Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms

ISSN No. 0976-5697

Volume 6, No. 3, May 2015 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms

D Paul Joseph
Dept. of Computer Science and Technology
Sir CRR College of Engineering
Chintalapudi, India
Pauljoseph91@gmail.com

M Krishna
Dept. of Computer Science and Technology
Sir CRR College of Engineering
Eluru, India
marlapallikrishna@gmail.com

K Arun
Dept. of Computer Science and Engineering
SSN College of Engineering
Ongole, India
Karun014@gmail.com

Abstract: Today is the era of Internet and networks applications. So the Information Security has been very important issue in data communication. Any loss to information can prove to be great loss to the organization. Encryption has come up as a solution, and plays a vital role in information security system. Many techniques are needed to protect the shared data. The present work focus on cryptography to secure the data while transmitting in the network. First the data which is to be transmitted from sender to receiver in the network must be encrypted using the encryption algorithms. Secondly, by using decryption techniques the receiver can view the original data. This paper provides a in depth comparison of five most common and used symmetric and asymmetric key algorithms: DES, 3DES, AES, RSA and MD5 algorithms and comparison has made based on their performance and time of encryption and decryption, block size, key size, and breakage of encryption/decryption time, throughput.

Keywords: Encryption, Decryption, private key, public key, DES, 3DES, AES, RSA, MD5.

I. INTRODUCTION

In present world, numerous algorithms are designed and developed to provide security to the information that is spread across globally through network. These algorithms can be mainly classified as Symmetric and Asymmetric algorithms. The important issue that differentiates them is usage of keys. In symmetric algorithms, only one key is used and it is termed as private key. In other words, symmetric algorithms are also termed as private key algorithms as they use private key both for encryption and decryption.

Asymmetric key algorithm uses two keys, which can be defined as private key and public key. Private Key is used for encryption purpose whereas public key is used for decryption purposes. These algorithms are also called as public key algorithms. In advantage to private key, public key algorithms uses computational and complex mathematical methods.

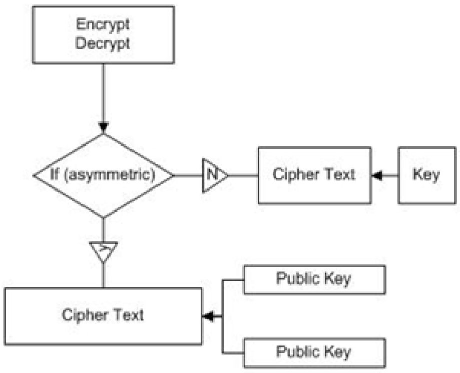


Fig1: Symmetric and Asymmetric Techniques

II. SYMMETRIC ALGORITHMS

In symmetric key algorithms, the same key is used for both encryption and decryption. Simply it can be understood as both the sender and the receiver uses same key to send or receive the message. Typically there are few algorithms which fall under this category. These can be classified as:

- Rot13
- Caesar cipher
- DES
- 3DES
- AES
- Skipjack.

III. DATA ENCRYPTION STANDARDS ALGORITHM

The DES algorithm based on LUCIFER, designed by Horst Feistel, was developed at IBM in 1972. This algorithm was approved by the National Bureau of Standards (now NIST) after assessment of DES strength and modifications by the National Security Agency (NSA), and became a Federal standard in 1977.

Features:

- Block Size:64bit
- Key size = 56 bits (in reality, 64 bits)
- Number of rounds = 16
- 16 intermediary keys, each 48 bits
- In DES, in each byte, the 8th bit is parity-check bit.

CONFERENCE PAPER
4th National Conference on Recent Trends in Information Technology 2015 on 25/03/2015
Organized by Dept. of IT, Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada-7 (A.P.) India

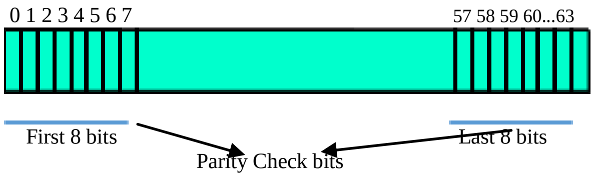


Fig. 2. Parity Check Bits

DES, 16 cycle Feistel system is used, with an overall 56-bit key permuted into 16 48-bit sub keys, one for each cycle. For decryption, the same algorithm is used, with the order of sub keys reversed.

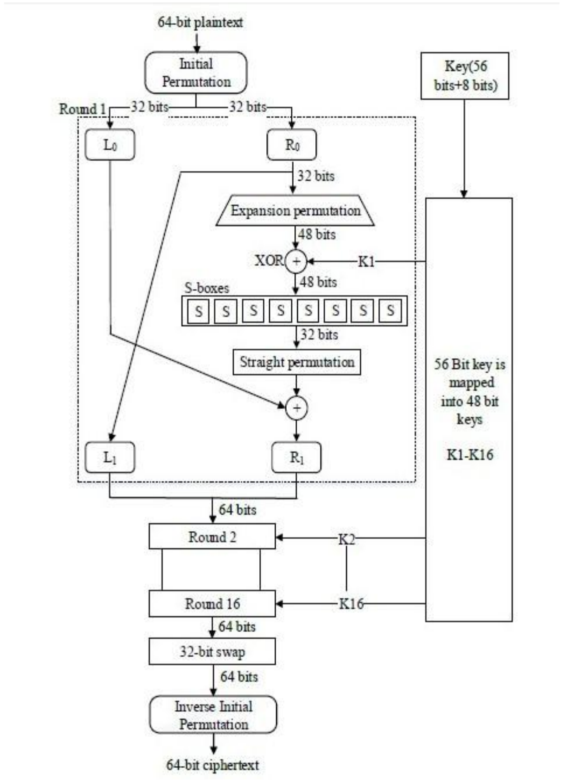


Fig. 3. Structure of DES in detail

The Left and Right blocks are 32 bits each (4bytes), totaling an overall block size of 64 bits. The hash function "f" uses "S-boxes", which takes a 4-byte data block and one of the 6-byte sub keys as input and produces 4bytes of output.

- DES uses 16 48-bits keys generated from a master 56-bit key (64 bits if we consider also parity bits)
- Weak keys: keys make the same sub-key to be generated in more than one round
- Result: reduce cipher complexity
- Weak keys can be avoided at key generation.
- DES has 4 weak keys
  - 01010101 01010101
  - FEFEFEFE FEFEFEFE
  - E0E0E0E0 F1F1F1F1
  - 1F1F1F1F 0E0E0E0E
- Using weak keys, the outcome of the Permuted Choice 1 (PC1) in the DES key schedule leads to round keys (K1---K16) being either all zeros, all ones or alternating zero-one patterns.
- Since all the sub keys are identical, and DES is a Feistel network, the encryption function becomes self-inverting; that is, encrypting twice with a weak key K produces the original plaintext.

–E_K (E_K(x)) =x for all x, i.e., the encryption and the decryption are the same

IV. TRIPLE DATA ENCRYPTION STANDARD ALGORITHM

3DES is the enhanced version of the DES algorithm. Since the DES seemed to be less efficient because of dictionary and brute force attacks, design of new algorithm was essential. In 3DES, it follows three steps.
For encryption it follows:

Encryption – Decryption - Encryption

For decryption it follows:

Decryption – Encryption – Decryption.

Features:

- Block size:64bits
- Cipher: Symmetric Block Cipher
- Key length:168 bits
- Keys:3keys(each of 64bit)

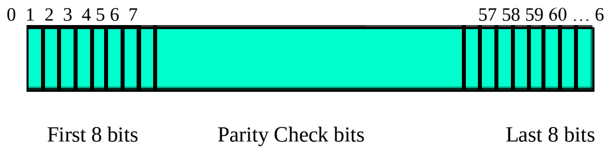
This standard specifies three keying options:

- Keying option 1: All three keys are independent
- Keying option 2: K_1 and K_2 are independent, and K_3 = K_1
- Keying option 3: All three keys are identical, i.e. K_1 = K_2 = K_3
- Keying option 1: the key space is 56 x 3= 168 bits
- Keying option 2 provides less security than option 1, with 2 × 56 = 112 key bits
- Keying option 3 is equivalent to DES, with only 56 key bits. This option provides backward compatibility with DES

Drawbacks:

- Encrypt: C = EK3 [DK2 [EK1 [P]]]
- Decrypt: P = DK1 [EK2 [DK3 [C]]]

If we use three completely different keys, will there be 168bits effectively strength?



Parity Check Bits

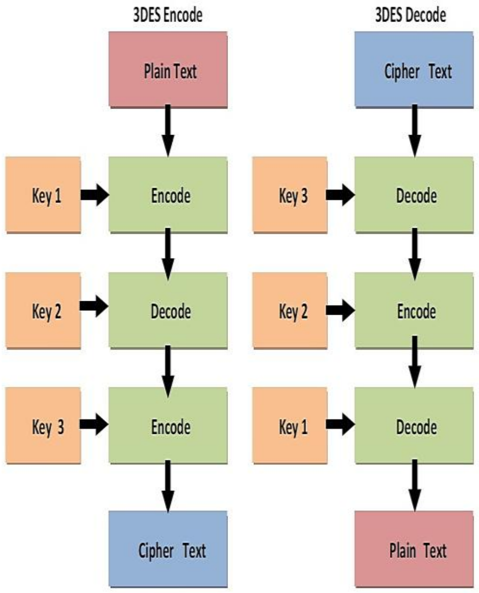


Fig. 4. Structure of 3DES

3DES works efficiently in hardware environment rather than working in software environment. Because as DES was developed to work efficiently in hardware, 3DES sucks time three times when compared to DES.

V. ADVANCED ENCRYPTION STANDARD ALGORITHM

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher which can encrypt (encipher) and decrypt (decipher) the information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext.

The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. The algorithm specified in this standard may be implemented in software, firmware, hardware, or any combination thereof. The specific implementation may depend on several factors such as the application, the environment, the technology used, etc. The algorithm shall be used in conjunction with a FIPS approved or NIST recommended mode of operation.

- Block Size: 128bits
- Key size: 128,192 and 256 bits
- Encryption: 10rounds of Encryption for 128bit
- 12 Rounds for 192 bit,14 for 256bit
- 128bit key is XORed with 128bit of plain text
- Consists of Four Operations:
    - Substitute Bytes
    - Shift Rows
    - Mix Columns
    - Add Round Key

A. *Substitute Bytes*

In AES algorithm the function of the sub byte is only nonlinear function and that operates independently on each byte of the state using a substitution table (Sbox). It substitutes all bytes of the state array using a LUT which is a 16x16 matrix of bytes, often called S-box Units.

B. *Shift Rows*

As transformation is almost the same in the decryption process except that the shifting offsets have different values. The main goal of this process is to correlate and scramble the byte order inside each 128-bit block. In the shift the bytes in the last three rows of the State are cyclically shifted over different numbers of bytes (offsets).in this process the row 0 is not shifted, row0 is shifted one byte to the left, row 2 is shifted two bytes to the left and row 3 is shifted three bytes to the left.

C. *Mix Column Transformation*

This transformation is based on Galois Field multiplication. Each byte of a column is replaced with another value that is a function of all four bytes in the given column. The Mix Columns transformation is performed on the State column-by column.

D. *Add Round Key*

In this operation, the round key is applied to the State by simple bit by bit XOR. Key Expansion unit generates the next round key as for three different key sizes. AES consist of 10, 12 or 14 rounds. After every round a new round key is produced. This process utilizes the concept of shifting the bytes and substitution of bytes which were used in data processing unit

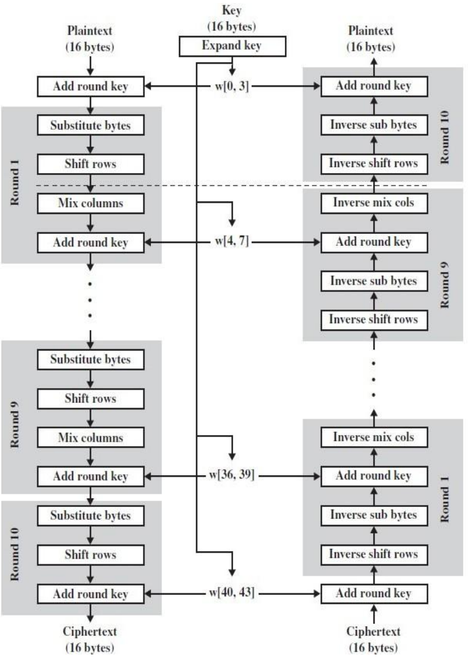


Fig. 5. Structure of Advance Encryption Standard Algorithm

VI. DISADVATNAGES OF SYMMETRIC TECHNIQUES

A major problem with such a system is that the sender and receiver must know the key prior to transmission. This requirement makes such a system difficult to use in practice. The key cannot be openly transmitted since that would compromise the security of system. One possibility is for the two parties to meet and exchange the keys prior to transmitting their messages. However, this exchange becomes more difficult when many parties are involved in a communications network.

Secondly, most of the symmetric algorithms contain more number of rounds, which leads to large processing time. Thirdly, these algorithms contain a bit of smaller block sizes, which may lead to numerous times of block division. Since these contains only single key for all transmissions, if that key is anyhow known, then whole transmission would be a failure.

Another disadvantage is that there is no provision for data origin authentication and data integrity protection. In other words, the recipient can neither authenticate the sender nor verify that the decrypted message is the same as the original message and finally cannot provide digital signatures that cannot be repudiated

VII. ASYMMETRIC ALGORITHMS

Asymmetric cryptography algorithms use two keys which can be referred as public key and private key. Public key is used for encryption purpose and private key is used for decryption purpose. These two keys are mathematically related, but it is very difficult to obtain one from the other unless one knows the transformation. The public key can be revealed without compromising the security of the system. The corresponding private key, however, must not be revealed to any party. Currently information is electronically processed and conveyed through public networks. The main objective of cryptography is, to conceal the content of messages transmitted through insecure channels such that it guarantees privacy and confidentiality in the communications to the authorized users. The different algorithms designed under this category are RSA, MD5 and SHA.

VIII. RIVEST, ADI SHAMIR, AND LEONARD ADLEMAN ALGORITHM

RSA is designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key, based on number theory, which is a block cipher system. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose. Sender encrypts the message using Receiver public key and when the message gets transmit to receiver, then receiver can decrypt it using his own private key.

Key Generation Procedure:

- Choose two distinct large random prime numbers p & q such that $p \neq q$.
- Compute $n= p \times q$
- Calculate: $\varphi (n) = (p-1) (q-1)$.
- Choose an integer e such that $1<e<\varphi (n)$
- Compute d to satisfy the congruence relation $d \times e = 1 \bmod \varphi (n)$; d is kept as private.
- The public key is (n, e) and the private key is (n, d). Keep d, p, q and φ secret.
- Encryption text: P < n Cipher text: $C= P^e \bmod n$.
- Decryption text: C.Plaintext: $P=C^d \bmod n$

RSA encryption is a deterministic encryption algorithm (i.e., has no random component) an attacker can successfully launch a chosen plaintext attack against the cryptosystem, by encrypting likely plaintexts under the public key and test if they are equal to the cipher text.

RSA has the property that the product of two cipher texts is equal to the encryption of the product of the respective plaintexts. That is $m_1^e m_2^e \equiv (m_1 m_2)^e \pmod{n}$. Because of this multiplicative property a chosen-cipher text attack is possible.

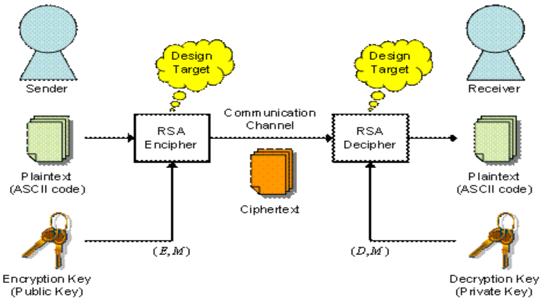


Fig. 6. Structure of RSA Algorithm

E.g., an attacker, who wants to know the decryption of a cipher text $c \equiv m^e \pmod{n}$ may ask the holder of the private key to decrypt an unsuspicious-looking cipher text $c' \equiv cr^e \pmod{n}$ for some value *r* chosen by the attacker. Because of the multiplicative property *c′* is the encryption of *mr* (mod *n*). Hence, if the attacker is successful with the attack, he will learn *mr* (mod *n*) from which he can derive the message *m* by multiplying *mr* with the modular inverse of *r* modulo *n*.

IX. MESSAGE DIGEST ALGORITHM

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

Advantages of MD5:

- Utilizes a fast computation algorithm
- Provides collision resistance
- Is in widespread use
- Provides a one-way hash.

MD5 is one in a series of message digest algorithms designed to be a secure replacement for MD4. But later Md5 was proved that it was vulnerable to Collision Resistant, Preimage Vulnerability and some other vulnerability. In addition it was also not applicable to SSL certificates and Digital certificates.it also contains security flaws and vulnerabilities. It is less secure than the SHA-1 algorithm.

MD5 uses the Merkle–Damgård construction, so if two prefixes with the same hash can be constructed, a common suffix can be added to both to make the collision more likely to be accepted as valid data by the application using it. An example MD5 collision, with the two messages differing in 6 bits, is shown in below figures:

```
d131dd02c5e6eec4   693d9a0698aff95c 2fcab58712467eab
4004583eb8fb7f89 55ad340609f4b302 83e488832571415a
085125e8f7cdc99f   d91dbdf280373c5b d8823e3156348f5b
ae6dacd436c919c6 dd53e2b487da03fd 02396306d248cda0
e99f33420f577ee8    ce54b67080a80d1e c69821bcb6a88393
96f9652b6ff72a70
```

```
d131dd02c5e6eec4 693d9a0698aff95c 2fcab58712467eab
4004583eb8fb7f89
55ad340609f4b302 83e488832571415a 085125e8f7cdc99f
d91dbdf280373c5b
d8823e3156348f5b ae6dacd436c919c6 dd53e2b487da03fd
02396306d248cda0
e99f33420f577ee8 ce54b67080a80d1e c69821bcb6a88393
96f9652b6ff72a70
```

```
d131dd02c5e6eec4   693d9a0698aff95c 2fcab50712467eab
4004583eb8fb7f89 55ad340609f4b302 83e4888325f1415a
085125e8f7cdc99f    d91dbd7280373c5b d8823e3156348f5b
ae6dacd436c919c6 dd53e23487da03fd 02396306d248cda0
e99f33420f577ee8    ce54b67080280d1e c69821bcb6a88393
96f965ab6ff72a70
```

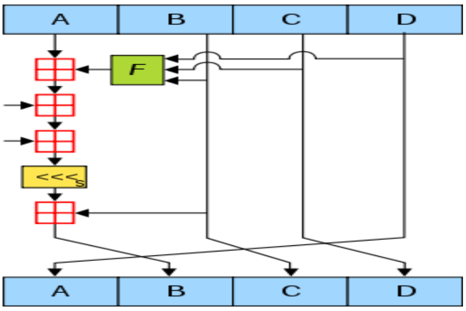


Fig. 7. Structure of MD5 Algorithm

Table I. Symmetric versus Asymmetric

Algorithms	***DES***	***3DES***	***AES***	***RSA***	***MD5***
Author	IBM	IBM	Joan Daemen, Incent Rijmen	Rivest, Shamir, Adleman	Ronald Rivest
Year	1975	1978	1998	1977	1992
Structure	Festial	Festial	Substitution Permutation	Public key algorithm	Merkle Damgard
Rounds	16	48	10, 12, 14	1	4
Key (bits)	56	168	128, 192, 256	Greater than 1024bits	512
Block size (in bits)	64	64	128	128	512
Security	Vulnerable	Adequate vulnerable	Strongly ciphered	High security	Moderately secured
Execution speed	Moderate	Moderate	Faster	Slower	Moderate
Vulnerabilities	Brute-Force, Cryptanalysis	Cryptanalysis	Brute force(not yet proved)	Oracle attacks	Collision, Preimage vulnerability
Power Consumption	Low	Low	Low	High	Moderate
Encryption/ Decryption speed	Moderate	Moderate	Faster	Low	Faster
Possible Keys	2^56	2^112, 2^168	2^128, 2^192, 2^256	2^128	2^512
Resultant size	Resultant text size is lesser or equal to original text.			Resultant text size is greater than original text.	
Type of Algorithm	Symmetric Algorithm			Asymmetric Algorithm	
Usage	Can be used for only Encryption and Decryption(Confidentiality)			Can be used for Confidentiality as well as Integrity and Non-repudiation checks.	

X. COMPARISION OF SYMMETRIC AND ASYMMETRIC ALGORITHMS

- Larger the block size→slower execution
- Larger key size→High security
- Increased Rounds→more execution time
- Larger key size→more arithmetical operations

→More consumption of time

XI. Conclusion

In this paper a new comparative study between DES,3DES, AES, RSA and MD5 were presented on various factors Which are key length, cipher type, block size, developed, possible keys. All these algorithms are compared

CONFERENCE PAPER
4th National Conference on Recent Trends in Information Technology 2015 on 25/03/2015
Organized by Dept. of IT, Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada-7 (A.P.) India

in sense of encryption and decryption time and their results are jotted down. Though RSA also withstands to symmetric algorithms, as its larger prime number leading to great encryption/decryption time, it cannot be proved as best one.But overall theoretical and practical simulation experiments proved AES is better in terms of execution speed, consumption of time, Time to break the algorithm and security. Our future work will focus on comparison of existing cryptographic algorithms and it will include practicality on image and audio data further more resulting for the advanced encryption techniques.

XII. REFERENCES

[1] Xinmiao Zhang and Keshab K. Parhi "Implementation approaches for the Advanced Encryption Standard Algorithm" IEEE 2002

[2] Dawn Xiaodong Song David Wagner Adrian Perring "Practical Techniques for Searches on Encrypted Data" Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on 2002.

[3] Chia Long Wu, Chen Hao Hu, "Computational Complexity Theoretical Analyses on Cryptographic Algorithms for Computer Security Applications.

[4] Abdel-Karim Al Tamimi, Swati. "Performance Analysis of Data Encryption Algorithms ", International Journal of Advanced Research in Computer Science and Software Engineering 3(2), pp. 147-149, February – 2013.

[5] Nidhi Singhal1, J.P.S.Raina2," Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technologypp.177-181, Aug 2011.

[6] Pratap Chandra Mandal, " Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish ", Journal of Global Research in Computer Science Department of Computer Application, vol 3, pp 67-70, August 2012.