International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 5 Issue 7, July 2018

ISSN: 2394-4404

Cryptography Algorithms - Issues On Recent Trends

T. Naga lakshmi

Assistant Professor (CSE),
Department of Computer Science & Engineering,
AITS-Rajampet

S. Jyothi

Professor,
Department of Computer Science, SPMVV, Tirupathi

Abstract: ***Cryptography in the olden days was used in keeping military information, diplomatic correspondence secure and in protecting the national security. However, the use was limited. Nowadays, the range of cryptography applications have been exploited lot in the modern area after the development of communication. To provide the security, cryptography is essentially required to ensure that data are protected against penetrations and to prevent espionage. There are various cryptography techniques used for protecting the data such as symmetric and asymmetric algorithms. The survey is done on some of the more popular and interesting cryptography algorithms currently in use and their advantages and disadvantages are also discussed. This paper provides a fair performance comparison between the various cryptography algorithms.***

IJIRAS

I. INTRODUCTION

Nowadays, cryptography plays a major role in protecting the information of technology applications. Information security is an important issue, for some applications such as ecommerce, e-banking, e-mail, medical databases, and so many more, all of them require the exchange of private information.

Cryptography is the craftsmanship and exploration of accomplishing security by encoding messages to make them clear. The introduction of cryptographic algorithms started at the 70's. The most robust and secure asymmetric algorithm was proposed by Rivest, Shamir and Adelmann (RSA) in 1977 and proved to become a defacto standard, with a large basis of products and applications that are still in operation. At the same time, a symmetric crypto-algorithm was adopted by the National Bureau of Standards, by evolving an IBM's earlier crypto-system known as LUCIFER. The Data Encryption Standard (DES) was released in January 1977, and reviewed every five years. The standardization of the DES algorithm ended in 1998, with the announcement of the Advanced Encryption Standard contest.

II. CRYPTOGRAPHY GOALS

By using cryptography many goals can be achieved, These goals can be either all achieved at the same time in one application, or only one of them, These goals are:

- ✓ *Confidentiality:* it is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.
- ✓ *Authentication:* it is the process of proving the identity, that assures the communicating entity is the one that it claimed to be, This means that the user or the system can prove their own identities to other parties who don't have personal knowledge of their identities. (The primary form of host to host authentication on the Internet today is name-based or address-based; and both of them are notoriously weak).
- ✓ *Data Integrity:* its ensures that the received message has not been altered in any way from its original form, This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.
- ✓ *Non-Repudiation:* it is mechanism used to prove that the sender really sent this message, and the message was received by the specified party, so the recipient cannot claim that the message was not sent [2].

- ✓ *Access Control:* it is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources, If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access.

III. BASIC TERMINOLOGY OF CRYPTOGRAPHY

Computers are used by millions of people for many purposes. such as banking, shopping, military, student records, etc. Privacy is a critical issue in many of these applications, how are we need to make sure that an unauthorized parties cannot read or modify messages.

- ✓ *Cryptography* is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing
- ✓ The information that we need to hide, is called plaintext. The data that will be transmitted is called cipher text.
- ✓ *Cipher* is the algorithm that is used to transform plaintext to cipher text, This method is called encryption or enciphers (encode). The opposite of cipher mechanism is called decipher (decode) that is the algorithm which recovers the cipher text, this method is called decryption, in other words it's the mechanism of converting "meaningless" data into readable data.
- ✓ *Cryptanalysis* (code breaking) is the study of principles and methods of deciphering cipher text without knowing the key, typically this includes finding and guessing the secrete key, It's a complex process involving statistical analysis, analytical reasoning, math tools and pattern-finding, The field of both cryptography and cryptanalysis is called cryptology
- ✓ *Symmetric encryption* refers to the process of converting plaintext into cipher text at the sender with the same key that will be used to retrieve plaintext from cipher text at the recipient. Asymmetric encryption refers to the process of converting plaintext into cipher text at the sender with different key that will be used to retrieve plaintext from cipher text at the recipient.

IV. TYPES OF ENCRYPTIONS

SYMMETRIC AND ASYMMETRIC ENCRYPTION

Symmetric encryption is known as secret key or single key, The receiver uses the same key which the sender uses to encrypt the data to decrypt the message,. This system was the only system used before discovering and developing the public key., A safe way of data transfer must be used to moving the secret key between the sender and the receiver in symmetric encryption which is shown in figure:1

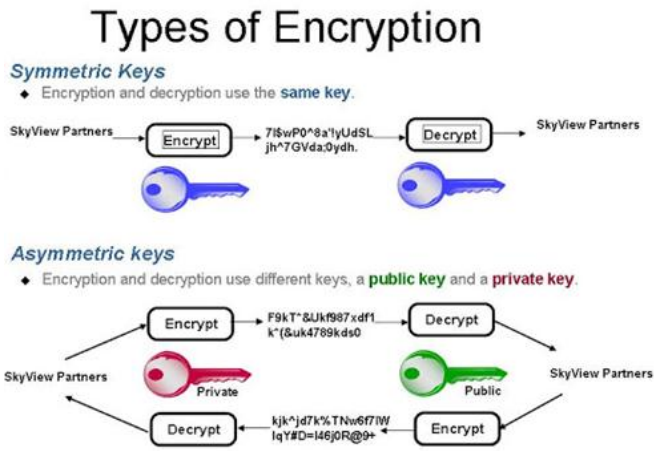


Figure 1: Types of Encryption

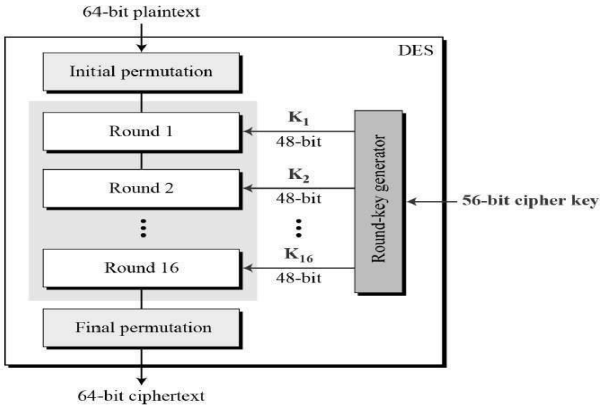
In the two-key system is also known as the public key system, one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. If a sending computer first encrypts the message with the intended receiver's public key and again with the sender's secret, private key, then the receiving computer may decrypt the message, first using its secret key and then the sender's public key which is shown in figure:1

V. CRYPTOGRAPHIC ALGORITHMS

In this paper the five commonly used encryption algorithms are discussed. They are:

A. DES

- ✓ In the first step, the 64-bit plain text message is handed over to an Initial permutation (IP) function.
- ✓ The initial permutation is performed on plain text.
- ✓ The IP produces two halves of the permuted message; Left Plain Text (LPT) and Right Plain Text (RPT).
- ✓ Now, each of LPT and RPT go through 16 rounds of encryption process.
- ✓ In the end, LPT and RPT are rejoined and a final permutation (FP) is performed on the combined block.
- ✓ The result of this process produces 64-bit cipher text. Rounds: Each of the 16 rounds, in turn, consists of the broad level steps and shown in Figure 3.1.



IJIRAS

Figure 2: DES Encryption

B. TRIPLE DES

Triple DES was designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry. Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits, but experts would argue that 112-bits in key strength is more like it. Despite slowly being phased out, Triple DES still manages to make a dependable hardware encryption solution for financial services and other industries.

C. AES ENCRYPTION

The AES cipher is almost identical to the block cipher Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. The number of internal rounds of the cipher is a function of the key length. The number of rounds for 128- bit key is 10.

The encryption process in AES involves following steps:

- ✓ Do the one-time initialization process:
  - Expand the 16-byte key to get the actual Key Block to be used.
  - Do one time initialization of the 16-byte plain text block (called State).
  - XOR the state with the key block
- ✓ For each round do the following:
  - Apply S-Box to each of the plain text bytes.
  - Rotate row k of the plain text block (i.e. state) by k bytes.
  - Perform mix columns operation.
  - XOR the state with the key block

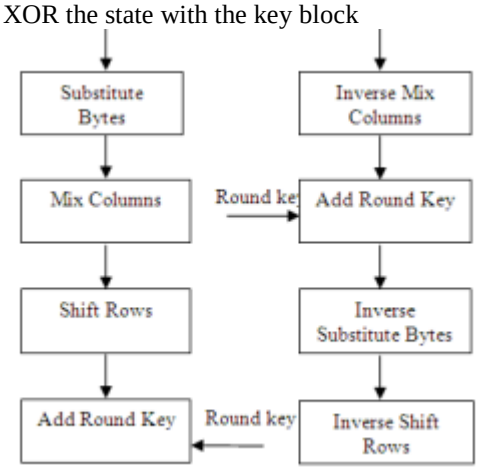


Figure 4: AES Encryption

D. BLOWFISH

Blowfish is one of the most common public domain encryption algorithms provided by Bruce Schneier - one of the world's leading cryptologists, and the president of Counterpane Systems, a consulting firm specializing in cryptography and computer security. The Blowfish algorithm was first introduced in 1993. The blowfish encryption is shown in figure below

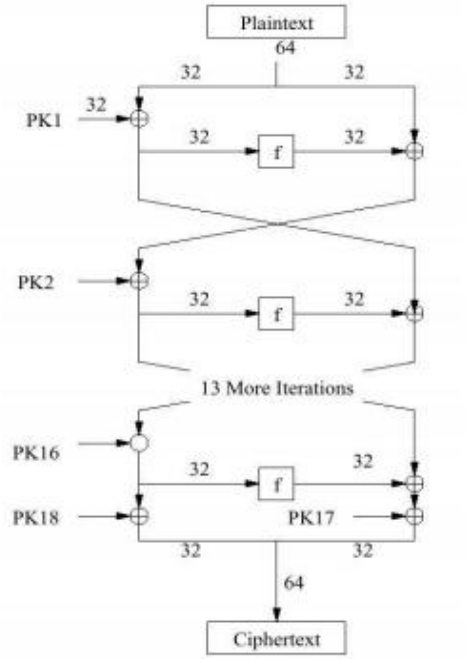


Figure 6: Blowfish Encryption

Blowfish encrypts 64-bit block cipher with variable length key. It contains two parts Subkey Generation: This process converts the key upto 448 bits long to subkeys to totaling 4168 bits. Data Encryption: This process involves the iteration of a simple function 16 times. Each round contains a key dependent permutation and key- and data dependent substitution.

E. RSA

RSA is a public key algorithm invented by Rivest, Shamir and Adleman [7]. The key used for encryption is different from (but related to) the key used for decryption. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

The keys for the RSA algorithm are generated the following way:

- ✓ Choose two distinct large prime numbers p and q.
- ✓ For security purposes, the integer's p and q should be chosen at random, and should be of similar bitlength. Prime integers can be efficiently found using a primarily test.
- ✓ Compute n = pq; n is used as the modulus for both the public and private keys
- ✓ Select the public key (i.e. the encryption key) E such that it is not a factor of $(p - 1)$ and $(q - 1)$.
- ✓ Select the private key (i.e. the decryption key) D such that the following equation is true:
  (D*E) mod (p-1)*(q-1) = 1
- ✓ For encryption, calculate the cipher text CT from the plain text PT as follows:

CT = PT^E mod N

- ✓ Select CT as the cipher text to the receiver.
- ✓ For decryption, calculate the plain text PT from the cipher text CT as follows:
  PT = CT^D mod N

VI. COMPARISONS

Comparision of cryptographic algorithms is shown as follows:

Algorithm	Created by	Key size	Block size
DES	IBM in 1975	56	**64**
AES	IBM in 1978	112 or 168	**64**
RSA	JOAN DAEMEN & VINCENT RIJMEN IN 1998	256	**128**
Blowfish	BRUCE SCHNEIER IN 1993	32 – 448	**64**

Table 1

For encryption, the best solution is to combine public- and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems. The four encryption algorithms (AES. 3DES, Blowfish and DES) have been tested with different text file sizes. The experiment results are shown below: Comparison of encryption time has been explained in the Table

Text file size (KB)	AES	3DES	BLOWFISH	DES
20	42	34	25	20
48	55	55	37	30
108	40	48	45	35
242	91	82	46	51
322	115	115	48	47
780	165	170	65	85

Table 2

VII. ISSUES ON RECENT TRENDS [7]

- ✓ The paper by Michael Scott “Missing a trick: Karatsuba variations” takes the reader for a tour through different versions of Karatsuba multiplication. This is of considerable interest for efficient implementations of public-key cryptography and in particular for Elliptic Curve Cryptography
- ✓ The paper ”Security of BLS and BGLS signatures in a multi-user setting” by MarieSarah Lacharite provides a security analysis of several signature schemes in the multi-user ´ setting: this corresponds to a realistic scenario in which multiple users are employing the scheme
- ✓ The paper ”On generating invertible circulant binary matrices with a prescribed number of ones” by Toma´s Fab ˇ si ˇ c, Otokar Gro ˇ sek, Karol Nemoga and Pavol Zajac first studies ˇ how to generate invertible binary matrices with a prescribed number of ones in a direct and efficient way.
- ✓ In the area of block cipher cryptanalysis, Tingting Cui, Huaifeng Chen, Long Wen and Meiqin Wang present statistical integral distinguishers on two block ciphers. Their paper, entitled ”Statistical Integral Attacks on CAST-256 and IDEA”, describes a 29-round key recovery attack of CAST-256 and a 4.5-round attack on IDEA.

VIII. CONCLUSION

In this remote world these days, the security for the information has turned out to be very vital since the offering and purchasing of items over the open system happen habitually. Those encryption methods are examined and broke down well to advance the execution of the encryption strategies likewise to guarantee the security procedures. This paper presents the performance evaluation of various algorithms. For better performance we need better cryptographic algorithms.

REFERENCES

[1] Atul Kahate “Cryptography and Network Security”, Tata McGraw-Hill Companies, 2008.
[2] William Stallings “Network Security Essentials (Applications and Standards)”, Pearson Education, 2004.
[3] Davis, R., “The Data Encryption Standard in Perspective,” Proceeding of Communication Societymagazine, IEEE, Volume 16 No 6, pp. 5-6, Nov. 1978.
[4] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha “Performance Evaluation of Symmetric Cryptography Algorithms,” International Journal of Electronics and Communication Technology Volume 2 Issue 3, September 2011
[5] R.L.Rivest, A.Shamir, and L.Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communication of the ACM, Volume 21 No. 2, Feb. 1978.
[6] R.L.Rivest, A.Shamir, and L.Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communication of the ACM, Volume 21 No. 2, Feb. 1978.
[7] https://link.springer.com/content/pdf/10.1007%2Fs12095-017-0269-y.pdf

IJIRAS