and proposed method SSC-KT.

Table 5.1: The correlation from plaintext to ciphertext values

Plaintext	Method	Correlation
In$pire	SSC	0.6977
	KT	0.3634
	SSC-KT proposed method	**0.0222**
Devl0per	SSC	0.7125
	KT	0.3388
	SSC-KT proposed method	**0.0976**
Att@ck	SSC	0.3854
	KT	0.8051
	SSC-KT proposed method	**0.0739**

Table 5.2 shows the experimental finding of the correlation coefficient values for SSC, MT method and proposed method SSC-MT.

Table 5.2: The correlation from plaintext to ciphertext values

Plaintext	Method	Correlation
Kn0wledgE	SSC	0.3247
	MT	0.3587
	SSC-MT proposed method	**0.0332**
Authentic	SSC	0.3115
	MT	0.1040
	SSC-MT proposed method	**0.0647**
Mi$si0n	SSC	0.9217
	MT	0.3248
	SSC-MT proposed method	**0.1612**

VI. CONCLUSION

Cryptography is essential for secure data communication. Either Kamal Transform or Mellin Transform is weaker cryptographic approaches as they allow decryption using basic modular arithmetic. This paper introduced SSC-KT and SSC-MT methods, integrating the SSC with Kamal and Mellin Transforms. Unlike the SSC, which maintains the same frequency for repeated characters, the proposed methods vary frequencies, preventing frequency attacks. Correlation tests show that SSC-KT and SSC-MT offer better encryption, with lower correlation values. While SSC may outperform in some cases, the proposed methods enhance data security in communication.

REFERENCES

[1]. Al-Haija, Q. A., Asad, M. M., & Marouf, I. (2018). "A systematic expository review of Schmidt-Samoa cryptosystem", International Journal of Mathematical Sciences and Computing (IJMSC), 4(2), 12-21.

[2]. Ashfaque, J. M. (2019). "The Mellin Transform A Basic Introduction", https://www.researchgate.net/publication/337465283.

[3]. Bisht, N., & Singh, S. (2015). "A comparative study of some symmetric and asymmetric key cryptography algorithms", International Journal of Innovative Research in Science, Engineering and Technology, 4(3), 1028-1031.

[4]. Debnath, L., & Bhatta, D. (2014). "Integral transforms and their applications", CRC press.

[5]. Kahate, A. (2006). Cryptography and Network security.

[6]. Kamal, A., & Sedeeg, H. (2016). "The new integral transform Kamal transform", Advances in Theoretical and Applied Mathematics, 11(4), 451-458.

[7]. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). "Handbook of applied cryptography", CRC press.

[8]. Mittal, A., & Gupta, R. (2019). "Kamal transformation based cryptographic technique in network securing involving ASCII value", International Technology and Exploring Engineering, 8(12), 3448-3450.

[9]. Nagalakshmi, G., Sekhar, A. C., Sankar, N. R., & Venkateswarlu, K. (2019). "Enhancing the data security by using RSA algorithm with application of Laplace transform cryptosystem", International Journal of Recent Technology and Engineering, 8(2).

[10]. Nagalakshmi, G., Sekhar, A. C., Sankar, N. R. (2020). "An Implementation of ElGamal Scheme for Laplace Transform Cryptosystem", International Journal of Computer Science and Engineering (IJCSE), ISSN: 2231-3850, 11(1).

[11]. Paar, C., & Pelzl, J. (2009). "Understanding cryptography: a textbook for students and practitioners", Springer Science & Business Media.

[12]. Santana, Y. C. (2014). "A Cryptographic Scheme of Mellin Transform", arXiv preprint arXiv:1401.1232.

[13]. Stallings, W. (2006). "Cryptography and network security", 4/E. Pearson Education India.
[14]. Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). "A review paper on network security and cryptography", Advances in Computational Sciences and Technology, 10(5), 763-770.
[15]. Thakkar, A. & Gor, R. (2021). "A Review paper on Cryptographic Algorithms and Mathematical Transformations", Proceeding of International Conference on Mathematical Modelling and Simulation in Physical Sciences (MMSPS), Excellent Publishers, ISBN: 978-81-928100-1-0, 324-331.
[16]. Thakkar, A. & Gor, R. (2022). "Cryptographic method to enhance the Data Security using RSA algorithm and Kamal Transform", IOSR Journal of Computer Engineering (IOSR-JCE), 24(3), pp. 01-07.
[17]. Thakkar, A. & Gor, R. (2022). "Cryptographic method to enhance the Data Security using ElGamal algorithm and Kamal Transform", IOSR Journal of Computer Engineering (IOSR-JCE), 24(3), pp. 08-14.
[18]. Thakkar, A. & Gor, R. (2022). "Cryptographic method to enhance Data Security using ElGamal algorithm and Mellin Transform", IOSR Journal of Mathematics (IOSR-JM), 18(6), pp. 12-18.
[19]. Thakkar, A. & Gor, R. (2023). "Cryptographic Method to Enhance Data Security Using RSA Algorithm and Mellin Transform", International Journal of Engineering Science Technologies (IJOEST), 7(2), pp. 63-72.
[20]. Thakkar, A. & Gor, R. (2023). "Cryptographic method to enhance Data Security using RSA algorithm and Sumudu Transform", Quest Journal of Research in Applied Mathematics, 9(4), pp. 48-54.
[21]. Thakkar, A. & Gor, R. (2023). "Cryptographic Method to Enhance the Data Security using ElGamal Algorithm and Sumudu Transform", International Journal for Research in Applied Science and Engineering Technology (IJRASET), 11(7), pp. 853-861.
[22]. Thangavel, M., & Varalakshmi, P. (2016). "Enhanced Schmidt-Samoa cryptosystem for data confidentiality in cloud computing", International Journal of Information systems and change Management, 8(2), 160-188.
[23]. Undegaonkar, H. K., & Ingle, R. N. (2020). "Role of Some Integral Transforms in Cryptography", International Journal of Engineering and Advanced Technology, 9(3).