Comparative Study of Different Cryptographic Algorithms

Vanitha M1, Mangayarkarasi R2

1,2School of Information Technology and Engineering, VIT University, Vellore, India.
Email: mvanitha@vit.ac.in

Received on 25-10-2016
Accepted on 02-11-2016

Abstract:
As technologies in multimedia are growing quickly, a huge amount of multimedia data is produced and broadcasted. The internet also permits the extensive allocation of data. Because of this it becomes very simple to duplicate, alter and reproduce digital information. This becomes a serious safety and security issue and it became mandatory to ensure protection because. Of its confidentiality which may tolerate some crucial information that should be not or partly be accessed by the users which are general. The second issue with digital videos and information is that small alterations can be made with the help of extensively available minute devices, again putting the safety issue on stake. Cryptography focuses on protecting such crucial information being generated by digital devices and then being transmitted. This paper compares the AES, DES and Present cryptographic algorithms.

1. Introduction

Encryption in cryptography deals with encoding the message in such a manner that only the desired people could read it and not the undesired parties such as hackers. The basic idea of encryption is to prevent the hackers from reading the text being encrypted. Number of benchmarks associate with cryptography. Model protocols and algorithms serve as the basis for studies. In the modern era cryptography is not merely used to transmit secure defense information, but is considered as the key components of the security system of any association and acts as the benchmarks of the industry for providing granting security of data, trust, restricted admittance to information, and transactions of financial nature running electronically. The data which is to be sent is called the plaintext and is comprehensible and recognizable by the computer and the humans. While cipher text is the message which is neither understood by the human nor is completely understood by the system until it is completely decoded. Any system providing encryption and decryption is called a
cryptosystem. The cryptosystem examines the algorithm to be bought in use for encryption and decryption and the software module assisting it. Vitally not only the performance of the algorithm is the subject to be focused upon but another significant point is the design of the algorithm as both of them go together for appropriate functioning of the algorithm. But this faces some problems and negations. Another factor that challenges algorithm application is implementation with hardware. Even a minute change can bring significant changes.

In this paper, comparative study of different cryptography algorithms on the basis of different factors. Our objective is to show the demerits of DES and AES, the widely used cryptographic algorithms and how PRESENT algorithm a lightweight cryptographic algorithm is better than these algorithms.

2. Related Works

There are three types of cryptosystems: Symmetric, Asymmetric and hash functions. Symmetric key encryption uses one key encrypts and decrypt. Asymmetric uses two keys to encrypt and decrypt.

a) Symmetric Key – uses one key for encrypting and decrypting. Eg- AES and DES

b) Asymmetric key – uses two keys, private and public keys, one for encrypting and other for decrypting.

2.1. DES

DES concretes its basis from Substitution Permutation Network which is Feistal in nature. DES brings in use a key of 56 bits length and is partitioned using brute force method and these days is taken as outdated. The general 56 bit key is permuted into 16 length for which a sub key of length 48 bits is used, for every particular cycle. For decryption of the cipher text is used with the difference that the used key is turn around. The size of the block is 64 bits owing to the L and R blocks having length of 32 bits each. Using the s-boxes the design of the hash function is layer. This takes as input the 32 bit block and 48 bit key and gives output a 32 bit block. At times the key is considered to be of length 64 bits where apart from the 56 bits, the 8 bits are used for checking the parity. DES provides many loopholes as it is a linear key block algorithm and also has a small key size. [2][4]

Disadvantages of DES:

- The key size of 56 bits act as the greatest problem of the DES. With this short length cracking the key becomes an easy and quick task, hence subjecting the security issues on stake.

- Since DES was designed for hardware its implementation becomes relatively difficult and sluggish in software.
2.2. AES

The design standards for AES are set by substitution permutation network which is a design principle and is moduled for both software as well hardware. Working in a distinct manner as compared to DES it does not make use of feistal network. AES has a block size of 128 bits and has keys of length of either 128 bits or 192 or 256 bits respectively. AES algorithm says that both the block length and the key size should be manifolds of 32 and the least and last limits for each of them should be 128 bits and 256 bits respectively. AES functions using a 4x4 column-major order matrix of bytes, and are termed as state. A few versions of AES may have a block size of bigger length and can contain additive columns in the matrix. In AES the length of the key tells about the number of recurrence of the makeovers of the plaintext which is to be changed to the cipher text. The number of reoccurrences of the makeovers should be as follows:

- 10 series of recurrence for 128-bit keys.
- 12 series of recurrence for 192-bit keys.
- 14 series of recurrence for 256-bit keys.

Every round contains 5 steps which same to be same but actually distinct stages. After the plaintext is encrypted the converse key is functioned to decode the cipher text using decryption process [2][4].

Limitations

- It becomes cumbersome to apply converse cipher on a smart card.
- It brings into use extra number of codes and rounds.
- The cipher and its converse make use of diverse codes.
- The converse cipher on a hardware platform can partially employ the circuitry used for realizing the cipher.

2.3. Present algorithm

PRESENT is a new technology, an ultra-lightweight block cipher algorithm, developed by the Orange Labs (France), Ruhr University Bochum (Germany) and the Technical University of Denmark. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe designed PRESENT. It is 2.5 times smaller than AES (Advanced Encryption Standard), hence making it most compact approach for encryption of data. Present algorithm uses SP NETWORKS as its basis. It comprises of 31 circles or rounds. The length of the block is 64 bits and 80 and 128 bits is assisted as key length. Usually the key of length 80 bits is proposed...
for a broader range of applications. This is apt for any application requiring minimal security generally employed in tag based deployments but it acts significantly this algorithm competes with the design benchmarks of the design focused ciphers and thus permits us to conclude a genuine contrast.

**Benefits of Present**

When we plan for a block cipher which will be used in very restricted atmosphere, we focus on the fact that emphasis should not be laid on a wide spectrum of applications as we have AES in work for that purpose. But we are considering applications here with very absolute purposes. The above will generally abide to the following traits.

- Implementation of cipher should be in hardware.
- The level of safety desired by an application is average in nature. For this 80 bit security will be adequate.
- The applications do not involve decryption for voluminous data, therefore the application must be augmented for execution and space avoiding excessive applied approach. In a few applications it is possible that the device is fed with the key at the time of manufacturing itself. In such a situation no case arises to re feed the device with the key.
- When the security matter is resolved then the foremost consideration will be the space required physically. This requirement is trailed by the requirement for timing.
- Some applications will implement only the process of encryption whose head preference is management of space.

3. **Comparative Study**

In this section we will deal with the comparative study of DES, AES and PRESENT. Starting with DES, DES was developed in 1977, designed with care to work in hardware better than software For example; 16 bit switching from 30 bits is easier in hardware as compared to software. DES uses 56 bit key to encrypt 64 bit block size data which totals to 72 quadrillion options but could not meet the efficiency required for present computing requirements. It is also vulnerable to attacks like brute force. Hence DES is considered to be insecure as it could not sustain the development to technology.

AES outclasses DES both in software and in hardware [5],[6]. To replace DES, Rijndael algorithm was chosen for AES. It is an enhanced version of Rijndael algorithm. Advance Encryption Standard assessment conditions among others were [7],[8],[9],[10]
• Security

• performance of Software and Hardware

• Appropriateness in restricted-space settings

• Resistance to power analysis and implementation attacks

Rijndael was submitted by Joan Daemen and Vincent Rijmen. Rijndael’s Grouping of safety, performance, efficiency, implement ability, and flexibility, when taken together made it a suitable choice for AES. According to AES’s design it is faster in software and works competently in hardware. Its performance is faster when used for small devices like, smart phones, smart cards etc. Due to its large block size and long keys it provides more security than DES.

PRESENT algorithm is a combination of AES and SERPENT. The combination of characteristics of both AES and SERPENT makes it highly secure and compact. The main aim while scheming PRESENT was simplicity along with security and efficient implementation [1][3].

<table>
<thead>
<tr>
<th>Factors</th>
<th>DES</th>
<th>AES</th>
<th>PRESENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key length</td>
<td>56,64 bits</td>
<td>128, 192, or 256 bits</td>
<td>80, 128 bits</td>
</tr>
<tr>
<td>Cipher type</td>
<td>Symmetric block cypher</td>
<td>Symmetric block cypher</td>
<td>Symmetric block cypher</td>
</tr>
<tr>
<td>Block size</td>
<td>64 bits</td>
<td>128 bits</td>
<td>64 bits</td>
</tr>
<tr>
<td>Structure</td>
<td>Balanced Feistel network</td>
<td>Substitution-permutation network</td>
<td>Substitution-permutation network</td>
</tr>
<tr>
<td>Execution time(milliseconds) for input size 49,59,100 (Kbytes)</td>
<td>29, 33, 49</td>
<td>56, 38, 90</td>
<td>2.5 times smaller than AES</td>
</tr>
<tr>
<td>Rounds</td>
<td>16</td>
<td>10,12,14 (depending on key size)</td>
<td>31</td>
</tr>
</tbody>
</table>

4. Conclusion

This paper deals with a new comparative study between different crypt analysis algorithm such as DES, AES and PRESENT based on different factors and conditions such as block size, structure, key length etc. Among the factors the time complexity of PRESENT is smaller than DES and AES as well as PRESENT is the most compact encryption method, making it most efficient and proves to be better than AES and DES.
References


