Design of a Hybrid Cryptographic Algorithm

Wang Tianfu, K. Ramesh Babu
School of Computing Science and Engineering, VIT University, TamilNadu, India
165559672@163.com

Abstract—Internet is a public-interacted system; the amount of information exchanged over the internet is completely not safe. Protecting the information transmitted over the network is a difficult task and the data security issues become increasingly important. At present, various types of cryptographic algorithms provide high security to information on networks, but there are also has some drawbacks. To improve the strength of these algorithms, we propose a new hybrid cryptographic algorithm in this paper. The algorithm is designed using combination of two symmetric cryptographic techniques. These two primitives can be achieved with the help of Advanced Encryption Standard (AES) and Data Encryption Standard (DES). This new hybrid cryptographic algorithm has been designed for better security with integrity.

Keyword: AES, DES, Hybrid, Cryptographic, Security.

1. INTRODUCTION

Curiosity is the most common human characteristic. In order to secure the transmission of messages, spies, military and business people sometimes pass misleading information.

A key is used in conjunction with a cipher to encrypt or decrypt text. The key might appear meaningful, as would be the case with a character string used as a password, but this transformation is irrelevant the functionality of a key lies in its being a string of bit determining the mapping of the plain text to the cipher text [2].

1.1 Why need hybrid cryptographic algorithm?

A Computer Network is an interconnected group of autonomous computing nodes, which use a well defined, mutually agreed set of rules and conventions known as protocols, to interact with one-another meaningfully and allow resource sharing preferably in a predictable and controllable manner. Communication has a major impact on today’s business. It is desired to communicate data with high security. With the rapid development of network technology, internet attacks are also versatile, the traditional encryption algorithms (single data encryption) is not enough for today’s information security over internet, so we propose this hybrid Cryptograph Algorithm.

2. METHODOLOGIES

2.1 AES

Advanced Encryption Standard (AES) is based on a design principle known as a substitution-permutation network[8]. It is fast in both software and hardware. Unlike its predecessor, DES, AES does not use a Feistel network [1].

AES has a fixed block size of 128 bit and a key size of 128, 192, or 256 bit, whereas Rijndael has specified with block and key sizes in multiples of 32 bit, with a minimum of 128 bit. The block size has a maximum of 256 bit but the key size has no theoretical maximum [5].
AES operates on a 4x4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field. AES encryption and decryption process is shown in Fig. 1.


![Fig. 2 AES Substitute byte process](image)

**Shift rows** [2] — a simple permutation.

![Fig. 3 AES Shift rows process](image)

**Mix columns** [2] — transformation operates on the State column-by-column, treating each column as a four-term polynomial, the columns are considered as polynomials over GF (2^8)

![Fig. 4 AES Mix columns process](image)

**Add round key** [2] — a simple bitwise XOR of the current block with a portion of the expanded key.

![Fig. 5 AES Add round key process](image)

### 2.2 DES

DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bit and transforms it through a series of complicated operations into another ciphertext bit string of the same length. DES also uses a key to customize the transformation, so that decryption can only be performed by those who know the particular key used to encrypt. In the case of DES, the block size is 64 bit [6], but only 56 bit are used and the remaining 8 bit can be used for parity, and then discarded in the algorithm.[3] Therefore, the effective key length of DES is 56 bit. The algorithm’s overall structure is shown in Fig. 6: there are 16 identical same processes, termed rounds. There is also an initial and final permutation, known as IP and FP (the FP is inverse function of IP (IP ”revocation” FP operations, and vice versa)).

Before the main rounds, the block is divided into two 32 bit half block and processed at same times; this crossing process is known as the Feistel scheme. Feistel scheme is used to ensure the similarity of both the encryption and decryption processes. The only difference is the sub-key, which is reversed and used in decryption process and remaining part it is the same. This design simplifies the algorithm implementation, especially for hard implementation. The ⊕ symbol denotes the (XOR) operation.
Fig. 1 AES overall structure

Fig. 6 DES overall structure
The “F- function” scrambles data process with one sub-key, then the output from F-function doing the XOR operation with other half block data, and the halves are swapped before the next round. After the final round, the halves are not swapped; this is a feature of the Feistel structure which makes encryption and decryption similar processes [3].

2.2.1 F-function

The F-function, depicted in Figure 7, operates on half a block (32 bit) at a time and consists of four stages [8]:

Expansion — expand 32 bit half block to 48 bit, the output divided into 8 blocks, each block has 6 bit (4 bit is corresponding outputs and other 2 bit is neighbor block).

Key mixing — uses XOR operation process the expanding result and mix with one sub-key. 16 48-bit uses to every F function transform.

Substitution — after key mixing operation, blocks divided into eight 6-bit blocks, and then uses S-boxes to perform a byte-by-byte substitution of the block (same as substitution byte operation in AES).

Permutation — the 32 outputs of S-boxes restructuring by fix permutation.

3. DESIGN ISSUES OF HYBRID CRYPTOGRAPHIC ALGORITHM

It is a design for transfer data with better security. At present, various types of cryptographic algorithms provide high security to information on networks, but there are also has some drawbacks. This hybrid algorithm is designed for better security by combinations of AES and DES.

3.1 Overall Structure

Fig. 8 show the overall structure of the design, each byte of the plaintext is uses AES or DES algorithms; $k_a$ and $k_d$ represent the key for AES and DES.

For example, we have 8 bit size of plaintext, first bit uses AES to encrypt and second bit uses DES to encrypt. The decryption process is invert of the
4. RESULT AND CONCLUSION

The AES, DES and Hybrid algorithms have been implemented in VC++ and the following results were obtained. In Fig. 9 shows main interface, which include multiple feature I. AES Encryption, II. AES Decryption, III. DES Encryption, IV. DES Decryption, V. Hybrid Algorithm Encryption, VI. Hybrid Algorithm Decryption, VII. Encrypt/Decrypt file, VIII. Encrypt/Decrypt String.

4.1 Result of AES and DES algorithm

Fig. 10 shows that string Encryption and Decryption by AES, Fig. 11 shows that file Encryption and Decryption by AES. Fig. 12 shows that string Encryption and Decryption by DES, Fig. 13 shows that file Encryption and Decryption by DES.
**Fig. 11** File Encryption & Decryption by AES

**Fig. 12** String Encryption & Decryption by DES
4.1 Result of Hybrid Cryptographic algorithm

Fig. 14 shows that string Encryption and Decryption use Hybrid algorithm, Fig. 14 shows that file Encryption and Decryption use Hybrid algorithm, From those results, we use same plaintext and key to encryption by three different algorithms, the output by used Hybrid algorithm is more complex. Transform data will more security than other two algorithms.

Fig. 13 File Encryption & Decryption by DES

Fig. 14 String Encryption & Decryption by Hybrid Cryptographic algorithm
References


