Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms

D Paul Joseph¹, M Krishna², K Arun³
C.R Reddy College of Engineering¹
Assoc. Professor, C.R Reddy College Of Engineering²
Assoc. Professor, SSN Engineering College³

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 comparison between 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 encryption/decryption time, in the form of throughput.

Index Terms: Encryption, Decryption, private key, public key, DES, 3DES, AES, RSA, MD5

1. 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

2. 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.

3. DATA ENCRYPTION STANDARD 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: 56bits (in reality, 64bits)
- Number of rounds: 16
- 16 intermediary keys, each 48bits
- In DES, in each byte, the 8th bit is parity-check bit.

**Fig 2. Parity Check Bits**

Each parity-check bit is the XOR of previous bit. In DES, 16cycle Feistel system is used, with an overall 56-bit key permuted into 1648-bitsubkeys, one for each cycle. For decryption, the same algorithm is used, with the order of sub keys reversed.

The Left and Right blocks are 32-bit each (4bytes), totaling an overall block size of 64bits. The hash function "H" uses "S-boxes", which takes a 4-byte datablock and one of the 6-byte subkeys as input and produces 4byteofoutput.

- DES uses 1648-bits keys generated from master 56-bit key (64bit if we consider all parity bits)
- Weakkeys: keys make the same sub-key to be generated in more than one round
- Result: reduce ciphertext complexity
- Weakkeys can be avoided at key generation.
- DES has 4 weakkeys
  - 01010101010101
  - FEFEFEFEFEFEFEE
  - E0E0E0EF1F1F1F1
  - 1F1F1F1F0E0E0E0

Using weakkeys, the outcome of the Permed Choice1(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 weakkeyK produces the original plain text.

- \( EK(EK(x)) = x \) for all x, i.e., the encryption and the decryption are the same.

### 4. Triple Data Encryption Standard Algorithm

![Diagram](image)

**Fig 3. Structure of DES**

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 algorithms was essential. In 3DES, it follows three steps.

- **For encryption it follows:**
  - *Encryption - Decryption - Encryption*
- **For decryption it follows:**
  - *Decrypt - Encrypt - Decrypt.*

**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 56×3 = 168bits.
- 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.

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 off sets 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, row 0 is shifted one byte to the left, row 2 is shifted two 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.

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

D. Shift Rows:
As transformation is almost the same in the decryption process except that the shifting off sets 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, row 0 is shifted one byte to the left, row 2 is shifted two bytes to the left.

E. 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

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

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

5. ADVANCED ENCRYPTION STANDARDS 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 that can encrypt (encipher) and decrypt (decipher) 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.
- 12 Rounds for 192 bit, 14 for 256bit
gated column. The Mix Columns transformation is performed on the State column-by-column.

Since these contains only single key for all transmissions, if that key is anyhow known, then whole transmission would be a failure.

7. Asymmetric Algorithms

Asymmetric cryptography algorithms uses 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.

8. Rivest, AdiShamir, 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 larger and odd prime numbers p & q such that p≠q.
- Compute n = pq.
- Calculate: φ(n) = (p-1)(q-1).
- Choose an integer e such that 1<e<φ(n).
- Computed to satisfy the congruence relation d xe = 1 mod φ(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 mod n.

Decryption text: C Plaintext: C = P^d mod 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 ciphertexts is equal to the encryption of the product of the respective plaintexts. That is \( m_1m_2^e \equiv (m_1m_2)^e \pmod{n} \). Because of this multiplicative property a chosen-ciphertext attack is possible.

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

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:

```
d131dd02c56e6e44 693d9a698af95c3
2fcbab7832467eab 4004583eb8f789
55ad3406097f4b2b 83e488832571415a
085125e877c499f d91dbd72803733e5b
8828b3156348f5b 02396306d248cda0
d53e2b47103f3f 02396306d248cda0
e99f34205777e8 e54b67080a801e
f89821b6a83393 96f9652b6f727a0
```

### 10. COMPARISON OF SYMMETRIC AND ASYMMETRIC ALGORITHMS

- Larger the block size \( \rightarrow \) slower execution
- Larger key size \( \rightarrow \) High security
- Increased Rounds \( \rightarrow \) more execution time
- Larger key size \( \rightarrow \) more arithmetical operations \( \rightarrow \) More consumption of time
Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms

Table 1. Symmetric versus Asymmetric

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>DES</th>
<th>3DES</th>
<th>AES</th>
<th>RSA</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td>IBM</td>
<td>IBM</td>
<td>JoanDaemen, Incet Rijmen</td>
<td>Rivest, Shamir, Adleman</td>
<td>Ronald Rivest</td>
</tr>
<tr>
<td>Structure</td>
<td>Festial</td>
<td>Festial</td>
<td>Substitution Permutation</td>
<td>Public key algorithm</td>
<td>Merkle Damgard</td>
</tr>
<tr>
<td>Rounds</td>
<td>16</td>
<td>48</td>
<td>10, 12, 14</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Key (bits)</td>
<td>56</td>
<td>168</td>
<td>128, 192, 256</td>
<td>Greater than 1024bits</td>
<td>512</td>
</tr>
<tr>
<td>Block size (in bits)</td>
<td>64</td>
<td>64</td>
<td>128</td>
<td>128</td>
<td>512</td>
</tr>
<tr>
<td>Security</td>
<td>Vulnerable</td>
<td>Adequate vulnerable</td>
<td>Strongly ciphered</td>
<td>High security</td>
<td>Moderately secured</td>
</tr>
<tr>
<td>Execution speed</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Faster</td>
<td>Slower</td>
<td>Moderate</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Brute-Force, Cryptanalysis</td>
<td>Cryptanalysis</td>
<td>Brute force(not yet proved)</td>
<td>Oracle attacks</td>
<td>Collision, Preimage vulnerability</td>
</tr>
<tr>
<td>Power Consumption</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Encryption/Decryption speed</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Faster</td>
<td>Low</td>
<td>Faster</td>
</tr>
<tr>
<td>Possible Keys</td>
<td>$2^{56}$</td>
<td>$2^{112}, 2^{168}$</td>
<td>$2^{128}, 2^{192}, 2^{256}$</td>
<td>$2^{128}$</td>
<td>$2^{512}$</td>
</tr>
</tbody>
</table>

11. CONCLUSION

In this paper a new comparative study between DES, 3DES, AES, RSA and MD5 were represented on various factors which are key length, cipher type, block size, developed, possible keys. 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.

REFERENCES