AHCS (Advanced Hybrid Cryptographic System)

Mohit Prakash

[1]Department of Computer Science and Engineering, Bhagwan Parshuram Institute Of Technology, PSP-4,Sector-17,Rohini,Delhi-89

Abstract: ***At present, various types of cryptographic algorithms provide high security to information networks, but they are also have some drawbacks .To improve the strength of these algorithms, we propose a new hybrid cryptographic algorithm in this paper. The proposed algorithm makes use of both the public and the private key encryption algorithms.***

Keywords: Hybrid Encryption, Cryptography, Symmetric Key Encryption, Asymmetric Key encryption

1. Introduction

A hybrid cryptosystem is a system that uses a combination of both symmetric and asymmetric cryptosystems. It is created by combining the strengths of both the primitive systems.

In asymmetric key systems, the procedure is complicated and is mathematically time consuming. Therefore, it is generally inefficient than symmetric cryptosystems. The asymmetric or public key systems have a high cost of encrypting messages, hence, they are prohibitive.

Symmetric key ciphers have been known to be susceptible to cryptanalysis and other attacks such as brute forcing etc. However, symmetric key algorithms offer efficiency since they are not as time consuming as compared with public key or asymmetric key algorithms.

A hybrid encryption scheme [7] is one that blends the convenience of an asymmetric encryption scheme with the effectiveness of a symmetric encryption scheme.

Hybrid encryption is achieved through data transfer using unique session keys along with symmetrical encryption. Public key encryption is implemented for random symmetric key encryption. The recipient then uses the public key encryption method to decrypt the symmetric key. Once the symmetric key is recovered, it is then used to decrypt the message. The combination of encryption methods has various advantages. One is that a connection channel is established between two users' sets of equipment. Users then have the ability to communicate through hybrid encryption. Asymmetric encryption can slow down the encryption process, but with the simultaneous use of symmetric encryption, both forms of encryption are enhanced. The result is the added security of the process along with overall improved system performance.

2. Literature Survey

In [3] Mukhopadhyay talks about the different types of Symmetric Key Ciphers including Modern Block Cipher, Full Size and Partial-Key Size Cipher, Feistal and Non-Feistal Ciphers. According to his inference, operations such as split, combine, swap etc. can be applied to an n-bit Modern Block Cipher along with properties such as Diffusion and Confusion. Also, the Feistal Cipher, which is not particularly a cipher but a block cipher design, can split Plaintext as well as Cipher text with the help of a round function and a sub key. In [4] Ayushi explains the cryptographic system, cryptographic techniques namely public key and private key cryptography and along with this proposes a new symmetric key algorithm. In the proposed algorithm, the 8-bit binary representation of the ASCII value of a letter is taken into consideration and then worked upon with the help of a 4-bit randomly generated key. The Cipher text that is yielded is a combination of 3-bit remainder and 5-bit quotient. This algorithm focused on simplicity and security with CRC checking at the receiving end. There was focus on Cryptographic goals, Modes of Encryption/Decryption and the Performance Analysis of Symmetric Key Cryptographic Algorithms i.e. Data Encryption Standard, Advanced Encryption Standard and Blowfish by Thakur and Kumar in [5]. This paper focused on running different encryption settings with cipher modes such as Electronic Code Book and Cipher Block Chaining to process different sizes of data to check for each algorithm’s speed against each other. In [6] Deshmukh and Patil have proposed a Hybrid Cryptography technique using modified Diffie-Hellman and RSA encryption algorithm. The new proposed hybrid algorithm is divided into two parts : (i) The first part is based on the modified Diffie-Hellman Key Exchange (ii) The second part involves the use of RSA encryption algorithm to encode and decode the message but on both sides two keys are generated with this RSA encryption approach. These keys are labeled as Sender key and Receiver key for the encryption and decryption process respectively. This Hybrid algorithm is secure because the encoding and decoding process is done with a secretly generated sender key and receiver key due to which a two-step security procedure is mechanized.

3. Method

In this algorithm, the Encryption process [4] is done by first generating an ASCII value of the letters of the message. Then, the corresponding 8-bit binary value of the generated ASCII value is taken. This binary value is reversed and then divided by a randomly generated 4-bit binary key to obtain a Remainder and Quotient. This, Remainder as well as the Quotient is modified to make the remainder store the first 3 bits and the quotient store the next 5 bits, so as to create a 8-bit cipher text.

3.1 Data Encryption

1. Generate ASCII value of a letter. (Ex. t=84)
2. Generate corresponding binary value (8-bit).if the corresponding value is not 8-bit add 0's to the LHS
t(binary)=1010100
i.e. t=01010100(adding 0 to the L.H.S)
3. Reverse the binary value.
t'=00101010
4. generate a random key (4-bit) starting from 1000
k=1000
5. Divide t' with k.

$$t' / k \tag{1}$$

00101010/1000
Remainder (r) =10;
Quotient (q) =101;

6. Store the remainder as the first 3 bits and the quotient as the next 5 bits to obtain an 8-bit cipher text. If quotient and remainder are less than 3 bit and 5 bit respectively, we add 0 to the LHS.
r'=010
q'=00101
C=01000101
here, the cipher text corresponds to the alphabet 'C'.

3.2 Symmetric Key Encryption

In hybrid cryptography, this symmetric key k' will be input as plaintext in the RSA algorithm and encrypted . The following is presented below.

1. Take 2 large prime numbers A and B of equal length. obtain their product(N).

$$N = A \times B \tag{2}$$

$$P = (A-1) \times (B-1) \tag{3}$$

3. Choose the receivers public key (E) which is randomly chosen number with no common factors with P.
4. We obtain the private key of the receiver from the receiver's public key.

$$D = E^{-1} (\bmod P) \tag{4}$$

We take the 4 bit long key (k') as the plaintext . The encrypted cipher text is

$$S = k'^{E} (\bmod N) \tag{5}$$

3.3 Decryption of Symmetric Key Using RSA

1. Our first goal is to obtain the decrypted symmetric key i.e. k' . We obtain k' by decrypting it through RSA.

$$k' = S^{D} (\bmod N) \tag{6}$$

3.4 Data Decryption

Since we have obtained the symmetric key k' we can easily decrypt the data. The procedure is as follows:-
1.Multiply last 5 bits(q') of the cipher text C with the key.
C=01000101

$$C' = q' \times k' \tag{7}$$

C'=00101*1000
C'=101000
2. OR 1st 3 bits of the cipher text (r')with C'.
C' OR r'
3.If the result produced is not an 8 bit number add O's to the LHS.
4.Reverse the number to get the original text.

4. Result

This section will show the results which are obtained by running the simulation program using different data loads. The results show the impact of changing data load on each algorithm. The experiment was conducted using CFB mode, the results are shown in figure below.

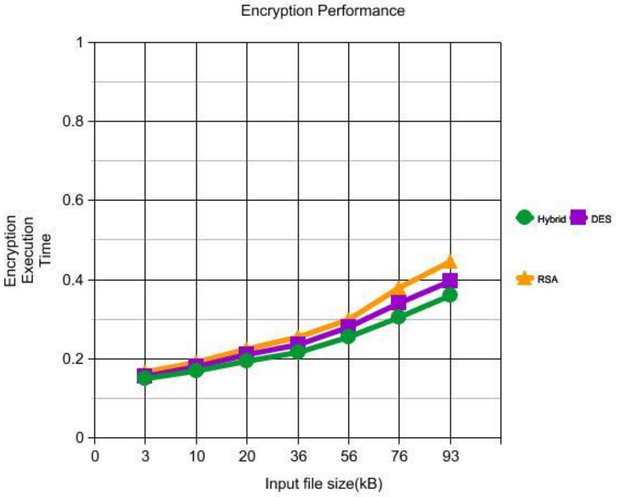

Figure 5.2: Encryption Execution Time

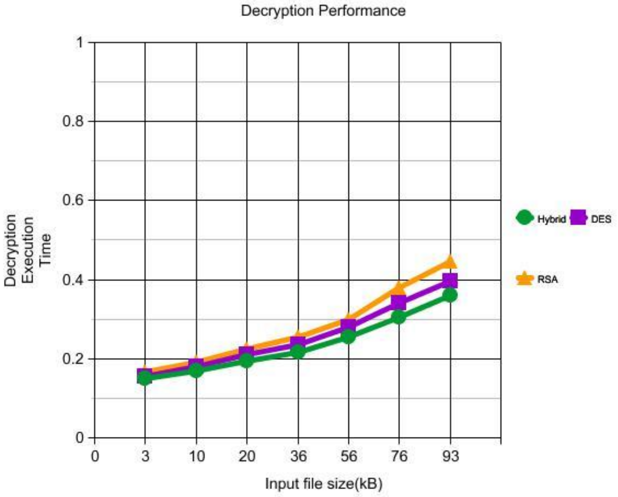

Figure 5.3: Decryption Execution Time

Table 5.2 Encryption Execution Time

Input File Size(kB)	Encryption Execution Time(seconds)		
	Hybrid	DES	RSA
3	0.15	0.155	0.16
10	0.16	0.18	0.19
20	0.18	0.21	0.22
36	0.20	0.235	0.245
56	0.24	0.28	0.29
76	0.28	0.34	0.37
93	0.33	0.395	0.42

Table 5.3 Decryption Execution Time

Input File Size(kB)	Decryption Execution Time(seconds)		
	Hybrid	DES	RSA
3	0.15	0.155	0.17
10	0.18	0.18	0.19
20	0.21	0.21	0.23
36	0.23	0.235	0.255
56	0.27	0.28	0.31
76	0.33	0.34	0.39
93	0.39	0.395	0.47

5. Conclusion

The proposed Hybrid Encryption Algorithm shows lesser message delivery time as compared to other encryption algorithms such as Symmetric Encryption Algorithm, Asymmetric Encryption Algorithm. Also, our Hybrid Encryption Algorithm has a higher complexity factor as compared to the above mentioned public key, private key and hybrid algorithms. Therefore, the proposed Hybrid Cloud Cryptosystem has greater performance value than the already existing encryption algorithms.

References

[1] Margaret Rouse. http://searchsoftwarequality.techtarget.com/definition/cryptography.
[2] Hybrid Cryptosystems. http://en.wikipedia.org/wiki/Hybrid_cryptosystem.
[3] Assistant Prof. Debdeep Mukhopadhyay. Symmetric Key Ciphers.
[4] Lecturer Ayushi. A Symmetric Key Cryptographic Algorithm.
[5] Jawahar Thakur & Nagesh Kumar. DES, AES & Blowfish: Symmetric Key Cryptographic Algorithm Simulation based Performance Analysis.
[6] Shyam Deshmukh & Prof. Rahul Patil. Hybrid Cryptographic technique using D-H & RSA.
[7] http://www.techopedia.com/definition/1779/hybrid-encryption

Author Profile

Mohit Prakash received the degree of Bachelor Of Technology (Computer Science) from Bhagwan Parshuram Institute Of Technology in 2015, respectively.