Proceedings of the Third International Conference on Smart Systems and Inventive Technology (ICSSIT 2020)
IEEE Xplore Part Number: CFP20P17-ART; ISBN: 978-1-7281-5821-1

Cryptographic Algorithms to Secure Networks -A Technical Survey on Research Perspectives

Rojasree. V (*Author*)
Department of Computer Science, *Rajah Serfoji Govt. College(A)*
(Affiliated to Bharathidasan University)
Thanjavur-613005, Tamilnadu, India.
rojasree.v@gmail.com

Dr. J. Gnanajayanthi (*Author*)
Department of Computer Science, *Rajah Serfoji Govt. College(A)*
(Affiliated to Bharathidasan University)
Thanjavur-613005, Tamilnadu, India.
jgnanajayanthi@gmail.com

***Abstract*— Cryptology - the art of secret writing is a branch of science with the fundamental objective as "To enable people to communicate securely over a public insecure channel". Cryptology guarantees secure communication. This paper is to make a survey paper on the evolution of cryptographic systems and the cryptanalysis that lead to the failure of each system over time from the classical cryptosystems till modern cryptosystem. The paper also lights on the new research scopes for budding scholars. The survey takes into account the discovery, the acceptance of the system by the society, the drawbacks thus lead to the discovery of the next cryptosystem. This paper outlines a good idea on the earlier cryptosystems and also gives a spark for new research fields that are yet to be touched and discovered.**

Keywords— Cryptography, Cryptanalysis, Classical Cryptosystems, Modern Cryptosystem, ECC, Comparative Analysis of Cryptosystem.

I. INTRODUCTION

The advancement of digital electronics and computer networks has reached such an extent that the extensive use of Internet through wired, wireless and ad hoc networks for communication, remote resource access, any time any place banking transactions have increased the risk factors and the authenticity associated with all the tasks and transactions [1]. The more the advancement in the technologies the more is the risks associated. Till date, cent-percent secure environment is never achieved in any of these advancements. There is always a back door open for hacking and eavesdropping. It has become an unnoticed habit among all the computer-based communication users to use the cryptography. Cryptography is a science that every user in the ICT (Information Communication Technology) world nowadays use even without their knowledge. When a user is authenticated with OTP (One Time Password), when he signs into an email while entering the PIN (Personal İdentification Number) in ATM (Automated Teller Machine) while swiping the credit card and many more occasions cryptography is applied. While pondering on the *evolution of cryptography* it is an astonishing great journey in the life of secret messaging. Many articles prove that secret-keeping was there as early around the paleolithic age onwards [2].

The science of Cryptology deals with cryptography, *Science of keeping secrets secret* and cryptanalysis, *Science of studying attacks against cryptography techniques* [3]. Traditional to modern cryptography algorithms, all use the English alphabets and Arabic numerals both for encryption (a method of hiding the information) and decryption (a method of unhiding the information) since the English language is more flexible than several other languages [4].

The eras of cryptographic methods have given thousands of cryptographic techniques which were considered to be mightier than the just previous best version. But all these are still proving to be vulnerable and have not proved to create a cent-percent secure system. All the best known cryptographic methodologies are crypt-analyzed and proved to be open to risks and flaws. To know the availability of research paths, a detailed literature survey of the history of cryptography is a must.

This paper provides a vertical and horizontal survey of the various techniques used from the ancient times till date. In this survey, section II deals with a brief tour on various technological backgrounds of secret messaging and a list of some of the ancient methods of message hiding is listed. In section III almost all possible cryptographic mechanisms the reason for their invention the flaws in them are discussed briefly. A detailed survey on the symmetric and asymmetric cryptographic mechanisms are reviewed and concise as both these mechanisms go hand in hand in various applications. The challenges faced in these mechanisms kindles the researchers in the network to march towards developing new security algorithms. Section IV gives a brief explanation about the hash function and its types and a few cryptanalysis are enumerated. Section V deals with a detailed research perspective analysis of the cryptographic mechanisms discussed in section IV. Based on section V the future scope in cryptology is discussed and the survey is concluded in section VI.

II. TECHNOLOGICAL BACKGROUND

One way of communicating messages secretly is the message concealment. This kind of message concealment has evidence of use in the 1900BC from the stones carved with ciphertext from Egypt, which is jumbled letters like "In afct, tslil od htsi otayd" for "In fact, still do this today" [5].

The medieval cryptography from 800AD to 1586 was used to communicate about sensitive ruling political or religious topics among people. This period was the time when many cipher codes like caesar cipher, vegineres auto key cipher using monoalphabetic or poly alphabets were formulated [6].

Then for a while, cryptography took a silent pace and after 1800 through world war-I and world war-II cryptography and cryptanalysis took amusing empowerment in the military and Warfield were many machines like Enigma rotor machine (cipher machine used by Germany Army), JN-25 (Japanese Navy cryptography system) etc. were designed for encrypting, decrypting and also for cryptanalysis [5, 6].

From ancient times, saints songs contained the cryptographic schemes. A single couplet of the Thirukural, when read by different people, gives a different meaning to them based on their lifestyle. The great poet Thiruvalluvar hid so much information in a single couplet. The need of the readers was delivered to them when they read the couplets of the poem with their urge in mind [7]. It can be noticed that in the couplets words are broken and separated, or merged with previous or rear words. That was Thiruvalluvar's style of hiding information.

This proves that *cryptography is there from ancient times and is called classical cryptography which requires the entire system to be maintained as a secret between the source and the destination.*

The various terms used in cryptography are (i) *Plaintext:* The ordinary message that is communicated between the sender and the receiver. (ii) *Ciphertext:* The message after converting to symbolic code. This ciphertext is transmitted over the communication channels. (iii) *Encryption:* The technique of changing the ordinary message to ciphertext. (iv) *Decryption:* The technique of changing the ciphertext back to the ordinary text on the receiver side. (v) *Key Size:* To encode and decode a secret is essential, and the length of the key determines the strength of the cryptosystem. the greater the key size the more secure is the system.

Modern cryptography is based on binary sequences of information which is manipulated using some known mathematical algorithms and maintaining the *Secret Key* between the source and the destination [8]. This modern era of cryptography has advanced with many breathtaking techniques and have triumphed a great success still with unseen flaws. These computerized modern cryptography algorithms which are used in all ICT from the ancient to modern information techniques are analysed in Section III wherein the flaws and complaints that were proved are also discussed thus paving a way to new research scope.

III. CRYPTOGRAPHY MECHANISMS

As the technology explodes there is a growing requirement for security too. Cryptography is the linchpin of modern computer and communication technologies. Whatever be the area; e-commerce, medical and health care, data/information storage and access, Internet of Things (IoT), banking or simple messaging, it requires (i) *Integrity* (the sender and receiver must be confident that the messages are not modified deliberately or accidentally during transmission), (ii) *Data-Authentication* (origin of the information must be known by the receiver), (iii) *Entity-Authentication* (the sender and the receiver must be able to identify each other), (iv) C*onfidentiality* (the secrecy must be preserved between the sender and the receiver) and (v) *Non-Repudiation* (sender should not be able to later deny that he has not sent the message). These are considered the main objectives of cryptography.

Based on this feature, modern cryptography is classified into two categories [1] as (i) *Symmetric Cryptography* and (ii) *Asymmetric Cryptography*. In symmetric cryptography, a secret key is common to the sender and the receiver. In asymmetric cryptography, a pair of keys is used between sender-receivers. One key is the public key, used by the sender to encrypt the message and the other key is a secret key with which the decryption is done at the receiving end. A detailed discussion of these types of cryptosystems is explained in Section 3.1 and Section 3.2.

3.1. Symmetric Cryptography

Symmetric cryptography is a classical cryptography mechanism [9] in which the message to be communicated called as *plaintext* (M) is converted into a meaningless format called *ciphertext* (C). In symmetric cryptography, the same key is used to encrypt and decrypt the message and is shared between the sender and receiver. If the encryption function is implemented on fixed-size blocks, the scheme is called a Block *cipher* and if the encryption function is implemented on streams of bits of information, it is called a Stream *cipher.*

3.1.1. Stream Cipher

The survey on stream ciphers included several mechanisms that have been proposed and few of the noteworthy are Vernam's Cipher, AE5/1,2, RABBIT, RC4 and Turing. Out of these, Vernam's cipher is considered strong as it did not retain the output text and multiple messages produced the same M.

A. Vernam's One-Time Pad.

In 1917 Gilbert Vernam invented and patented this cipher from AT&T Lab [12,13]. Vernam's One-Time Pad (OTP) is considered as the strongest algorithm ever known then. The cryptanalysis of this scheme proved that the padding bit used for XORing with the plaintext must be used only once and then discarded. Reusing the padding bit is meaningless, and so it is called OTP. *However, exhibiting the vulnerability of reusing the key more than once Vernam's One Time Padding lead path for the next new innovative cipher mechanism.*

B. RC Algorithms

RC algorithms, stand for Rivest's Cipher / Ron's Code, developed by Ron Rivest, are a set of algorithms that have improved versions from RC1 namely, RC1, RC2, RC3, RC4, RC5, and RC6. Of them, RC1 and RC3 were not released [14]. RC2, RC5, RC6 are block ciphers which are

briefed in Section 3.1.2.

RC4 is the most widely used stream cipher also known as Alleged RC4(ARC4), developed in 1984 (before RC5 and RC6) and was used secretly by the NSA until 1994. RC4 supports key sizes between 8 and 2,048 bits [15]. RC4 is remarkable for its simplicity and speed in software multiple vulnerabilities made it insecure [16].

C. Rabbit

RABBIT is a stream cipher, developed by Martin Boesgaard et.al [17] and presented in Fast Software Encryption Workshop in 2003. The core portion of this cipher is a bitstream generator, encryption 128bits in every iteration.

D. VEGINÈRE CIPHER

Veginère cipher is a polyalphabetic stream cipher in which a message is encrypted using a series of interwoven letters of a keyword. Veginere cipher is easily broken by kasiski examination or Fiedman test in which the key length is easily determined. The letter frequency analysis also led to breaking the Veginère cipher more easily by analyzing the cipher text [18].

3.1.2. Block Cipher

Block cipher is a symmetric encryption scheme defined as $\mathbf{M = C = \{0,1,\}^n}$, where cipher block length n, fixed key K, plaintext M and ciphertext C. The function of a block cipher is referred as E(Encryption): M*K ☢C. The block cipher encrypts messages to produce ciphertext of the same size. For every small change in the message a new cipher text of fixed length is produced.

The various modes of operations in block cipher are: (i)*Electronic Code Book Mode (ECB)* where each block of M is encrypted separately, (ii)*Cipher Block Chaining Mode (CBC)* in which an Initialization Vector (IV) a random value is chosen is first Exclusive-ORed (XORed) with the M, in the first round, and the forthcoming rounds take C of the previous round is taken for XORing, (iii) *Cipher Feedback Mode (CFB) is different from the previous two modes M never enters the encryption algorithm at all* (iv) *Output Feedback Mode (OFB)* is similar to CFB as M never goes into the encryption algorithm but IV is given before XORing with the M, (v)*Counter Mode (CTR)*where every encryption operation is completely separate and useful for parallelization of encryption, (vi) *Galois Counter Mode (GCM)* is differing in two ways nonce field is elimination and using the Message Authentication Code(MAC) to ensure that the message has not tampered in the transit [19].

The various block cipher schemes are (i) Digital Encryption Standard (DES), (ii) Blowfish, (iii) E-DES, (iv) IDEA, (v) CAST, (vi) MARS, (vii) RC2, (viii) RC5, (ix) RC6, (x) TripleDES (TDES), (xi) Advanced Encryption Standard (AES) (xii) Twofish and (xiii) Serpent and these are briefed as follows.

A. Digital Encryption Standard (DES)

Horst Feistel designed DES at IBM in the 1970s [20, 21]. In the 1990s the DES was widely used in Governments, bank and commercial applications as a basis for secure and authenticated processes. In the DES algorithm, the size of M, C, are 64-bits and key is 56-bits. *However, in 1999, the Internet and worldwide network with plenty of computers were able to break DES due to small key size and found a key in 22hours and 15 minutes* [21].

B. Blowfish

Blowfish is a 64bit cipher, developed by Bruce Schneier in 1993, intended as an alternate to the vanishing DES [22, 23]. *The announcement of AES by NIST and the vulnerability of Blowfish to birthdayattack made blowfish unnoticed.*

C. Educational-DES (E-DES)

EDES is used as a support for DES before TDES was found [24]. *E-DES has larger key, block size and F function with enhanced key program and complicated permutations.*

D. International Data Encryption Algorithm (IDEA)

IDEA is introduced by James Massey in 1991 [25] and takes a 64-bit input and performs 8 identical rounds with a 28-bit key. However, *IDEA was broken using meet-in-the-middle attack and bicliques attack* [26, 27].

E. CAST

CAST is based on DES substitution permutation invented by Carlisle M. Adams in 1996. CAST-128 or CAST5 is a 12 or 16 round, 64-bit block-sized Feistel network with a key size between 40 to 128bits. CAST is prone to meet-in-the-middle attack, brute-force attack, linear, differential and linear-difference cryptanalysis[28].

F. MARS

MARS, developed by IBM to take part in NIST's AES competition in 1999 [29, 30]. *The failure of MARS is the long runs of ones and zeros that may be prone to attacks. In 2004 John Kelsey and Bruce Schneier crashed MARS using meet-in-the-middle attack by cracking 21 out of 32 rounds.*

G. RC2

RC2 is a 64-bit cipher with variable key size up to 1,024-bits, developed in 1987 [31] and performs 18 rounds with 16 rounds of one type and 2 rounds of another type of unbalanced feistel network. *RC2 is vulnerable to related-key attacks using 2^{34} chosen plaintexts.*

H. RC5

RC5 is a 32/64/128 bit cipher, variable key size and number of rounds; developed in 1994 to overcome the drawbacks in RC4 [32]. *However, RC5 is subject to Brute force and differential attacks.*

I. RC6

RC6, a proprietary algorithm patented by RSA security, is a fixed cipher of 128-bit, based on RC5; developed in 1997, with variable key size 128 / 192 /256-bits [33]. *However, the royalty issues made RC6 a loser in the AES competition.*

J. Triple-DES (TDES)

DES was critically analysed by W. Diffie et. al and suggested using DES in multiple encryption modes [34]. *In 1997, NIST called for developing successors of DES with block size 128-bits. Out of the several proposals,*

NIST finally declared Rijndael cipher as the proposed Advanced Encryption Standard (AES) in 2000 [19].

K. Advanced Encryption Standard (AES)

15 were selected for the final selection among several proposals, from the Call-for proposals for the successors of DES by NIST in 1997. Rijndael, MARS, RC6, Serpent, and Twofish were the top 5 in the final list. Rijndael, Serpent and Twofish were tried [35]. In 2000, Rijndael was announced as the winner of the final selection. The new AES was declared [36], used 128/192/256 bits key.

L. Twofish

Twofish, proposed by Rivest et. al, one of the finalists of AES was vulnerable to birthday attacks [37]. *The s-box key database maintained itself as a flaw* [38].

M. Serpent

The serpent with 128/192/256 bits key, designed to process 32-bits in parallel, with 16-rounds to fight against known attacks and opted for 32-rounds for future unknown attacks. Thus making *Serpent a bulky mechanism when compared to Rijndael* [38].

The vulnerability of the symmetric algorithm is the single key shared between sender-receiver if breached, the entire system breaks. This leads to a requirement of a new mechanism, to have more than one key. This is later called an asymmetric algorithm.

3.2. Asymmetric Cryptography

The small size of the keys and the confidentiality of sharing the key among the Sr-Rr raised a new scheme of a cryptosystem. To implement digital signatures and confidentiality, every user (Sr or Rr) maintained a secret key known only to himself and another public key (PK) shared to everyone [39]. So until and unless the secret key is known, no one could decrypt the message. The basic requirement of public-key cryptography is a family of functions so that each and every function f could be computable by an efficient algorithm. The function f should have a secret information *trapdoor information*) to be kept secret so that the inverse of the function f is efficiently computable at the same time computation of the preimage of f must be infeasible and are called *one-way functions (trapdoor function).*

The literature survey included several algorithms and some of the noteworthy are Diffie Hellman Algorithm (DHA), RSA (Rivest, Adi Shamir, Leonard Adleman), ECC (Elliptic Curve Cryptography) in this section.

A. Diffie Hellman Algorithm (DHA)

In 1976, Diffie et. al introduced DHA algorithm, the strongest method and widely used in RSA and ECC by generating secret and public keys[8].

B. RSA (Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman)

RSA was the first asymmetric algorithm described in 1977 based on the difficulty in factoring the product of 2 big prime numbers [39]. RSA, a trustworthy algorithm, was put to strong cryptanalysis and approved as a reliable algorithm to date. The difficulty in factoring the large numbers is the strength of RSA [42, 43]. *The various other attacks include common modulus attack, low-encryption-exponent attack, small message space attack and attack on encryption and signing with RSA* [44].

C. ECC (Elliptic Curve Cryptography)

Victor Miller et. al proposed ECC, introducing elliptic cubic curves (supersingular curves), functions to create public and private keys and minimized attacks by producing different curves [40, 41]. *Whenever anomalous curves appear in sub-exponential time, attacks occur* [45, 46, 47]. NIST declares the anomalous curves (*which are to be tested and avoided*) that are not good for usage in cryptography[48]. The ECC key size is the least of all the methods in the literature.

The asymmetric algorithms require a broad use of assets for a network user and they are suitable for bulk messages. If these algorithms are used for small messages such as password, Personal Identification Numbers (PIN), which is expensive. Despite known attacks of asymmetric algorithms these algorithms can be nominal to most of the applications.

IV. HASH FUNCTIONS

Cryptographic hash functions are the transformations that take an input of the variable size and return a fixed-size string, called a hash value/hash code/Message Digest (MD) as output. Cryptographic hash functions assure data integrity by means of message integrity checks, to verify digital signatures. In the literature, it is observed that several algorithms are proposed using hash functions and remarkable are Tiger, xxhash, RipeMD, MD5 and Secure Hash Algorithm (SHA). MD5 and SHA are briefed here.

MD5: Message Digest 5 hash function takes as input a string of information and encodes it into a 128-bit fingerprint. The MD family consists of hash functions MD2, MD4, MD5 and MD6. MD5 is often widely used as a checksum to verify data integrity. *MD5 is a very old algorithm and suffers from extensive hash collision vulnerabilities. In 2004, an analytical attack was reported to be successful in just an hour using a computer cluster. This attack resulted in the compromise of MD5 and is no longer recommended for use*[62].

A. SHA

SHA takes an input and produces a 160-bit message digest that is 20byte long. SHA is designed by the United States National Security Agency (NSA). The family of SHA includes four SHA algorithms as SHA-0, SHA-1, SHA-2 and SHA-3. SHA-0 was published by NIST in 1993 and had few weaknesses and so did not become popular. SHA-1 is the most widely used hash function and is employed in several applications and protocols including Secure Socket Layer (SSL) security. SHA-2 was designed with four further variants as SHA-224, SHA-256, SHA-384 and SHA-512 based on the number of bits in their hash value. *SHA-2's basic design is still like SHA-1 and hence NIST called for new competitive hash function designs*[63].

Birthday attacks. One of the major issues in the hash function is how large to choose the parameter *n* is obtained by the birthday attack [64]. The birthday attack is based on the concept that the probability of two persons with the same birthday in a group with more than 23 members is greater than (1/2).

V. Cryptography – Research Perspectives

Cryptography from the Paleolithic age till today has travelled a long way and many new cryptographic inventions and mechanisms are proved the best and later crypt analyzed to exhibit the weakness of the so-called best-known mechanism. The block diagram below summarizes the classifications and the various cryptography mechanisms that are taken into consideration in this literature survey. To summarize the science of information hiding- "Cryptography"- can be broadly classified into two categories as symmetric and asymmetric cryptography based on the common secret key or the public and private key. The hash function is used in many places where storing data to the database is used in digital signatures, login password storage and many more. All the cryptographic methods as in figure Figure 1. discussed in this paper have its pros and cons and are still in use in some place or other. This survey is meant to have a detailed awareness about what happened in the entire journey of cryptography so far and thus analyze the possible research perspectives. The various cryptography algorithms are classified and discussed and a detailed study of those algorithms can be compared for research issues and challenges for future research works.

A. Recent Cryptographic Research Scenario

The recent mesh of networking and communication technologies deal with various diverse types of data, machines, application complexities etc. All these require confidentiality, integrity, security and authentication. The need for encryption and the usage of a combination of two or more types of the above said encryption may be required to achieve this. As the days go, the security mechanisms need to be updated, since there is a possibility that the attackers could find a back-door to break the security mechanisms implemented. Hence, the very idea of security is itself a huge area of researching any field of choice. As discussed in the above sections, the various techniques have pros and cons. Now according to the current trend, the issues of implementing ECC is considered as the best method.

There are many papers on the comparative analysis of the above discussed cryptographic schemes [47, 48, 49]. The ECC is considered the best among all the above-mentioned techniques mainly because of its smaller key-size. The smaller key size of ECC makes its computational cost very less and thus enhances its application in areas where memory and power consumption is of greater consideration. Many research scholars have contributed their work to check the performance analysis of ECC on various platforms like Tiny-OS-TOSSIM [50], Kerberos of Athena project at Massachusetts Institute of Technology [48], in Wireless Body Area Networks (WBAN) [51], on Voice Over Internet Protocol server (VOIP) [52], In Satellite-based multicasting [53], in e-commerce application and in areas where memory availability is very limited [54] and the list goes on. Thus a new area of interest could be chosen and research could be carried out to provide a performance benchmark in that area.

Moreover, security means not just implementing an Encryption-Decryption algorithm. The security provided by the cryptography mechanism will be successful, if and only if, some protocols are conserved in that system. Therefore, there are enormous opportunities to design protocols to suit the area of implementation of the security measures as contributed in the references [55, 56, 57, 58]. The reference [59, 60] demonstrates clearly, of how the currently used ECC based protocols are vulnerable to attacks. In [61] of Junfen et. al, a new speed record for FPGAs (Field Programmable Gate Arrays- an IC-based implementation) in cracking ECC was reported. It is proved that the elliptic curve numbered ECC2k-130 which was projected as a challenge of Certicom Corp (A giant elliptic curve cryptography security solutions provider) can be cracked by using 128 FPGA in around $2^{58.7}$ iterations in one year.

B. Research Challenges

The exploding wireless industries lead to a need for a full and efficient public key infrastructure for secure web transactions and secure messaging. Even though ECC is considered the best for over a decade, the idea of ECC is implemented on the older version as Elliptic Curve Diffie-Hellman Algorithm (ECDHA) and Elliptic Curve Digital Signature Algorithm (ECDSA), thus the high-security confidence provided by ECC is mainly because of the discrete logarithm problem that the generation of a point on the elliptic curve by either repeated addition or doubling is easy in the forward direction but almost infeasible in the reverse direction. There is a possibility that an exhaustive function could break the keys of ECC. Moreover, different surveys prove that the various attacks like Man-In-The-Middle attack, clogging attack, database attack, and some of the flaws of the already proved-secure protocols are also possible while using ECC. This leads to scope and necessity to develop a new cryptography mechanism/scheme which could be stronger than ECC and more resistant to the so long proved attacks.

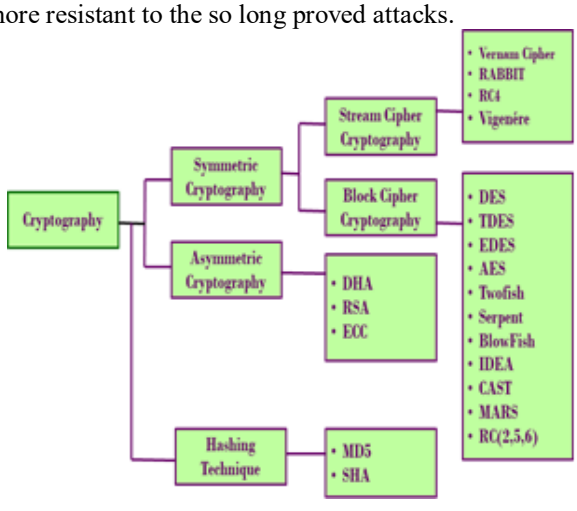

Figure 1: Classification of Cryptography

VI. Conclusion And Future Research Work

The overview of the literature of symmetric, asymmetric and hashing algorithms in this paper has paved a way for enormous research directions and kindled research interests in the domain of Cryptography. Based on the calibre of the researcher, the problems could be chosen. The various opportunities and directions can be put in a nutshell as follows. (i) Choose a platform or application area where ECC has not yet reached; monitor ECC and its breakthroughs. (ii) Design a new protocol to a chosen platform such that the above-said attacks are also taken into consideration. (iii) Design a new algorithm from the core that can prove to be a better algorithm than the ones exıstıng so far. Our further research work is focussed on to design and develop a new cryptography algorithm in the perspectives of new, novel and unique one, apart from the concepts of symmetric/asymmetric/ hashing algorithms.

Acknowledgment

The authors sincerely express their special thanks and sincere gratitude to TamilNadu State Council for Higher Education (TNSCHE) and Department of Science and Technology (DST), India, for sponsoring this research work.

References

[1] A. M. Qadir and N. Varol, "A Review Paper on Cryptography", 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, PP:1-6, @ IEEEXplore DOI: 10.1109/ISDFS.2019.8757514.

[2] Vijaya Ramaswamy, “Historical dictionaries of peoples and cultures”, e-ISBN 9781538106860, Rowman & Littlefield, 2017.

[3] William Stallings, "Cryptography and Network Security Principles And Practice", Prentice Hall, 5th edition, 2016.

[4] Norman L.Biggs, “Codes: An Introduction to Information Communication and Cryptography”, Springer book, ASIN: B00FBSSTP4, Edn. 2008.

[5] Evolution of Cryptography. @url: https://sherpasoftware.com/blog/the-evolution-of-cryptography/ Last visited on 21-03-2020

[6] Mohd Zaid Waqiyuddin Mohd Zulkifli, “Evolution of Cryptography”, 17 January 2007 @url http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.698.2641&rank=190.

[7] "Gnana Thiruvadi" monthly magazine September 2012, Registered with the registrar of newspapers for india under no. TNTAM18193-160708., Regd. No. SP. SRM/L/RNP/08/2012-14.

[8] W. Diffie and M. Hellman, "New directions in Cryptography", In ``IEEE *Transactions on Information Theory*, ISSN:0018-9448 Vol. 22, No. 6, PP: 644-654, Nov-1976. @IEEEXplore DOI: 10.1109/TIT.1976.1055638

[9] S. Vollala, V. V. Varadhan, K. Geetha, N. Ramasubramanian, "Efficient modular multiplication algorithms for public key cryptography", In the Proceedings of the IEEE International Advance Computing Conference (IACC), Gurgaon, 2014, E-ISBN: 978-1-4799-2572-8,PP:74-78, @IEEEXplore, DOI: 10.1109/IAdCC.2014.6779297.

[10] Sandeep Tayal, Nipin Gupta, Pankaj Gupta, Deepak Goyal, Monika Goyal, “A Review Paper on Network Security and Cryptography”, In: Advances in Computational Sciences and Technology, Research, India, ISSN 0973-6107, Vol-10, No. 5, PP: 763-770, 2017.

[11] Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, “Handbook of Applied Cryptography”, CRC Press LLC, ISBN: 0-8493-8523-7, 1997.

[12] Vernam Cipher a perfect Cipher. Last Visited On 20-December 2017.@. url: http://www.cs.miami.edu/home/burt/learning/Csc609.051/notes/02.html.

[13] https://patents.google.com/patent/US1310719

[14] Andrei Popov, “Prohibiting RC4 Cipher Suites”, RFC 7465, February 2015, DOI:10.17487/RFC7465

[15] Allam Mousa, Ahmad Hamad, "Evaluation of RC4 Algorithm for Data Encryption", In the International Journal of Computer Science & Applications, ISSN 0972-9038, Vol.3, No.2, PP:44-56, June 2006.

[16] Sheetal Charbathia, Sandeep Sharma, "A Comparative Study of Rivest Cipher Algorithms", In the International Journal of Information & Computation Technology, ISSN 0974-2239, Vol.4, No.17, PP:1831-1838, 2014. http://www.ripublication.com/irph/ijict_spl/ijictv4n17spl_13.pdf

[17] Boesgaard, Martin, Vesterager, Mette, Zenner, Erik. “The Rabbit Stream Cipher”, 2008. DOI:10.1007/978-3-540-68351-3_7

[18] Bruen, Aiden A, Forcinito, Mario A., “Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century”, John Wiley & Sons. 2011, ISBN 978-1-118-03138-4.

[19] Sultan Almuhammadi, I. Al-Hejri, "A comparative analysis of AES common modes of operation”, In the Proceedings of the 30th Canadian Conference on Electrical and Computer Engineering (CCECE), E-ISBN:978-1-5090-5538-8, PP:1-4, @ IEEEXplore, DOI:10.1109/CCECE.2017.7946655

[20] Horst Feistal, “FIPS46: Data Encryption Standard”. In: Federal Information Processing Standards Publication 46, U. S. Department of Commerce / National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1977.

[21] D. Coppersmith, "The Data Encryption Standard (DES) and Its Strength Against Attacks", IBM Journal of Research and Development, ISSN: 0018-8646, PP: 243-250, May 1994.

[22] A. Mousa, "Data Encryption Performance based on Blowfish", In the Proceedings of the 47th International Symposium on ELMAR, Zadar, 2005, pp. 131-134, @ IEEEXplore, DOI: 10.1109/ELMAR.2005.193660

[23] T. Nie, T. Zhang, "A Study of DES and Blowfish encryption algorithm," In the Proceedings of the IEEE Region 10 Conference on TENCON, Singapore, PP:1-4, 2009, @ IEEEXplore, DOI:10.1109/TENCON.2009.5396115

[24] Omar G. Abood, Shawkat K. Guirguis,"A Survey on Cryptography Algorithms", In the International Journal of Scientific and Research Publications, ISSN 2250-3153, Vol.8, Issue.7, PP:495-561, DOI:10.29322/IJSRP.8.7.2018.p7978

[25] Biham, Eli, Dunkelman, Orr; Keller, Nathan; Shamir, Adi, "New Attacks on IDEA with at Least 6 Rounds", In the Journal of Cryptology, Vol. 28, Issue.2, ISSN 0933-2790, PP:209–239, 2011, DOİ:10.1007/s00145-013-9162-9.

[26] Khovratovich, Dmitry; Leurent, Gaëtan; Rechberger, Christian, “NARROW- Mobile Computing and Communications, Dallas, Texas, ISBN-10: 0-8493-3833-6 Journal of Designs, Codes and Cryptography, ISSN:0925-1022, Vol.12, PP:283–316, 1997. https://doi.org/10.1023/A:1008229029587

[27] B. Preneel, A. Bosselaers, V. Rijmen, B. Van Rompay, L. Granboulan, J. Stern, S. Murphy, M. Dichtl, P. Serf, E. Biham, O. Dunkelman, V. Furman, F. Koeune, G. Piret, J-J. Quisquater, L. Knudsen, H. Raddum, "Comments by the NESSIE Project on the AES Finalists", NIST, 2000.

[28] John Kelsey and Bruce Schneier, "MARS Attacks! Preliminary Cryptanalysis of Reduced-Round MARS Variants" In the proceedings of the Third AES Candidate Conference April 2000, pp. 169–185., @url https://www.schneier.com/academic/paperfiles/paper-mars-attacks.pdf

[29] R. Rivest, "A Description of the RC2(r) Encryption Algorithm", Request for Comments (RFC): 2268, Category: Informational, March 1998, https://dl.acm.org/doi/pdf/10.17487/RFC2268

[30] Ronald L.Rivest, “The RC5 Encryption Algorithm”, In the Proceedings of the Leuven Workshop on Fast Software Encryption, @ Springer Berlin Publishers, e-ISBN:978-3-540-47809-6, Vol.1008, PP:86-96, 1995, DOI:https://doi.org/10.1007/3-540-60590-8

[31] Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, Y.L. Yin, "The RC6 Block Cipher", Version 1.1, M.I.T. Laboratory for Computer Science, and RSA Laboratories, August 1998, https://people.csail.mit.edu/rivest/pubs/RRSY98.pdf

[32] D. Coppersmith, D. B. Johnson, S. M. Matyas, "A Proposed Mode for Triple-DES Encryption", In IBM Journal of Research and Development, Vol. 40, No. 2, PP:253-262, March 1996, DOI: 10.1147/rd.402.0253

[33] James Nechvatal et.al, "Status report on the first round of the development of the development of the Advanced Encryption Standard", In the Journal of research of the National Institute of Standards and Technology, Gaithersburg, MD 20899-0001, Vol.104, No.5, PP:435-459, 1999.

[34] Joan Daemen, Vincent Rijmen, "AES submission document on Rijndael", 1999.

[35] AES: The Advanced Encryption Standard, visited on 21-Mar-2018, @url: https://competitions.cr.yp.to/aes.html

[36] Chowdhury, Z. J., Pishva, D., Nishantha, G. G. D, "AES and Confidentiality from the Inside Out", In the Proceedings of the 12th International Conference on Advanced Communication Technology (ICACT), ISBN: 978-1-4244-5427-3, PP:1587-1591, 2010. @IEEEXplore

[37] Rivest, Ronald L., Adi Shamir, Len Adleman. "A method for obtaining digital signatures and public-key cryptosystems", In the Journal of Communications of the ACM, ISSN :00010782 , Vol.21. Issue.2, PP: 120-126, 1978. https://doi.org/10.1145/359340.359342

[38] Miller V.S., "Use of Elliptic Curves in Cryptography", In the Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (CRYPTO '85), @ Springer Lecture Notes in Computer Science on Advances in Cryptology, Williams H.C. (eds), ISBN: 978-3-540-39799-1, Vol. 218, PP:417-426, 1985. https://doi.org/10.1007/3-540-39799-X_31.

[39] N. Koblitz, "Elliptic Curve Cryptosystems", In the Journal of Mathematics of Computation, ISSN 1088-6842(online), Vol. 48, No. 177, PP: 203-209, 1987.

[40] Satoh. T., Araki. K, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves", Available from https://www.semanticscholar.org/paper/Fermat-Quotients-and-the-Polynomial-Time-Discrete-Satoh-Araki/c9c29b54acc7932cc7e788e3ead312b23274c7ad#paper-header, 1998.

[41] Kocher Paul C, "Timing Attack on Implementations of Diffie-Hellman, RSA, DSS and other systems", In the Proceedings of the Annual International Cryptology Conference (CRYPTO '96), @Springer Berlin Heidelberg Lecture Notes in Computer Science book series, ISBN-978-3-540-68697-2, Vol.1109, PP: 104-113, 1996.

[42] Majid Bakhtiari, Mohd Aizaini Maarof, 2012], "Serious Security Weakness in RSA Cryptosystem". In the Journal of International Journal of Computer Science Issues (IJCSI), ISSN (Online): 1694-0814, Vol. 9, Issue 1, No 3, PP: 175, 2012.

[43] Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press LLC, ISBN: 0-8493-8523-7, 1997

[44] Menezes. A. J, Okamoto. T, Vanstone. S, "Reducing elliptic curve logarithms to logarithms in a finite field", In the Proceedings of the 23rd annual ACM symposium on Theory of computing, ACM Press, ISSN: 0018-9448, Vol.39, Issue-5, PP:1639-1646, 1993.

[45] Semaev. I. A., "Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p", In the Journal of Mathematics of Computation, ISSN 1088-6842(online), Vol. 67, No. 221, PP: 353-356, 1998.

[46] Brown M. et. al, "Software Implementation of the NIST Elliptic Curves Over Prime Fields", In the Proceedings of the International conference on RSA (CT-RSA 2001), @Springer Lecture Notes in Computer Science on Topics in Cryptology, Naccache D. (eds), Berlin, Heidelberg, e-ISBN: 978-3-540-45353-6, Vol. 2020, PP: 250–265, 2001, DOI: https://doi.org/10.1007/3-540-45353-9_19.

[47] E.Thambirajah, G.Ramesh, Dr.R.Umarani, "A survey on various most common encryption techniques", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 22776451, Vol 2, Issue 7, PP:226-233 , July 2012.

[48] Najmus Saquib-Ummer Iqbal, "Security in Wireless Sensor Networks using ECC", In the Proceedings of the IEEE International Conference on Advances in Computer Applications (ICACA), @IEEEXplore ISBN: 978-1-5090-3770-4, PP:270-274, 2016.

[49] E. Pavithra, F. Anishya, M. Nivetha Kumari, "Elliptic Curve Cryptography Based Security Enhancement for Wireless Body Area Network System". In the Asian Journal of Applied Science and Technology (AJAST), ISSN : 2456-883X, Vol-1, Issue- 5, PP:142-146, June 2017.

[50] T. Subashri, Arjun A, Ashok S, "Real Time Implementation Of Elliptic Curve Cryptography Over a Open Source VOIP Server", In the Proceedings *Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, IEEE, Electronic ISBN: 978-1-4799-2696-1, PP: 1-6, 2014, **DOI:** 10.1109/ICCCNT.2014.6963029.

[51] Attila Altay Yavuz, Fatih Alagoz, Emin Anarim, 2006, "A New Satellite Multicast Security Protocol Based on Elliptic Curve Signatures". In the Proceedings of the Information and Communication Technologies (ICTTA 06), IEEE, ISBN: 0-7803-9521-2, PP: 2512-2517, 2006.

[52] Junfeng Fan, Miroslav Knezevic, Dusko Karaklajic, 2009, "FPGA-based Testing Strategy for Cryptographic Chips: A Case Study on Elliptic Curve Processor for RFID Tags". In: On-Line Testing Symposium, IOLTS 2009. 15th IEEE International, ISSN: 1942-9398, PP:189-191, 2009.

[53] M. Aydos, B. Sunar and Ç. K. Koç, "An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication", In the Proceedings of the 2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Dallas, Texas, ISBN-10: 0-8493-3833-6 1998.

[54] C. Sajeev, G. Jai Arul Jose, 2010 "Elliptic Curve Cryptography Enabled Security for Wireless Communication". In: International Journal on Computer Science and Engineering (IJCSE), Vol. 02, No. 06, PP:2187-2189, 2010.

[55] Najmus Saquib, "Key Exchange Protocol for WSN Resilient against Man in the Middle Attack", In: IEEE International Conference on Advances in Computer Application (ICACA), ISBN: 978-1-5090-3770-4, PP:265-269, 2016.

[56] Binod Vaidya, Dimitrios Makrakis, Hussein T. Mouftah, "Authentication Mechanism for Mobile RFID based Smart Grid Network", In: Electrical and Computer Engineering (CCECE), In the Proceedings of the IEEE 27th Canadian Conference, Toronto, Canada, ISSN: 0840-7789, PP:1-6, 2014.

[57] Swapnoneel Roy and Chanchal Khatwani, "Cryptanalysis and Improvement of ECC Based Authentication and Key Exchanging Protocols", In: MDPI Journal- Cryptography, 2017.

[58] Jen-Ho Yang and Chin-Chen Chang, "Cryptanalysis of ID-Based Digital Signature Scheme on Elliptic Curve Cryptosystem", In the Proceedings of the IEEE Eighth International Conference on Intelligent Systems Design and Applications (ISDA), ISBN 978-0-7695-3382-7, PP:3-5, 2008,

[59] Jufeng Fan, Daniel V. Bailey, Lejla Batina, Tim Güneysu, Christof Paar and Ingrid Verbauwhede, "Breaking Elliptic Curve Cryptosystems using Reconfigurable Hardware", In: IEEE, Computer Society. International Conference on Field Programmable Logic and Application, ISSN: 1946-147X, PP:133-138, 2010.

[60] Damgard I, "A Design Principle for Hash Functions", In the Proceedings of the CRYPTO' 89, Advances in Cryptology CRYPTO' 89, @ Springer Berlin / Heidelberg Lecture Notes in Computer Science, ISBN: 978-0-387-34805-6, DOI: https://doi.org/10.1007/0-387-34805-0_39, Vol. 435, PP:416–427. 1990.

[61] National Institute of Standards and Technology, "FIPS 180, Secure Hash Standard", Federal İnformation Processing Standard (FIPS), publication 180. Available from http://csrc.nist.gov, May 1993.

[62] Marc Girault, Robert Cohen, Mireille Campana, "A Generalized Birthday Attack", In the Proceedings of Advances in Cryptology (EUROCRYPT '88), ISBN: 978-3-540-50251-7, Vol: 330, JPP:129-156, 1988.