Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i1.2508

Investigation of Cryptography for Secure Communication and Data Privacy Applications

Sukhveer Singh
Asst. Professor, Department of Mathematics, Graphic Era Hill University,
Dehradun Uttarakhand India

Article Info
Page Number: 551-560
Publication Issue:
Vol. 70 No. 1 (2021)

Abstract
In many applications, secure communication and data privacy are crucially supported by cryptography. The study of cryptography is now essential for creating strong and dependable security systems due to the growing risks to sensitive information in the digital era. The fundamentals of cryptography, its guiding principles, and its useful applications in securing communication channels and preserving data privacy are explored in this research article.Beginning with symmetric and asymmetric encryption techniques, the inquiry first looks at the fundamental ideas of encryption and decryption. It explores the mathematical underpinnings of cryptography, including discrete logarithms, prime numbers, and modular arithmetic, which serve as the foundation for many cryptographic systems.The paper also examines the various cryptographic protocols and algorithms that are frequently used in secure communication systems. It examines well-known encryption algorithms like Elliptic Curve Cryptography (ECC), Rivest-Shamir-Adleman (RSA), and Advanced Encryption Standard (AES). To determine whether a given algorithm is appropriate for a given use case, its advantages, disadvantages, and distinguishing characteristics are examined.The inquiry also looks at other cryptographic methods including digital signatures, hashing, and key management in addition to encryption. In secure communication systems, these methods are essential for guaranteeing data integrity, authentication, and non-repudiation.

Article History
Article Received: *25 January 2021*
Revised: *24 February 2021*
Accepted: *15 March 2021*

Introduction

Secure communication and data privacy have emerged as the two most important problems in an increasingly linked and digital society. Secure lines of communication are used by businesses, governments, and people to send sensitive information while guarding against unauthorised access and data tampering. These issues are addressed and the secrecy, integrity, and authenticity of data are ensured via cryptography, the science of encoding and decoding information [1].

This investigation's goal is to learn more about the field of cryptography and how it's used for secure communication and data privacy. The [2] process of converting plaintext data into ciphertext, which is incomprehensible to unauthorised parties, is known as cryptography. The ciphertext can subsequently be transformed back into its original form by the intended recipients using a corresponding decryption key.The analysis starts by looking at the foundational ideas of encryption and decryption. It [3] examines both symmetric and asymmetric encryption techniques, which use different keys for encryption and decryption respectively. Symmetric encryption algorithms use the same key for both operations. Key management, cryptographic protocols, and

mathematical underpinnings are only a few of the many facets of the study of cryptographic approaches.

Modular arithmetic is one of the basic mathematical ideas that underlies cryptography. Numerous cryptographic activities, such as the creation and modification of encryption keys, are made possible by it. Other [5] crucial elements of cryptographic algorithms like the Diffie-Hellman key exchange and the ElGamal encryption scheme include prime numbers and discrete logarithms.

This inquiry investigates the strengths and limitations of frequently used encryption algorithms in order to get a thorough understanding of cryptography. AES, which is widely used in many applications, provides a high level of security and effectiveness. For secure key exchange and digital signatures, the Rivest-Shamir-Adleman (RSA) technique, which is based on the challenge of factoring big composite numbers, is frequently used. Elliptic Curve Cryptography (ECC), based on the mathematics of elliptic curves, also offers robust security with shorter key lengths than other algorithms [7].

For maintaining [4] data integrity and verification, cryptographic techniques like digital signatures and hash functions are essential in addition to encryption. Digital signatures confirm the legitimacy of communications and the senders' identities, whereas hash functions produce cryptographic hashes of a defined size.This inquiry also discusses the difficulties and developments in the realm of cryptography. Traditional cryptography methods may be under danger as a result of the development of quantum computing, as these systems are capable of breaking many of the current encryption techniques. Post-quantum cryptography is being created to combat this and guarantee long-term security while withstanding assaults from quantum computers.Additionally, the inquiry looks into how cryptography is used in cutting-edge technologies like blockchain, the Internet of Things (IoT), and cloud computing. These areas have particular security needs and depend on cryptographic techniques to protect user privacy and provide secure communications.

I. Related Work

Symmetric encryption and asymmetric encryption, commonly referred to as public-key cryptography, are[9] the two basic categories of cryptography. The same key is utilised in symmetric encryption for both encryption and decryption. Although this kind of cryptography is frequently quicker, secure key distribution is necessary. In contrast, asymmetric encryption employs two sets of keys that are connected mathematically: a public key for encryption and a private key for decryption. Digital signatures, key distribution, and safe key exchange are all made possible by this method.[8] Different cryptographic methods and protocols are used by cryptography to ensure security. The Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and Elliptic Curve Cryptography (ECC) are a few examples of widely used cryptographic algorithms. By encrypting the data, these methods are intended to offer confidentiality, integrity, and the detection of any manipulation [10].

The guidelines[9] and practises for secure network communication are governed by cryptographic protocols, such as the Transport Layer Security (TLS) protocol, Secure Socket Layer (SSL), and Pretty Good Privacy (PGP). The confidentiality and integrity of data conveyed are guaranteed by these protocols, which also create secure connections and verify the persons involved.

Cryptography[11] is a field that is continually changing to meet new problems and dangers. It includes fields like homomorphic encryption, which enables computations to be done on encrypted data without having to decrypt it, and post-quantum cryptography, which tries to create algorithms resistant to attacks by quantum computers.

II. Proposed Method and Cryptographic Algorithm

The suggested encryption algorithm protects personal data using a three-level cypher. Through this compression procedure, the data's information content is maintained while its size is reduced.Basic cryptography mechanism shown in figure 1. The encrypted data undergoes a modification that adds mathematical complexity, making it more difficult to decrypt without the proper decryption keys. The approach improves the security of the encrypted data by using nonlinear equations.The encryption algorithm's third level involves using delta () encoding techniques. The difference or changes between successive values in a sequence are represented using a technique called delta encoding. The algorithm further obscures the encrypted data by using this encoding technique, increasing its resistance to unauthorised access.

The suggested technique tries to offer strong security for personal data by combining these three degrees of encryption. Data size is reduced by the words compression flowchart, mathematical complexity is increased by the transformation into systems of nonlinear equations, and encryption is further strengthened by the delta encoding principles. Together, these tiers function synergistically to protect the integrity and security of personal data.

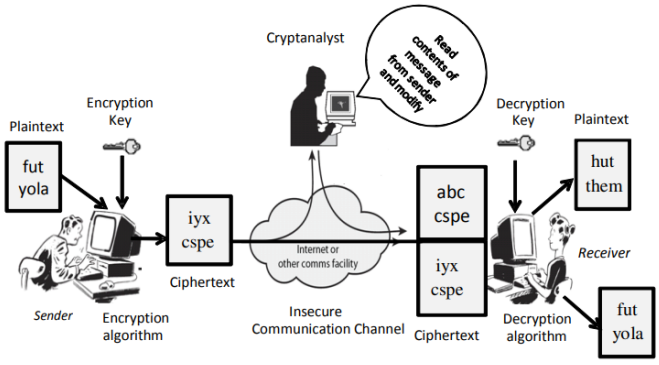

Figure 1: Basic Cryptography encryption and decryption system

Widely[12] used symmetric encryption technique The Advanced Encryption Standard (AES) uses mathematical operations to achieve secure encryption. The AES method can be described by mathematical equations even though it is primarily dependent on a sequence of substitution and permutation operations.

Elliptic curves are used in ECC (Elliptic Curve Cryptography), a public-key cryptographic technique that offers secure data encryption and communication. It is effective in contexts with limited resources because it provides robust security with reduced key lengths. In protocols like TLS/SSL, digital signatures, key exchange, and secure data storage, ECC is frequently employed [13].Elliptic Curve Cryptography, sometimes known as ECC, is a public-key cryptographic procedure that is used to encrypt communications and safeguard privacy. Following are the steps of ECC and the associated mathematical equations:

ECC Algorithm:

Step 1: Generating a Key:

- Decide on an elliptic curve and its base point.
- Pick a random integer (d) that falls inside a particular range for your private key.
- Calculate the public key by multiplying the base point by the private key in a scalar manner, as in Q = d * G, where Q is the public key and G is the base point.

Step 2: Encryption

- Choose an integer (k) at random from a range.
- Calculate the ephemeral public key R = k * G, which is the result of scalarly multiplying the base point by the random number.
- Calculate the shared secret, which is equal to S = k *
- Recipient's Public Key, by multiplying the recipient's public key by a random number.
- Using the proper encoding technique, transform the message to be encrypted into a point on the elliptic curve.
- Calculate the ciphertext by XORing the shared secret's coordinates with the message point's coordinates: Ciphertext = Message_Point S.

Step 3: Decryption

- Retrieve the shared secret by computing the scalar multiplication of the recipient's private key with the ephemeral public key received: S = Recipient's_Private_Key * R.
- Retrieve the original message by XORing the coordinates of the ciphertext with the coordinates of the shared secret: Message_Point = Ciphertext $\oplus$ S.
- Convert the message point back into its original form using the same encoding scheme.

Step 4: Key Aggrement

- Select a random integer (k) within a certain range.
- Compute the shared secret, which is the scalar multiplication of the other party's public key with the random integer: S = k * Other_Party's_Public_Key.

A symmetric [16] key encryption technique that works on 64-bit blocks of plaintext is called the International Data Encryption technique (IDEA). It consists of eight rounds of encryption and employs a 128-bit key. Here is a detailed explanation of how IDEA functions:

Key Expansion:

- Eight 16-bit subkeys (K1 to K8) make up the 128-bit key.
- These subkeys are further expanded to generate 52 round subkeys, each 16 bits in length.

Encryption:

- The 64-bit plaintext block is divided into four 16-bit blocks: P1, P2, P3, and P4.
- The encryption process consists of eight rounds.
- For each round:
- Perform a round key addition: Add the round subkeys (K1-K6 for the first round, K7-K12 for the second round, and so on) to the four plaintext blocks.
- Perform a substitution step: Apply a non-linear substitution function (S-box) to each 16-bit block independently.

- Perform a permutation step: Swap the positions of P2 and P3.
- Perform a modular addition step: For each 16-bit block, add the result of the permutation step to the previous 16-bit block, modulo 2^16.
- Perform a modular multiplication step: Multiply the result of the modular addition by a 16-bit subkey.
- Perform a modular addition step: For each 16-bit block, add the result of the modular multiplication to the previous 16-bit block, modulo 2^16.
- After eight rounds, the resulting four 16-bit blocks are the ciphertext blocks C1, C2, C3, and C4.

Output Transformation:

- The four ciphertext blocks C1, C2, C3, and C4 undergo a final transformation using four additional subkeys (K49-K52).
- For each ciphertext block, perform a round key addition using the corresponding subkey.
- The output of the output transformation step is the final 64-bit ciphertext block.

IDEA is a [15] [18] symmetric encryption technique, which means the same key is used for both encryption and decryption. This is significant information to keep in mind. The round subkeys are applied in reverse order during the decryption process, which uses the same stages as encryption.

Algorithm:

1) Select two 64-bit private keys, K1 and K2, using the random number generation function.
2) K1 Key A = K1 using the IDES algorithm
3) K2 Key B = K2 using IDES Algorithm
4) Compute 128 bit key
   Key: A + B
5) Computer Key Expansion function

The Key expansion function for IDES

```
Key Exp (byte ci[16], w[44])
{
char W
for (i=0; i<4; i++)
W[i] =(c [4*i], c [4*i+1], c [4*i+2], c [4*i+3]);
For (i=4; i<44; i++)
{
Temp = w [i-1];
If (I mod 4 = 0)
Temp = Sub Word (Rot Word (temp)) / Rcon [i/8];
W[i] = w [i-4] / temp;
```

Figure 1(b) Key Expansion pseudo Algorithm for IDES

1. Rot One-byte circular left shifts are applied to a word by Word.Word [A0, A1, A2, A3] from the input example is changed to [A1, A2, A3, A0].
2. Sub Word uses S-box 3 to perform a byte substitution on each input word's byte. Steps 1 and 2's outcome are XORed with Rcon[j], a round constant.

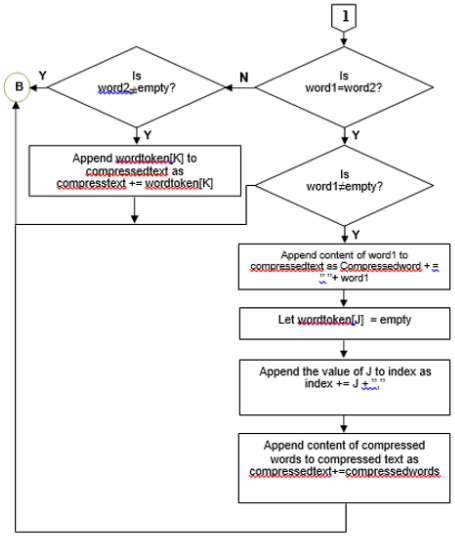

Figure 2: Proposed algorithm flowchart for encryption for nonlinear equation

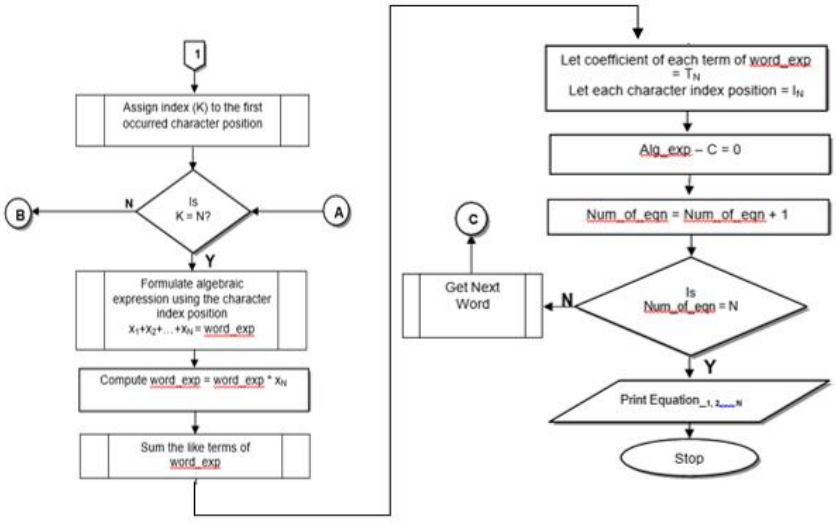

Figure 3: Proposed algorithm Decryption flowchart for nonlinear equation

III. Results and Discussion

Encryption Process:

Explanatory example 1:

We employ the method shown in Figures 2 and 3 to encrypt the message "who is promising who." The ciphertext is produced as a result.

$X_1^2 = X_1^2 + X_1 X_2 + X_1 X_2 = 6$
$X_1^{2+} X_1 X_2 = 3$
$4X_1^2 + 2X_1 X_2 + 3X_1 X_2 = 17$ ----------1(a)

$f(x1, x2, x3)$ = $X_1^2 = X_1^2 + X_1 X_2 + X_1 X_2 = 6$
$X_1^{2+} X_1 X_2 = 3$
$4X_1^2 + 2X_1 X_2 + 3X_1 X_2 = 17$ ----------1(b)

In place of the plaintext "who is promising who," equation (1b) is transformed into a system of nonlinear equations that is sent to the recipient.

Decryption Process:

In place of the plaintext "who is promising who," equation (1b) is transformed into a system of nonlinear equations that is sent to the recipient, for the purpose of this paper,

a. Because doing so would need more iterations to determine, explicit computation of the inversion of Jacobi is avoided.

b. Rather, we use the linear system:

$$x\ (p+1) = xp + \partial p$$

Ddemonstrates the outcome of the proposed algorithms for deciphering the text from the encrypted text (Equation (1b)).

Table 1: Recovering the plaintext for "Kill all Hippopotamuses in the Mississippi River"

Positionof Word s_k	$s_k = v_s + \sum_{n=1}^{k} \delta_x$,where = varkey	m the ble I(R.C)
1	$x_1 = 1 + 76 = 77$	77=w
	$x_2 = 2 + 76 - 10 = 68$	68=h
	$x_3 = 3 + 76 - 10 + 6 = 6f$	6f=o
2	$x_1 = 1 + 68 = 69$	69=i
	$x_2 = 2 + 68 + 9 = 73$	73=s
3		71=p
		70=r
		6ff=o
		6dd=m
		68=i
		71=s
	= 69	69=j
	= 6e	6e=e
		67=n

	$x_1 = 1 + 6d + 4 - 5 - 1 - 3 + 9 - 9 + 3 - 5 = 67$	
4		74=w
		69=h
	$x_3 = 3 + 76 - 10 + 6 = 6f$	6f=j

Table 2: Recover original message from the given ciphertext

Positionof Word s_k	$s_k = v_s + \sum_{m=1}^{K} \delta_x$, Where$s_k$ = varsolution	Fromthe Table 1(R.C)
1	$x_1 = 1 + 42$	43 =C
	$+ 42 + 2e$	72=r
		65=e
	$- 02$	64=d
	$- 02 + 04$	69=i
	$x_6 = 6 + 42 + 2e - 0e - 02 + 04 + 0a$	74=t
2		
		41=A
		2f=/
	$x_9 = 9 + 3a - 11 + 33$	63=c
3	$x_{10} = a + 44$	4e=N
	$x_1 = 1 + 44 + 2a$	6f=o
	$x_2 = 2 + 44 + 2a + 33$	3a=:
	.	.
	.	.
10	$+ 2c$	31=1
	$x_{10} = a + 2c - 04$	32 =2
	$x_8 = 8 + 2c - 04 + 03$	33 =3
	$+ 03$	34 =4
		35 =5

+ 03 + 00	

The characters are transcribed sequentially, maintaining their original order, with spaces placed in between them throughout the decompression process. When an index value newel generate char value that defined as the substitute character is replaced with the appropriate original character. Additionally, to retain legibility and organisation in the decompressed material, a gap is permitted between each printed word.

IV. Conclusion

The importance of cryptographic techniques in protecting sensitive information in today's digital environment has been underscored by the exploration of cryptography for secure communication and data privacy applications. This literature review has shown a number of significant findings.AES, RSA, ECC, and TLS are only a few of the different cryptographic algorithms and protocols that have been investigated. The confidentiality, integrity, authenticity, and non-repudiation of data are all crucially dependent on these methods. For choosing the best cryptographic solutions for particular applications, it is crucial to be aware of each one's advantages, disadvantages, and weaknesses.Future research paths will focus on decentralised systems, privacy-enhancing technologies, and hemimorphic encryption for safe computation. In an increasingly networked and data-driven society, these fields show considerable promise for tackling the difficulties of safe communication and data privacy.Overall, this overview of the literature highlights how crucial cryptography is to maintaining safe communication and data privacy. For researchers, practitioners, and policymakers, it offers a useful resource for comprehending the state, developments, difficulties, and potential future orientations of cryptographic techniques in safeguarding our digital infrastructure and sensitive data.

References:

[1] B. Figg. (2004). Cryptography and Network Security. Internet: http:/www.homepages.dsu.edu/figgw/Cryptography%20&%20Network%2 0Security.ppt. [March 16, 2010].

[2] A. Kahate, Cryptography and Network Security (2nd ed.). New Delhi: Tata McGraw Hill, 2008.

[3] M. Milenkovic. Operating System: Concepts and Design, New York: McGrew-Hill, Inc., 1992.

[4] P.R. Zimmermann. An Introduction to Cryptography. Germany: MIT press. Available: http://www.pgpi.org/doc/pgpintro, 1995, [March 16, 2009].

[5] W. Stallings. Cryptography and Network Security (4th ed.). Englewood (NJ):Prentice Hall, 1995.

[6] V. Potdar and E. Chang. “Disguising Text Cryptography Using Image Cryptography,” International Network Conference, United Kingdom: Plymouth, 2004.

[7] S.A.M. Diaa, M.A.K. Hatem, and M.H. Mohiy (2010). “Evaluating The Performance of Symmetric Encryption Algorithms” International Journal of Network Security, 2010, 10(3), pp.213-219

[8] T. Ritter. "Crypto Glossary and Dictionary of Technical Cryptography'. Internet: www.ciphersbyritter.com/GLOSSARY.HTM , 2007, [August 17, 2009]

[9] K.M. Alallayah, W.F.M. Abd El-Wahed, and A.H. Alhamani."Attack Of Against Simplified Data Encryption Standard Cipher System Using Neural Networks". Journal of Computer Science,2010, 6(1), pp. 29-35.

[10] D. Rudolf. "Development and Analysis of Block Cipher and DES System". Internet: http://www.cs.usask..ca/~dtr467/400/, 2000, [April 24, 2009]

[11] H. Wang. (2002). Security Architecture for The Teamdee System. An unpublished MSc Thesis submitted to Polytechnic Institution and State University, Virginia, USA.

[12] G.W. Moore. (2001). Cryptography Mini-Tutorial. Lecture notes University ofMaryland School of Medicine. Internet: http://www.medparse.com/whatcryp.htm [March 16, 2009].

[13] T. Jakobsen and L.R. Knudsen. (2001). Attack on Block of Ciphers of Low Algebraic Degree. Journal of Cryptography, New York, 14(3), pp.197-210.

[14] N. Su, R.N. Zobel, and F.O. Iwu. "Simulation in Cryptographic Protocol Design and Analysis." Proceedings 15th European Simulation Symposium, University of Manchester, UK., 2003.

[15] C.K. Laudan, and C.G. Traver. E-Commerce .Business .Technology .Society (2nd ed.). New York: Pearson Education, Inc., 2004.

[16] G.C. Kessler. Handbook on Local Area Networks: An Overview ofCryptography. United Kingdom: Auerbach. Available http://www.garykessler.net/library/crypto.html. 2010, [January 3, 2010].

[17] M.A. Yusuf. Data Security: Layered Approach Algorithm. An unpublished MSc Thesis submitted to Abubakar Tafawa Balewa University, Bauchi, Nigeria, 2007.

[18] J. Talbot and D. Welsh. Complexity and Cryptography: An Introduction. New York: Cambridge University Press, 2006