Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

Cryptographic Algorithms

***Pradip C. Togadiya*[1] *, Ankit S. Togadiya*[2]**

1Computer Science & Engineering, SLTIET
[2]Computer Science & Engineering, SLTIET

Abstract – *Cryptographic Algorithms are sorted into like in size key algorithm and asymmetric key algorithm.. This grouping is based on the number of keys or key groups used for the encryption and decryption. In like in size key algorithm ,same single key or key put is used for both encryption and decryption ,where in asymmetric key algorithm; different keys used. Public key is used for encryption and private key is used for decryption. widely used asymmetric key or public key systems like RSA ,Diffie-Hellman and like in size key or private key systems DES,3DES ,AES.*

Keywords -- *RSA, DES, 3DES, AES, Diffie-Hellman, Encryption, Decryption, Cryptography, Algorithm*

I. INTRODUCTION

The word cryptography comes from the Greek words (hidden or secret) and (writing). Oddly enough, cryptography is the art of secret writing. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Cryptanalysts are also called attackers. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. Data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption opening. The word cryptography comes from the Greek words (put out of the way or secret) and (writing). in a strange way enough, cryptography is the art of secret writing. Cryptography is the science of using mathematics to encrypt and decrypt facts. Cryptography enables you to store sensitive information or send it across unsafe networks(like the internet) so that it can not be read by anyone except the person one is going to be married to one who gets. While cryptography is the science of getting facts, cryptanalysis is the science of getting at details and breaking safe news. Cryptanalysts are also named attackers. The basic Service on condition that by cryptography is the power to send information between ones taking part in a way that keeps from taking place others from reading it. facts that can be read and got clearly without any special measures is named plaintext or clear wording. The careful way of making change in look of plaintext in such a way in connection with skin, leather its substance is telephoned encryption. Encrypting plaintext results in unreadable talk without clear sense called ciphertext. You use encryption to make certain that information is put out of the way from anyone for whom it is not person one is going to be married to, even those who can see the encrypted knowledge for computers. The process of reverting ciphertext to its first form plaintext is named decryption.

II. CRYPTOGRAPHY GOALS

1. **confidentiality**: The sender encrypts the note using a cryptographic encrypting algorithm with a right key. The one who gets decrypts the note using a cryptographic decryption algorithm with a matched key that may or may not be the same as the one used by the sender.

2. **integrity**: integrity assurance that data receivable is exjectly same as data sent by sender.

3. **authentication**: A user or system can make certain their mind and physical qualities to another who does not have personal knowledge of their mind and physical qualities done using by numbers, electronic statements made in writing by one in authority in a asymmetric cryptosystem.

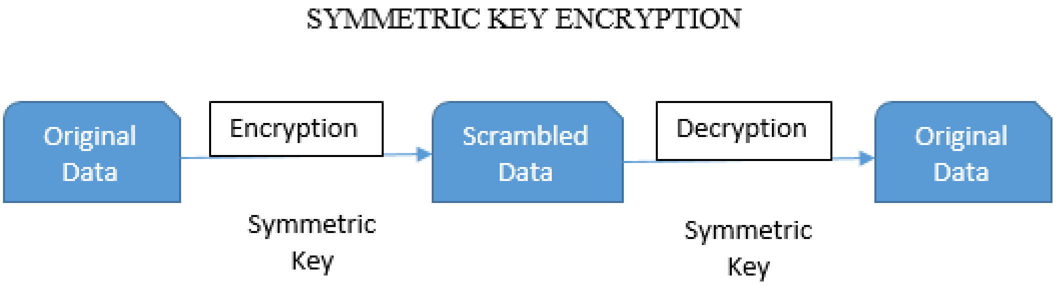
.

4. **non-repudiation**: The sender of a note can not later Claim he/she did not send it ready (to be used) only with asymmetric cryptosystems that can make come into existence by numbers, electronic sign-marks.

III. TYPES OF CRYPTOGRAPHY

Two types of cryptography:

I. **Secret key cryptography** : a private or secret key is an encryption/decryption key within one's knowledge only to the Party or parties that exchange secret notes. In old and wise secret key cryptography, a key would be shared by the knowledge exchangers so that each could encrypt and decrypt notes. The danger in this system is that if either Party loses the key or it is taken (property of another), the system is broken. A more nearby that possibly taking place in addition is to use a mix of public and private keys. In this system, a public key is used together with a private key.



1) **DES(Data Encryption Standard):**

The Data Encryption Standard (DES) was together developed in 1974 by IBM and the U.S. government to put a quality example that everyone could use to safely exchange with each other. however, this has now been put in place of by a new quality example certain as the increased Encryption Standard (AES).It is a like in size algorithm, means same key is used for encryption and decryption. DES is a 64 bit solid mass cipher which means that it encrypts facts 64 bits at a time. It used a key size of 128 bits however this was made lower, less to 56 bit s for DES. Even though DES actually takes a 64 bit key as input ,the still in the same way eight bits are used for parity checking and have no effect on DESs security. Decryption of DES algorithm is similar to encryption, only the round keys are in opposite order. The output is a 64 bit block.any attacks and methods recorded feeblenesses of DES,which has made it an unsafe solid mass encryption key.

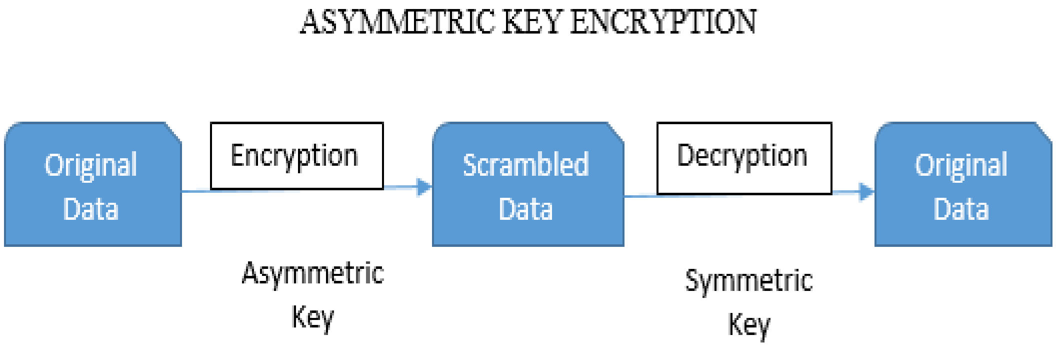
2) **3DES:**

triple DES is based on the Des algorithm.It takes three 64-bit keys, for an overall key length 16 of 192 bits. The encryption careful way is similar to the first form DES but it send in name for 3 times to increase the safe time and encryption level. The Procedure for encryption is exactly the same as regular DES ,but it is redone three times, for this reason the name triple DES.The facts is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key. triple DES runs three times slower than DES, but is much more safe if used properly.The Procedure for decrypting something is the same as the Procedure for encryption, except it is did, gave effect to in opposite.

3) **AES(Advance Encryption Standard)**

It is a like in size key encryption quality example took up by the in us government in 2001. It was designed by Vincent Rijndael and Joan Daemena in 1998. The more pleasing to all and widely took up like in size encryption algorithm is the increased Encryption Standard (AES). It is discovered at least 6 time quicker than triple DES. It encrypts facts gets in the way of 128 bits using like in form keys. It has a not fixed in value key length of 128, 192 or 256 bits, by Default 256 is used. AES encrypts 128 bits facts solid mass into 10, 12 and 14 round according to the key size. AES is different from DES in that it is nota feistel structure. have in mind, get memory of that in a feistel structure, half of the facts solid mass is used to modify the other half of the facts solid mass and then the separate half are made exchange of. In this Case the complete knowledge for computers get in the way of is processed in parallel during each round using things used for another and permutations

II. **Public key cryptography*:*** Public key cryptography is an asymmetric design that uses a of keys for encryption: a public key, which encrypts facts, and a being like (in some way) private, or secret key or decryption. You put into print your public key to the earth while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. Any one who has a public key can encrypt information but can not decrypt it. Only the person who has the being like (in some way) private key can decrypt the information



1) RSA

RSA is widely used in encrypted connection, by numbers, electronic statements made in writing by one in authority core algorithms. Public key algorithm invented in 1977 by Ron Rivest ,Adi Shamir and Leonard Adelman (RSA).keys are produced by receiver, one key is declared as public and another key is certain to only & only receiver. RSA uses a not fixed in value size encryption solid mass and a not fixed in value size key. The key is formed from a very greatly sized number N, that is the product of two prime numbers chosen. It uses the get in the way of size facts in which plaintext and cipher wording are complete numbers, not parts between 0 and n1 for some N values. Size of N is taken into account 1024 bits or 309 decimal any numbers 0 to 9

2) Diffie-Hellman

Diffie-Hellman algorithm was introduced in 1976.diffiehellman key exchange is a special careful way of safely exchanging cryptographic key over a public narrow way, The Diffie-Hellman algorithm grants 2 users to make certain a shared secret key and to exchange over an unsafe news narrow way, The biggest limiting condition of this algorithm is man in the middle attack.

IV. COMPARISION OF ALGORITHMS

.

Algorithm	Created By	Year	Key Size	Block	Round	Structure	Features
DES	IBM	1975	64 bit	64 bit	16	Festial	Not Strong Enough 3DES
3DES	IBM	1978	112 or 168	64 bit	48	Festial	Adequate Security
AES	Joan Daeman & incent Rijmen	1998	128,192,256 bit	128 bit	10,12,14	Substitution Permutation	Replacement for DES, Excellent Security
RAS	Rivest,Shamir, Adleman	1977	1024 to 4096	128 bit	1	Public Key Algorithm	Excellent Security, Low speed
Diffie Hellman	Whitfield,Diffie ,Hellman	1976	1024 to 4096	512	-	Asymmetric Algorithm	Many attacks

V. CONCLUSION

internet is mainly used by beings, Co-operatives and Governments. They have send information through internet. But there is a possible state of to protect the information .So to keep safe (out of danger) information, we need to encrypt/decrypt information by using cryptography algorithms .In this paper the having existence encryption techniques are studied and got at the details of to give help to the doing a play of the encryption methods also to make certain the safety business done at meeting. To amount of money up, all techniques are nothing like it in its own way, which might be right for different applications. The next way of doing that is widely used to keep safe (out of danger) our information is RSA.I have read many papers on Cryptography that mainly used RSA algorithm for information safety. RSA is the most safe& widely used by persons making observations. AES is better algorithms in terms of doing a play and safety. RSA can be used with many techniques like RSA& DES, RSA& AES, RSA& DIffie Hellman.

REFERENCES

[1] Anjula Gupta, Navpreet Kaur Walia,(2014) "Cryptography Algorithms: A Review", IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939.
[2] Divya sukhija "A Review Paper on AES and DES Cryptographic Algorithms", ISSN- 2277-1956.
[3] Rajesh R Mane (2015) "A Review on Cryptography Algorithms, Attacks and Encryption Tools", Vol. 3, Issue 9, ISSN (Online): 2320-9801
[4] Swati Kashyap, Er. Neeraj Madan, "A Review on: Network Security and Cryptographic Algorithm", Volume 5, Issue 4, April 2015. ISSN: 2277 128X.