Cryptographic Services to Enforce Secure Messaging and Data Storage

Girija Rani Suthoju[1]
Dept. of CSE,
Neil Gogte Institute of Technology,
Hyderabad, TS.

M. Suresh babu[2]
Dept. of CSE,
YV Sivareddy College of Engineering,
Anantapur, AP.

Abstract:- In secret key cryptography, a single key is used for both encryption and decryption. It achieves privacy and confidentiality. In this, sender sends the cipher text by encrypting the plain text with a secret key and receiver decrypts the cipher text by using same secret key to generate original plain text. The secret key must be shared between two authorized users secretly to apply at both the ends for encrypting and decrypting. Major challenge of secret key cryptography is the key sharing i.e., distribution of secret key to the sender and the receiver. This paper discusses the symmetric key cryptographic algorithms and evaluates step by step procedure of the algorithms with respect to the key bit size.

Keywords:- *Cryptography, Security, Symmetric Key, Cryptosystems, Plain Text, Cipher Text, Encryption, Decryption, Symmetric Algorithms,*

I. INTRODUCTION

In this digital technology world, the cyber threats plethora has been increasing day by day. Emerging internet use is proportionally decreasing the quality of the security. Thus the security experts must concentrate on the measures to reduce the risks in the cyberspace. As we know the cryptosystems are secured by its broad classification into two i.e., (i) symmetric key cryptography - shared key (single key) must be used for both encryption (process of transforming plain text to cipher text) and decryption (process of transforming cipher text to plain text), and (ii) asymmetric key cryptography - public and private key combinations are used for encryption and decryption i.e., public or private key is used at one end and vice versa at other end. But, despite of the advantages, there are many facts that the secret information is being revealed or copied directly to the opponent. Thus, this paper discusses the terminology of most prominently used secret key cryptographic algorithms with respect to their key size and implement in a better way to control the trust of clients. It also notifies how to use the key and challenges faced by sender and receiver.

II. CRYPTOGRAPHY IS EVERYWHERE

Almost all ancient civilizations knew cryptography as a special linguistic phenomenon, fixing on physical media the “secret languages” that existed in different social groups since time immemorial. These languages have an origin in magical ritual, but later they were understood as a tool for social communication. In this regard, cryptography has two main application areas in the ancient history:

“magic” – to conceal a meaning of names, magic rituals, secret ritual knowledge and another taboo information, i.e. for secret communications with the supernatural (that was an integral part of the lives of all ancient civilizations);

“practical” – to protect military reports, personal correspondence, and perhaps trade secrets, i.e. for secret communication in human society.

The most important encryption principles – replacement and permutation of characters – were empirically discovered in the Ancient World. In the Ancient World, these principles exhausted the arsenal of cryptographic protection methods for written texts, and they were realized only for special, very simple cases. Evolution of the cryptographic methods was extremely slow because the existing methods were generally sufficient.

Along with cryptography, the ancient civilizations used various methods of physical protection of messages by encoding and steganography. That served different practical purposes such as concealing the fact of message’s existence or transfer, hiding the names of senders or recipients, accelerating copying text and reducing the amount of material to be carried or memorized, transmitting messages at a rate greater than a man’s speed, and raising the value of the text to the reader. These objectives were often seen as a priority compared to concealing the message’s meaning from unauthorized persons.

While studying cryptography in the Middle Ages and the early New Ages (XVI – XVII centuries) it is reasonable to stress the following:

1. The encryption methods have become more complex in the Middle Ages: polyalphabetic substitution has been invented. The systematic methods of cryptanalysis have appeared in the Arabian world for the first time;
2. Signatures and stamps ensured a document’s authenticity for the first time in Byzantium, along with encryption ensuring the confidentiality of documents;
3. Ciphers are still considered a linguistic phenomenon: single words, sentences, paragraphs, sections of the document are converted.

One of the techniques that can be used to indicate a close relationship between history and modernity of cryptography and to inspire students who are accustomed to think in terms of modern mathematics and formal logic is to mathematically analyze ancient ciphers (like shift, replacement, affine and permutation ciphers). However, the general cases of substitutions and (or) permutation were not implemented in any classical ciphers and cryptographic devices, and the particular cases used essentially reduce the cipher strength. Nevertheless, a number of examples might illustrate the fact that the most secure classic ciphers such as the Vigenère cipher and “Latin squares” are widely regarded as almost unbreakable until the appearance of computers in the XX century.

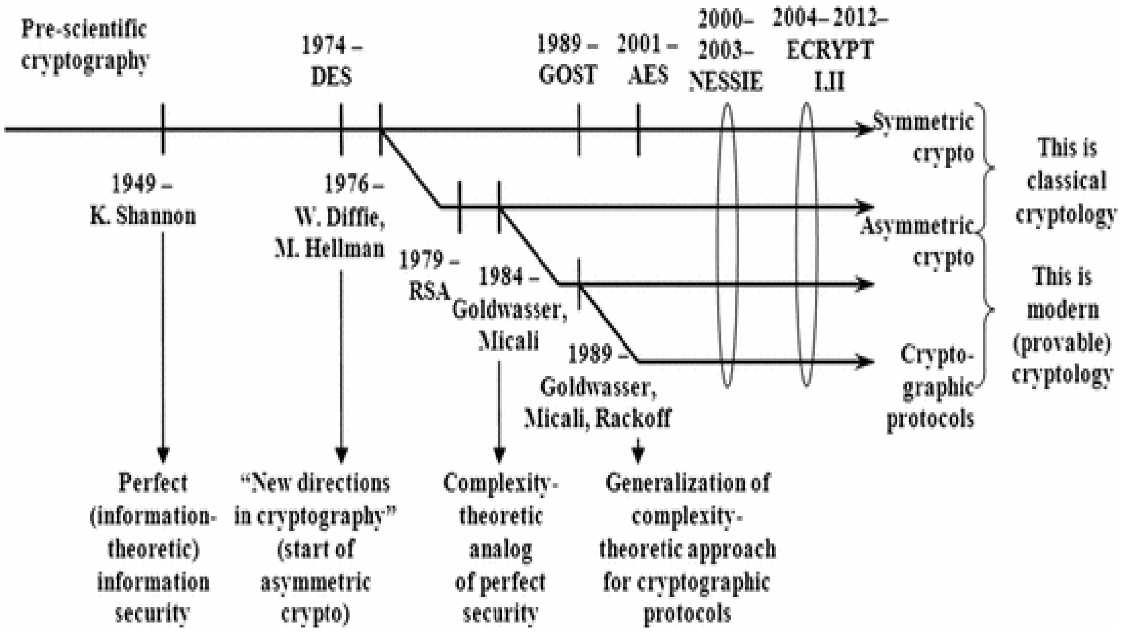
Pre-scientific cryptography
1974 – DES
1989 – GOST
2001 – AES
2000– 2003– NESSIE
2004– 2012– ECRYPT I,II
Symmetric crypto
Asymmetric crypto
Crypto-graphic protocols
This is classical cryptology
This is modern (provable) cryptology
1949 – K. Shannon
1976 – W. Diffie, M. Hellman
1979 – RSA
1984 – Goldwasser, Micali
1989 – Goldwasser, Micali, Rackoff
Perfect (information-theoretic) information security
“New directions in cryptography” (start of asymmetric crypto)
Complexity-theoretic analog of perfect security
Generalization of complexity-theoretic approach for cryptographic protocols

Fig 1:Classical and provable Cryptology

III. CRYPTOGRAPHY AND ITS TYPES

Cryptology is the study of cryptography and cryptanalysis. The procedure of changing original form of data to meaningless code by using any algorithm at sender and from meaningless code to original form of data by using same algorithm at receiver is known as cryptography [1]. To secure information we must encode the form of data into unreadable meaningless code.

The act of obtaining the plaintext or key from the encoded text that is used to obtain plaintext information to pass on modified or fake messages in order to deceive the original intended recipient i.e., breaking the cipher text is referred to as cryptanalysis.

Breaking ciphers may be legal or illegal. This type of breaking the ciphers depends on the types of hackers i.e., either white hat hackers who are legal and certified hackers or black hat hackers who are illegal and bad at works. There are gray hat hackers also who will in the field of legally illegal or vice versa.

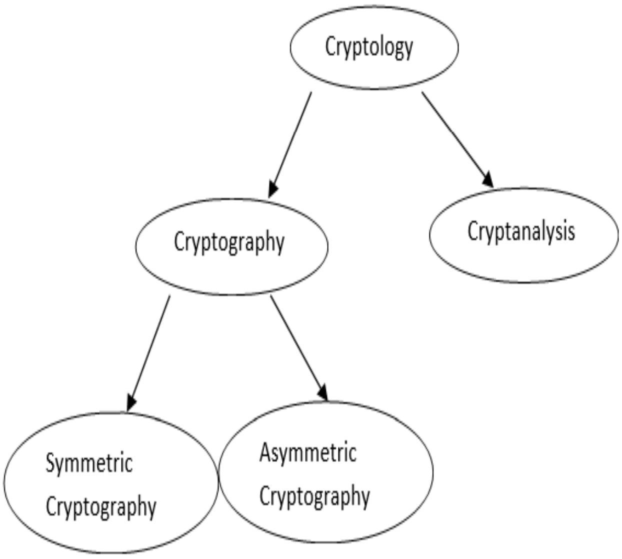

Fig 2: Cryptology Branches

A. Basic Cryptography

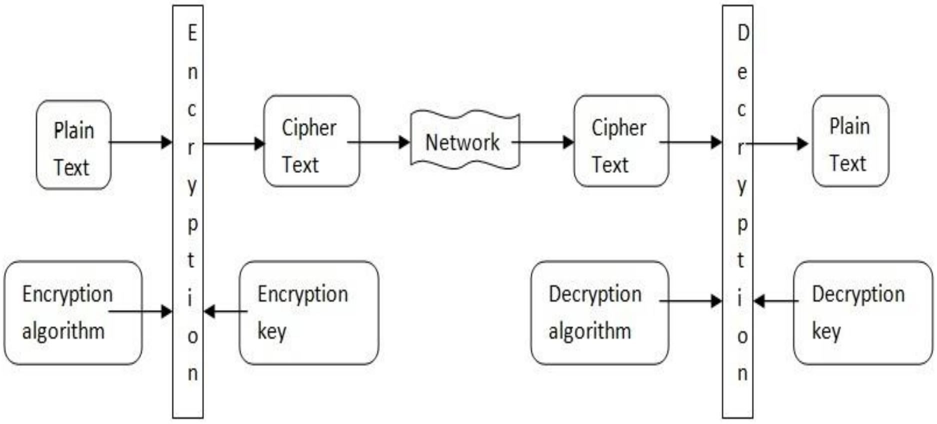

Fig 3: Basic Cryptography

Cryptography is of two types i.e., Symmetric cryptography and asymmetric cryptography. In Symmetric cryptography both sender and receiver will use same key called secret key which will be shared between sender and receiver for both encryption and decryption, whereas in asymmetric cryptography both sender and receiver will have their own set of public and private key combinations. Public key will be shared to network but private key will be maintained confidentially at their end points. If the encryption is done at sender by receiver's public key then it can be decrypted only by receiver's private key and if the encryption is done at sender by sender's private key then it can be decrypted by sender's public key at receiver end.

B. Symmetric Cryptosystems

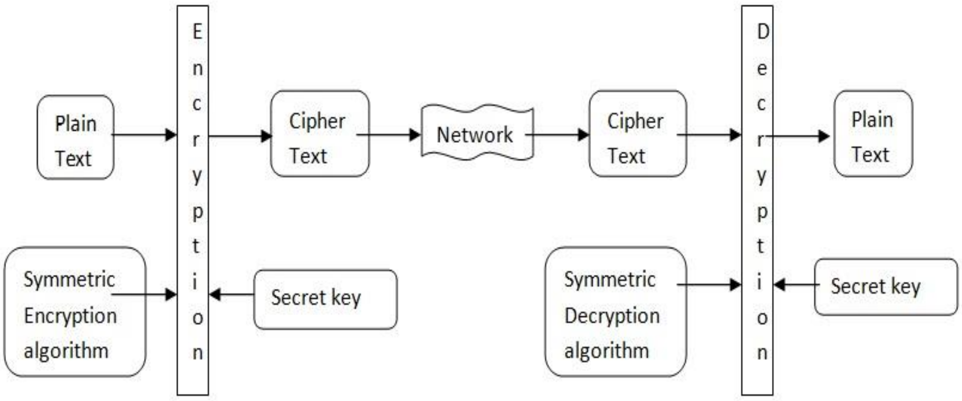

Fig 4: Symmetric Cryptography

C. Asymmetric Cryptosystems

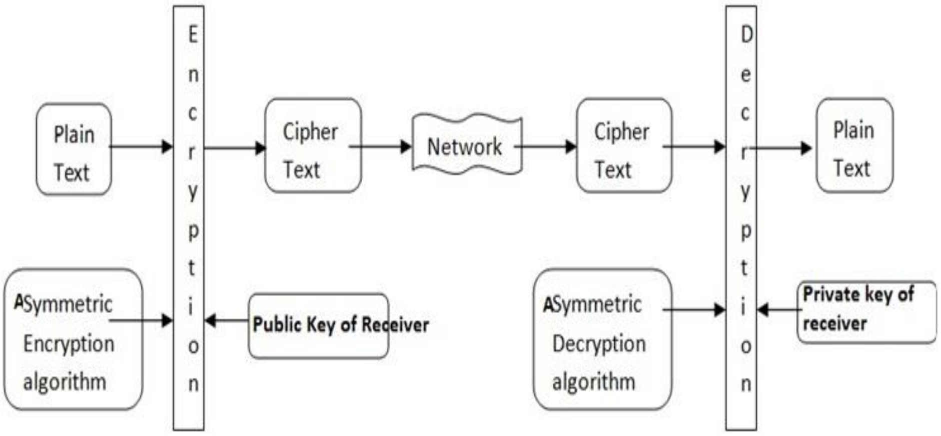

Fig 5: Asymmetric Cryptography

IV. FUTURE SCOPE AND CONCLUSION

Cryptography concerns the invention of encryption algorithms and the invention of decrypting methods. One of the cryptography methods that can be said to be currently attracting is “quantum cryptography”. Quantum means the “minimum unit that can be measured”, and here it refers to a photon, i.e., a quantum of light. Photons vibrate as they move. Encrypted information can be received by measuring the angle of photon vibrations, and whenever a communication is intercepted by anyone other than the intended recipient, the angle changes, thereby ensuring that the interceptions will be detected. The reason encryptions by quantum cryptography are considered impossible to decrypt, whereas encryptions in the past were considered “undecryptable within a reasonable amount of time”, is that the change in angle of the vibrations makes it possible to detect interceptions.

REFERENCES

[1]. Omar G. Abood. Shawkat k. Guirguis, International Journal of Scientific and Research publications, Volume 8, issue 7, July 2018. ISSN: 2250-3153.

[2]. https://ee.stanford.edu/~hellman/publications/73.pdf

[3]. https://www.researchgate.net/publication/326582882_A_Survey_on_Cryptography_Algorithms/link/5b58d72d0f7e9bc79a650f61/download

[4]. http://www.iosrjournals.org/iosr-jce/papers/Vol16-issue4/Version-3/B016431118.pdf

[5]. http://downloads.hindawi.com/journals/scn/2018/8214619.pdf

[6]. http://compmath-journal.org/dnload/Arvind-Kumar-Maurya-Avinash-Singh-Unnati-Dubey-Shivansh-Pandey-and-Upendra-Nath-Tripathi/CMJV10I01P0190.pdf

[7]. https://privacyandsecurityconference.pt/conference2019/Proceedings_Digital_Privacy_and_Security_Conference_2019.pdf#page=144

[8]. https://www.ijitee.org/wp-content/uploads/papers/v8i8/H6799068819.pdf

[9]. https://books.google.co.in/books?hl=en&lr=&id=ZbutDwAAQBAJ&oi=fnd&pg=PR11&dq=ieee+papers+on+cryptography+2019&ots=itiYBvLywH&sig=jqBLiWDN3PrgUa6_W30ceCYmgEY#v=onepage&q=ieee%20papers%20on%20cryptography%202019&f=false

[10]. http://home.deib.polimi.it/pelosi/lib/exe/fetch.php?media=teaching:blockcipherdes.pdf

[11]. http://galaxy.cs.lamar.edu/~bsun/security/lecture_notes/lecture3.pdf

[12]. https://www.ntu.edu.sg/home/anwitaman/TeachingMaterial/Cx4024-SecretKeyCrypto.pdf

[13]. http://www.ccs.neu.edu/home/noubir/Courses/CSU610/S06/cryptography.pdf

1. AUTHORS

[1] Ms. GIRIJA RANI SUTHOJU pursuing Ph.D in the Department of Computer Science and Engineering at JNTU Hyderabad. She received Masters degree (M.Tech) in the Department of CSE at Aurora’s Technological and Research Institute belongs to JNTU, Hyderabad in 2014 and Bachelors degree (B.Tech) in the Department of Computer Science and Engineering from the same University in 2012. She worked as an Assistant Professor for 5years in Aurora’s Technological and Research Institute affiliated to Jawaharlal Nehru Technological University, Hyderabad. She worked in KLEF (K L deemed to be University) Hyderabad from June 2019 to June 2022 and at present she is working in NGIT Hyderabad. She also received Teaching Excellence award for best teaching thrice from 2016 to 2018 from Aurora consortium and also in 2021 by KL University for her best performance in academics. She also received Global Eminent Teacher Award recently. Her area of research is Cryptography and network security.

[2] M. Suresh babu completed PhD (Computer Science) from Sri Krishnadevaraya University, Anantapur, M.Phil (Computer Science) from Bharthiar University in 2007, Master of Computer Applications from Osmania University,Hyderabad in 1997, PGDBA from Sri Krishnadevaraya University, Anantapur in 2002, DCOM from IGNOU, New Delhi and Bachelor of Science from Sri Krishnadevaraya University, Anantapur in 1993. His area of interests are Datamining, Cloud computing and Networks. He is a creative professional with around 18+ years of experience in Teaching & Student Management. Presently, he is working as Principal, in Y V Sivareddy college of Engineering, Ananthapur, AP. He worked as a Professor in Department of Computer Science & Engineering, S K D Engineering College, Ananthapur, AP and also as a Principal, Aurora’s Technological Institute, Uppal, Hyderabad from Jan- 2015 Aug-2015, also as Principal, Intel Institute of Science, Anantapur,from October 1998 - December 2012. He worked as Professor & Head, Department of Computer Applications, Madanapalle Institute of Technology & Science, from December 2012 to December 2014.