International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

COMPARATIVE ANALYSIS OF ENCRYPTION TECHNIQUES

Anubha Pandya[1], Asst. Prof. Prabhat Pandey[2]

[1]M.Tech (Embedded and VLSI Design) Department of Electronics and Communication Engineering AITR, Indore (M.P), India
[2]Asst. Prof, Department of Electronics and Communication Engineering, AITR, Indore (M.P), India

---

ABSTRACT - *Encryption is the process of jumbling a message so that only the expected receiver can read it. Encryption can be responsible for a means of safeguarding information. As progressively information is put in storage on computers or communicated via computers, the necessity to insure that this information is safe to interfering and/or tampering becomes more relevant. With the fast progression of digital data exchange in electronic way, Information Security is becoming much more important in data storage and transmission. Information Secrecy has a noticeable implication in the study of ethics, law and most recently in Information Systems. With the development of human intellect, the art of cryptography has become more difficult in order to make information more secure. Arrays of Encryption systems are being deployed in the world of Information Systems by various organizations. In this paper, a survey of various Encryption Algorithms is presented.*

Keywords – Encryption, DES, 3DES, AES

1. INTRODUCTION

A system for encoding and decoding a secret message is called as cryptography. More generally, people think of cryptography as the art of bungling information into apparent unintelligibility in a manner allowing a secret method of untangling. The basic service provided by cryptography is the ability to send information between participants in a way that intercept others from reading it. This kind of cryptography can provide other Services, such as

- Nobility checking - Reassuring the receiver of a message that the message has not been altered since it was generated by an authorized source.
- Authentication - Verifying someone's (or something's) identity.

A message in its genuine form is known as plain text or clear text. The bungle information is known as cipher text. The procedure for producing cipher text from plaintext is known as encryption. The interchange of encryption is called decryption. There are two types of encryption technique:

1.1 Symmetric cryptosystems

It is also known as secret key cryptography. Sender & receiver use same keys for encryption & decryption namely PUBLIC or PRIVATE respectively. The Secret key cryptography involves the use of a single key. Given a information called plaintext and the key, encryption construct incompressible data which is about the same size as the plaintext.[4] Decryption is the reverse of Encryption; it is the conversion of cipher to plain text and uses the same key as encryption. The symmetric algorithms can be splitter into stream ciphers and block ciphers. Stream ciphers encrypt only one bit of plaintext at a time, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers) and encrypt them as a single unit. Here the same are used for the encryption and decryption processes so it is called as the secret key cryptography.

1.2 Asymmetric cryptosystem

It is also known as public key cryptography. Sender & receiver uses different key & an encryption/ decryption data, i.e. the key is shared Public key cryptography is sometimes also referred to as asymmetric cryptography. Asymmetric ciphers also known as public-key algorithms, allow's the encryption key to be public (it can even be published to a web site), anyone has the permission to encrypt with the key, message can be decrypted only by the proper recipient (who knows the decryption key). The encryption key is also called the public key and the decryption key the private key. By keeping the private key secret we can provide security to the ciphers [3].

Public key cryptography is a relatively new field, invented in 1975 unlike secret key cryptography, keys are not shared. Instead, each individual has two keys: a private key that need not be revealed to anyone, and a public key that is preferably known to the entire world. The term private key must be used when referring to the key in public key cryptography that must not be made public There is something unfortunate about the terminology public and private. It is that both words begin with p. We will sometimes want a single letter to refer to one of the keys. The letter p won't do. We will use the letter e to refer to the public key, since the public key is used when encrypting a message. We'll use the letter d to refer to the private key, because the private key is used to decrypt a message.

2. Current Trending Technology

- DES
- 3DES
- AES

2.1 Data Encryption Standard (DES)

DES stands for the data encryption standard. The DES uses a 56-bit key to transform a 64-bit block of plaintext to a 64-bit block of cipher text. The AES uses 128-bit plaintext and cipher text blocks and a key size of 128, 192 or 256 bits.

Times more secure than the DES. At this point it remains to be seen if that is indeed the case. The most popular security enhanced version of the DES is two-key triple- DES: three rounds of DES, where the same key is used in the first and last round, but with a different key for the second round. Also, for compatibility with one-key single-DES, the second round uses the inverse of the DES, which is as hard to break as the DES itself. Two-key triple-DES supposedly attains strength equivalent to that of an ideal 80-bit key symmetric cryptosystem, at the actual cost of two 56-bit keys and three DES applications. Two-key triple-DES is easily available in hardware, despite the fact that one of the DES designers referred to it as an 'historical error'. Three-key triple-DES is much better, relatively speaking: it is believed to attain 112-bit key strength, at the cost of three 56-bit keys and three DES applications. Efficient hardware implementations of it are beginning to become available.

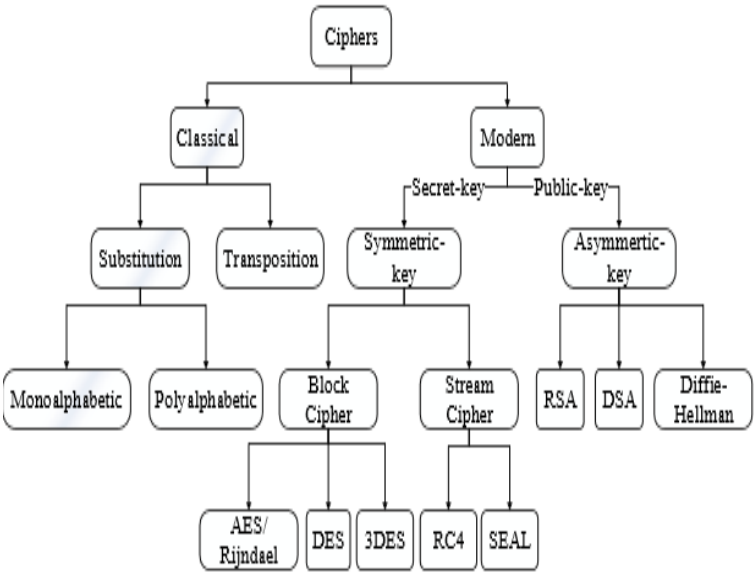

Fig 1: Classification of Encryption Methods

Single-DES implementation, then migration to three-key triple-DES is probably much cheaper than, and essentially as effective as, replacing the DES by the AES. It is conceivable that this applies to, for instance, customer banking transactions, since most of the financial transactions involved are low volume and not time-critical. If, however, speed is or will be an issue, or if large transmissions are anticipated, or if compatibility may become important, then it is probably best to upgrade to the AES as soon as adequate software and hardware implementation become available. In any case, continued use of one-key single-DES for anything of even the slightest importance is irresponsible. It can no longer be recommended.

2.2 Triple DES (3DES)

3DES or the Triple Data Encryption Algorithm (TDEA) was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56). TDEA involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt- Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3 [17].

2.3 Advanced Encryption Standard (AES)

The Advanced Encryption Standard, or AES, is the block cipher of choice for future applications AES is called 128-EIA 2 in LTE. The AES has a block length of 128 bits and supports 3 key lengths: 128, 192 and 256 bits. The versions with longer key lengths use more rounds and are hence slower by 20, respectively 40%.The strong algebraic structure of the AES cipher has led some researchers to suggest that it might be susceptible to algebraic attacks.

However such attacks have not been shown to be effective for the 192- and 256-bit key versions there are related key attacks. For AES-256 this attack, using four related keys, requires time $2^{99.5}$ and data complexity $2^{99.5}$. The attack works due to the way the key schedule is implemented for the 192- and 256-bit keys (due to the mismatch in block and key size), and does not affect the security of the 128-bit variant. Related key attacks can clearly be avoided by always selecting cryptographic keys independently at random. A bi-clique technique can be applied to the cipher to reduce the complexity of exhaustive key search. For example in [5] it is shown that one can break AES-128 with $2^{126.2}$ encryption operations and 2^{88} chosen plaintexts. For AES-192 and AES-256 these numbers become $2^{189.7}/2^{40}$ and $2^{254.4}/2^{80}$ respectively.

3. COMPARITIVE STUDY OF SECURITY ALGORITHMS

Table 1.[6] Shows that in Symmetric Algorithms is AES more secure algorithm as compared to DES and 3DES.

Factors	AES	3DES	DES
Key Length	128,192 or 256 bits	112,168 bits	56 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Block Size	128,192 or 256 bits	64 bits	64 bits
Developed	2000	1978	1977
Security	Considered secure	One only weak which exit in DES	Proven inadequate

4. CONCLUSION AND SCOPE OF FUTURE WORK

This paper presents a study of the popular Encryption Algorithms such as, DES, 3DES and AES. The use of internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used. In this paper, a survey on the existing works on the Encryption techniques has been done. To sum up, all the techniques are useful for real-time Encryption. Each technique is unique in its own way, which might be suitable for different applications and has its own pro's and con's. According to research done and literature survey it can be found that AES algorithm is most efficient in terms of speed, time, and throughput and avalanche effect. The Security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data. Our future work will explore this concept and a combination of algorithms will be applied either sequentially or parallel, to setup a more secure environment for data storage and retrieval.

5. REFERENCES

1. J.Balamurugan,Dr.E.Logashanmu, "Design of High Speed and Low Area Masked AES Using Complexity Reduced Mix-Column Architecture", IJCSEC-International Journal of Computer Science and Engineering Communications, Vol.2 Issue.3, May 2014.

2. G. H. Karimian, B. Rashidi, and A.farmani, "A High Speed and Low Power Image Encryption with 128-Bit AES Algorithm", International Journal of Computer and Electrical Engineering, Vol. 4, No. 3, June 2012.

3. Tanya Vladimirova, Roohi Banu and Martin N. Sweeting, "On-Board Security Services in Small Satellites".

4. Shi-hai Zhu, "Hardware Implementation Based on FPGA of AES Encryption and Decryption System", Scholars Journal of Engineering and Technology (SJET), Sch. J. Eng. Tech., 2014.

5. Lekshmi R , Sajan Xavier, FPGA Based Design of AES with Masked S-Box for Enhanced Security", International Journal of Engineering Science Invention, Volume 3 Issue 5‖ May 2014.

6. Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani "New Comparative Study Between DES, 3DES and AES within Nine Factors" JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617

7. Sumitra "Comparative Analysis of AES and DES security algoritham" International Journal of Scientific and Research Publications, Volume 3, Issue 1, January 2013 ISSN 2250-3153