[ICEMESM-18]
DOI-10.5281/zenodo.1220946

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

COMPARATIVE ANALYSIS OF DIFFERENT ENCRYPTION ALGORITHMS FOR IMPROVING SECURITY

Asfiya Shireen Shaikh Mukhtar[1] & Ghousiya Farheen Shaikh Mukhtar[2]
[1]Asst.Prof.,MCA Dept., SRPCE,Nagpur, Maharashtra, India.
[2]Asst.Prof., BCA Dept., S.S.Maniyar College of Science & Management, Nagpur, Maharashtra, India.

ABSTRACT

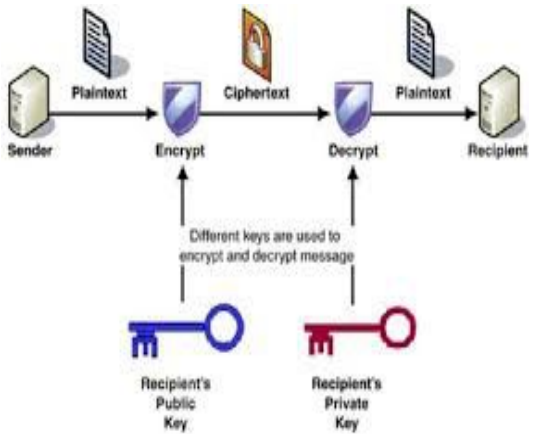
Cryptography is the process of securely transmission of data. Cryptography is the process of Encryption and Decryption of data. Data is Encrypted by using secret key and Encryption Algorithm hence data is in secret form(unreadable form or encoded form) similarly data is decrypted by using secret key and decryption algoritum.Cryptography not only protects data from theft or alteration, but can also be used for user authentication. This paper provides a comparison of different Cryptography Algorithm. We analysis and compare different Symmetric and Asymmetric Algorithm. The comparison has been conducted with different sizes of data blocks to evaluate the algorithm's encryption/decryption speed.

Keywords: *Encryption, Decryption, DES,AES,Symmetric Algoritum,Asymmetric Algoritum.*

I. INTRODUCTION

Cryptography is the process of storing and transmission of data. Data is Encrypted form so unauthorized user can not access the data. only the Authorized or intended user can access the data by using Share key. Cryptography have the following four objectives :

- Confidentiality
- Integrity
- Non-repudiation
- Authentication



There are five primary functions of cryptography :

1. *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
2. *Authentication:* The process of proving one's identity.
3. *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
4. *Non-repudiation:* A mechanism to prove that the sender really sent this message.
5. *Key exchange:* The method by which crypto keys are shared between sender and receiver.

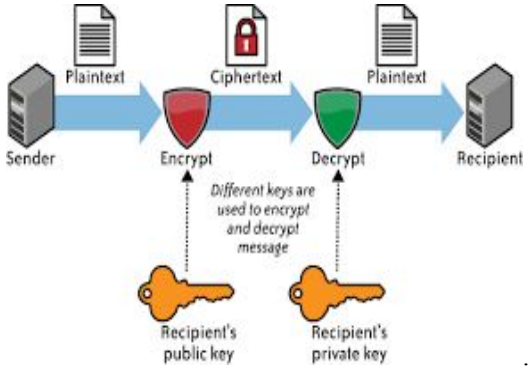
ISSN 2348 – 8034
Impact Factor- 5.070

In cryptography, Sender sends the data in insecure communication. Data is protected from unauthorized user by data or plaintext is encoded using Encryption algorithm and Encryption Key so data is in Encoded form any unauthorized use cannot access the data, this is called Encryption process. Similarly In Decryption encoded data is decoded by using Decryption algorithm and decryption key. Hence only intended receiver can access the data. This process is called Encryption Decryption process We used the following formula for Encryption and Decryption process.

$C=E_k(P)$

$P = D_k(C)$

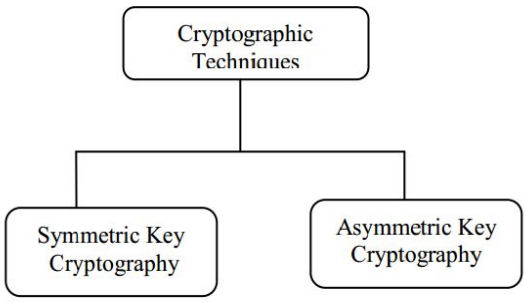
Where **P** = plaintext, **C** = cipher text, **E** = the encryption method, **D** = the decryption method, and **k** = the key.n many of the descriptions below. A malicious party is referred to as Mallory, an eavesdropper as Eve, and a trusted third party as Trent. Finally, *cryptography* is most closely associated with the development and creation of the mathematical algorithms used to encrypt and decrypt messages, whereas cryptanalysis is the science of analyzing and breaking encryption schemes. .



Cryptography is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems, yet it is surprisingly hard to do right. Cryptography has often been used to protect the wrong things, or used to protect them in the wrong way. We'll see plenty more examples when we start looking in detail at real applications. Unfortunately, the computer security and cryptology communities have drifted apart over the last 20 years. Security people don't always understand the available crypto tools, and crypto people don't always understand the real-world problems.

Different types of Cryptosystems:

There are three types of cryptosystems: Symmetric key, Asymmetric key. Symmetric key encryption uses one key to encrypt and decrypt. Asymmetric key encryption uses two keys; when one key is used to encrypt, the other is used to decrypt. symmetric key encryption algorithms include DES (the Data Encryption Standard) and AES (the Advanced Encryption Standard).



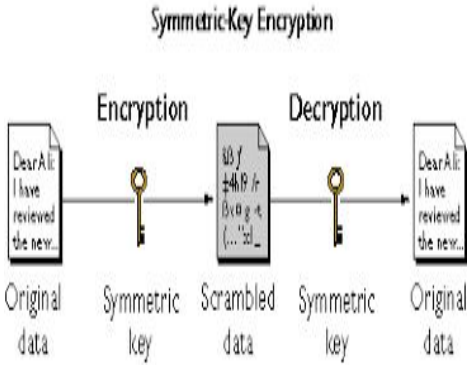
ISSN 2348 – 8034
Impact Factor- 5.070

(a) *Symmetric key Encryption/Decryption*

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.

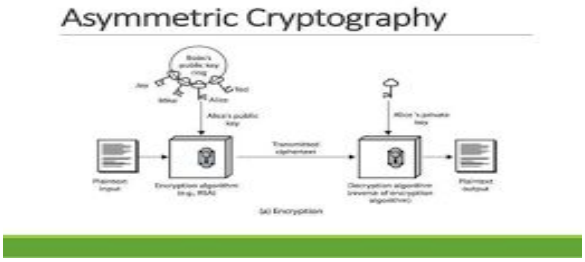
One round (out of 8.5) of the IDEA cipher, used in some versions of PGP for high-speed encryption of, for instance, e-mail

Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher



Asymmetric Key Encryption/Decryption

Asymmetric key encryption (also called public key encryption) uses two keys: a public and a private key. Data encrypted with one key can be decrypted only with the other key. Whitfield Diffie and Martin Hellman first publicly described this approach in November 1976in *New Directions in Cryptography*, where they announced: "We stand today on the brink of a evolution in cryptography."



Comparison between Symmetric and Asymmetric Encryption:

Symmetric vs. Asymmetric Key Systems

Attributes	Symmetric	Asymmetric
Keys	One key is shared between two or more entities	One entity has a public key, and the other entity has a private key
Key Exchange	Out-of-band	Symmetric key is encrypted and sent with message; thus, the key is distributed by in-bound means
Speed	Algorithm is less complex and faster	Algorithm is more complex and slower
Number of Keys	Grows exponentially as users grow	Grows linearly as users grow
Use	Bulk encryption, which means encrypting files and communication paths	Key encryption and distributing keys
Security Service Provided	Confidentiality	Confidentiality, authentication, and non-repudiation

ISSN 2348 – 8034
Impact Factor- 5.070

Symmetric Key Algorithms

A symmetric key algorithm (also known as a secret key algorithm), uses the concept of a key and lock to encrypt plaintext and decrypt cipher text data. The same "key" is used to both encrypt and decrypt the file. They are sub-classified by stream ciphers and block ciphers. A stream cipher is where plaintext digits are combined with a pseudo-random cipher digit stream. Block ciphers take the number of bits and encrypt them as a single unit (known as rounds), padding the plaintext so that it's a multiple of a block size.

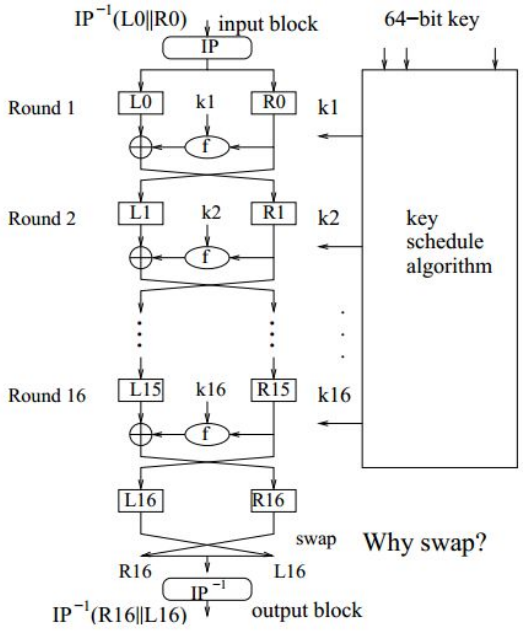
Symmetric algorithms encrypt and decrypt a message using the same key. If you hold a key, you can exchange messages with anybody else holding the same key. It is a shared secret. But be careful who you give the key to. Once it gets in the wrong hands, there is no getting it back. That person can read all of your past messages, and create new messages that are indistinguishable from valid data.

Several symmetric algorithms have been used in the past. These include:

- DES
- AES
- IDEA
- Blowfish

DES

The Data Encryption Standard or DES was, and probably still is, one of the more well-known algorithms of the modern cryptographic era. Today it is widely considered insecure. DES was developed in the 1970's by IBM and was later submitted to the National Bureau of Standards (NBS) and National Security Agency (NSA). The involvement of the NSA in the design sparked controversial rumours of backdoors, creating widespread scrutiny. It wasn't until 1976 that DES was approved as a cryptographic standard and published in FIPS.Since then, DES was fortified with new updates called double-DES and triple-DES, simply layering the cipher so that it would have to decrypt three times to each data block. Triple-DES is still used in some places, but AES has become the new s tandard since then.



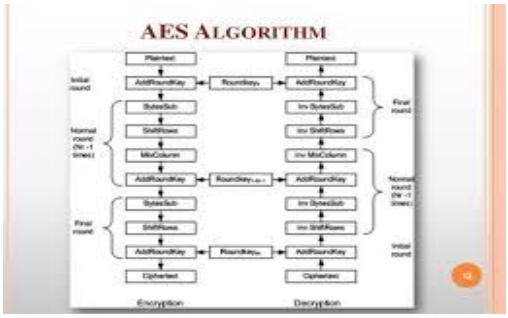
.

AES

AES is the successor of DES as standard symmetric encryption algorithm for US federal organizations (and as standard for pretty much everybody else, too). AES accepts keys of 128, 192 or 256 bits (128 bits is already very unbreakable), uses 128-bit blocks (so no issue there), and is efficient in both software and hardware. It was selected

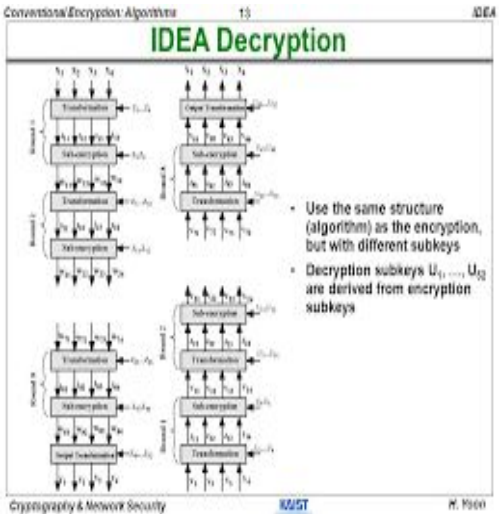
ISSN 2348 – 8034
Impact Factor- 5.070

through an open competition involving hundreds of cryptographers during several years. Basically, you cannot have. better than that



IDEA

The International Data Encryption Algorithm (IDEA), originally called the Improved Proposed Encryption Standard (IPES), was designed by James Massey of ETH Zurich under a research contract with the Hasler Foundation, now Ascom Tech AG, and was first discussed in 1991. IDEA was a minor revision of the Proposed Encryption Standard (PES), intended as a replacement of the DES.

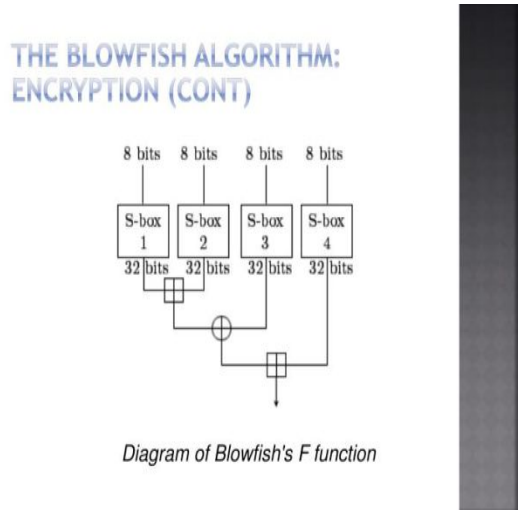


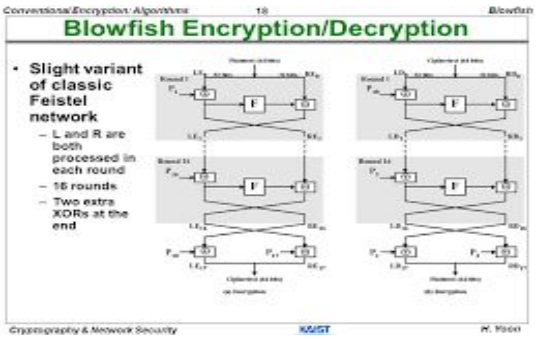
Blowfish

Blowfish is a block cipher proposed by Bruce Schneier, and deployed in some softwares. Blowfish can use huge keys and is believed secure, except with regards to its block size, which is 64 bits, just like DES and 3DES. Blowfish is efficient in software, at least on some software platforms (it uses key-dependent lookup tables, hence performance depends on how the platform handles memory and caches).

[ICEMESM-18]
DOI-10.5281/zenodo.1220946

ISSN 2348 – 8034
Impact Factor- 5.070

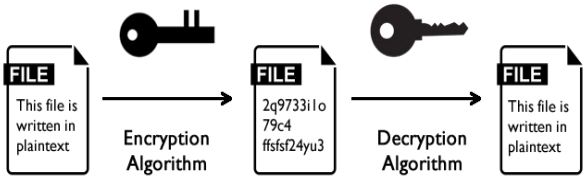




Comparison of different Symmetric Algorithm:

Algorithm	Type	Method	Key Size
AES	Symmetric encryption	128-bit block cipher	128-, 192-, or 256-bit key
DES	Symmetric encryption	64-bit block cipher	56-bit key
3DES	Symmetric encryption	64-bit block cipher	56-, 112-, or 168-bit key
Blowfish	Symmetric encryption	64-bit block cipher	32- to 448-bit key
Twofish	Symmetric encryption	128-bit block cipher	128-, 192-, or 256-bit key
RC4	Symmetric encryption	Stream cipher	40- to 2,048-bit key

Asymmetric Algorithms

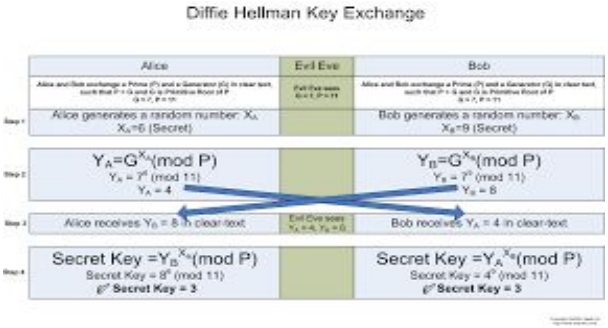


[ICEMESM-18]
DOI-10.5281/zenodo.1220946
ISSN 2348 – 8034
Impact Factor- 5.070

Asymmetric algorithms use a different key to encrypt than they do to decrypt. The encrypting key is called the *public key* and the decrypting key is the *private key*. If you hold the private key, I can send you a message that only you can read.
There are three asymmetric algorithms in use today:

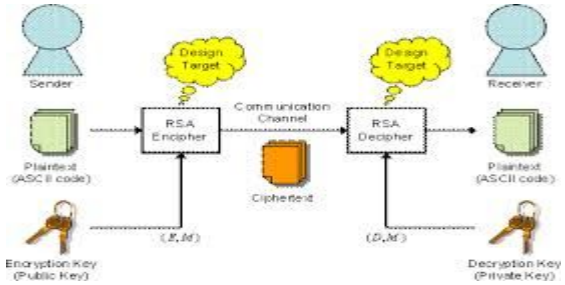
- Diffie-Hellman
- RSA
- Elliptic Curve

Diffie-Hellman:
Diffie-Hellman is one of the first recorded examples of asymmetric cryptography, first conceptualized by Ralph Merkle and put into fruition by Whitfield Diffie and Martin Hellman. Traditionally, secure encrypted communication would require both parties to first exchange their keys by some secure physical channel. Diffie-Hellman eliminated the need for the secure exchange by creating an additional key, the public key. At this moment in time, Deffie-Hellman is no longer the standard cryptographic algorithm because it has been found to be vulnerable to several attacks. A Logjam attack, for example, can allow man-in-the-middle attacks where the hacker can read and modify any data sent over the connection.



RSA
The Rivet-Shammir-Adleman algorithm, better known as RSA, is now the most widely used asymmetric cryptosystem on the web today. RSA is based on the factorization of prime numbers, because working backwards from two multiplied prime numbers is computationally difficult to do, more so as the prime numbers get larger. The challenge of breaking RSA is known as the 'RSA problem'.

RSA is a slow algorithm and because of this, it is used to encrypt and decrypt the symmetric keys which in turn, encrypt and decrypt the communications. The symmetric keys perform the bulk of the work, while RSA creates a strong and secure channel.



[ICEMESM-18]
DOI-10.5281/zenodo.1220946
ISSN 2348 – 8034
Impact Factor- 5.070

Elliptic Curve

ECC stands for Elliptic Curve Cryptography, which is an approach to public key cryptography based on elliptic curves over finite fields. Cryptographic algorithms usually use a mathematical equation to decipher keys; ECC, while still using an equation, takes a different approach.SSL/TLS Certificates most commonly use RSA keys and the recommended size of these keys keeps increasing (e.g. from 1024 bit to 2048 bit a few years ago) to maintain sufficient cryptographic strength. An alternative to RSA is ECC. Both key types share the same important property of being asymmetric algorithms (one key for encrypting and one key for decrypting). However, ECC can offer the same level of cryptographic strength at much smaller key sizes - offering improved security with reduced computational and storage requirements.schemes are available for security purpose This scheme is called cryptography. In cryptography we use key called public key and private key.With the help of these keys we encrypt and decrypt the data fro make secure. Encrypted data is called cipher text and decrypted data s called plaintext.

II. CONCLUSION

Security is an important aspect in network security .today is the Era of fast Communication. And transfer is data more secure manner. In this paper we analysis the different Cryptography algorithms which is used to improve security. And compare the different algorithms based on the different parameter.

III. FUTURE SCOPE

In our future work we will apply the methodology and algorithms to secure text and images and audio to secure transmission. Advanced Encryption standard algorithms and DES algorithm is more secure to transfer data.

REFERENCES

[1] *Yuliang Zheng. Digital signcryption or how to achieve cost(signature encryption) cost(signature) + cost(encryption). In CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, pages 165{ 179, London, UK, 1997.*

[2] *N. Islam, M. H. Mia, M. F. I. Chowdhury and M. A. Matin, "Effect of Security Increment to Symmetric Data Encryption through AES Methodology", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, (2008).*

[3] *William Stallings. Cryptography and Network security: Principles and Practices. Prentice Hall Inc., second edition, 1999.*

[4] *R. L. Rivest, "The RC5 Encryption Algorithm", Proceedings of the Second International Workshop on Fast Software Encryption (FSE), (1994).*

[5] *D. Coppersmith, "The data encryption standard (DES) and its strength against attacks", IBM Journal Research Develop., vol. 38, no. 3, (1994), pp. 243 -250.*

[6] *Cryptography and Network Security: Principles and Practice" by William Stallings*

[7] *Moon, Dukjae; Hwang, Kyungdeok; Lee, Wonil; Lee, Sangjin; Lim, Jongin (2002). "Impossible differential cryptanalysis of reduced round XTEA and TEA" (PDF). Lecture Notes in Computer Science. 2365: 49–60.Doi:10.1007/3-540-45661-9_4.*

[8] *Hong, Seokhie; Hong, Deukjo; Ko, Youngdai; Chang, Donghoon; Lee, Wonil; Lee, Sangjin (2003). "Differential cryptanalysis of TEA and XTEA". In Proceedings of ICISC 2003. doi:10.1007/978-3-540-24691-6_30.*