Implementation of Hybrid Cryptosystem Using BLOWFISH and RSA Algorithms

Harshala B. Pethe[1], Varsha C. Pande[1] and S. R. Pande[2]
[1]Department of Electronics and Computer Science RTMNU, Nagpur (India).
[2]Department of Computer Science, SSESA's Science College, Congress Nagar, Nagpur (India)
harshapethe@gmail.com; varshapande.var@gmail.com srpande65@rediffmail.com

ABSTRACT

An important data can be transferred through email, banking transaction and online purchase. Network security is an essential part to do such secured transactions and cryptography is the science that widely used for network security

This paper gives the implementation and analysis of hybrid cryptosystem using BLOWFISH and Rivest-Shamir-Adleman (RSA) algorithm. Blowfish is a symmetric block cipher and can be effectively used for encryption and safeguarding of data. It is suitable for applications where the key does not change often, like a communication link or an automatic file encryptor. RSA is an asymmetric key algorithm. In this algorithm two separate keys are used for encryption and decryption. The efficiency of the algorithm is measured by execution time. The program simulation result provides the better performance as well as security.

Keywords: Symmetric key cryptography, asymmetric key cryptography, encryption, decryption, BLOWFISH, RSA, Cryptographic algorithms.

1. INTRODUCTION

Cryptography is the science of keeping messages secret and widely used for network security. Cryptography means to transfer sensitive information across insecure networks such as internet. The goals of cryptography are confidentiality, integrity, authentication, and non repudiation [1] [2]. An original message is known as the plaintext, while the coded message is called the ciphertext. The process of converting from plaintext to ciphertext is called encryption; restoring the plaintext from the ciphertext is decryption.

Cryptography algorithms are either symmetric algorithms, which use symmetric keys (also called secret keys), or asymmetric algorithms, which use asymmetric keys (also called public and private keys) .

Symmetric Algorithms

Symmetric algorithms, sometimes called conventional algorithms, are algorithms where the encryption key can

be calculated from the decryption key and vice versa. These algorithms, also called secret-key algorithms, single key algorithms, or one-key algorithms, require that the sender and receiver agree on a key before they can communicate securely. The security of a symmetric algorithm rests in the key

Encryption and decryption with a symmetric algorithm are denoted by:

$E_K(M) = C$

$D_K(C) = M$

Symmetric algorithms can be divided into two categories. Some operate on the plaintext a single bit (or sometimes byte) at a time; these are called stream algorithms or stream ciphers. Others operate on the plaintext in groups of bits. The groups of bits are called blocks, and the algorithms are called block algorithms or block ciphers.

Public-Key Algorithms

Public-key algorithms are also called asymmetric algorithms and are designed so that the key used for encryption is different from the key used for decryption. The decryption key cannot be calculated from the encryption key. The algorithms are called "public-key" because the encryption key can be made public. Any person can use the encryption key to encrypt a message, but only a specific person with the corresponding decryption key can decrypt the message. In these systems, the encryption key is often called the public key, and the decryption key is often called the private key.

Encryption using public key K is denoted by:

$E_K(M) = C$

Even though the public key and private key are different, decryption with the corresponding private key is denoted by:

$D_K(C) = M$

In this paper we have done the comparative analysis of AES which is symmetric key algorithm and RSA, which is asymmetric key algorithm.

Blowfish is a symmetric block cipher designed by Brute Schneier in December 1993. Blowfish is a replacement of DES or IDEA. Blowfish algorithm is a symmetric block cipher with a 64-bit block size and variable key length from 32 bits to 448 bits [3].

RSA is asymmetric key algorithm developed in 1978. The simulation speed is fast different keys are used for encryption and decryption process. The power consumption of RSA algorithm is high[4].

2. GOALS OF CRYPTOGRAPHY

2.1 Confidentiality

Confidentiality means protection against unauthorized disclosure of information. It may be applied to whole messages, parts of messages, and even existence of messages. Confidentiality provides the protection of transmitted data from passive attacks.

2.2 Authentication

The process of proving one's identity. This includes verifying the message's source. Authentication is of two types: (i) Peer entity authentication, and (ii) Data origin authentication.

2.3 Data integrity

The integrity is an assurance that the message has not been modified. This can be applied to a stream of messages, a single message, or selected fields within a message. It assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays.

2.4 Access control

It is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

2.5 Non repudiation

Sender or receiver cannot deny for a transmitted message. When a message is sent, the receiver can prove that the sender in fact sent the message [5][6].

3. OVERVIEW OF BLOWFISH

The expansion of the key: break the original key into a set of subkeys. Specifically, a key of no more than 448 bits is separated into 4168 bytes. There is a P-array and four 32-bit S-boxes. The P-array contains 18 32-bit subkeys, while each S-box contains 256 entries.

The encryption of the data: 64-bit input is denoted with an x, while the P-array is denoted with a Pi (where i is the iteration).

- The input is a 64-bit data element, x.
- Divide x into two 32-bit halves: XL, XR.
- Then, for i = 1 to 16.
- XL = XL XOR Pi
- XR = F(XL) XOR XR
- Swap XL and XR
- After the sixteenth round, swap XL and XR again to undo the last swap.
- Then, XR = XR XOR P17 and XL = XL XOR P18.
- Finally, recombine XL and XR to get the cipher text [7].

Blowfish is unpatented and license-free, and is available free for all uses. Blowfish Algorithm is a Feistel network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors [8].

4. OVERVIEW OF RSA

RSA is widely used in encrypted connection, digital certificates core algorithms. Public key algorithm invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA).It is the main operation of RSA to compute modular exponentiation [9]. Especially, when RSA decrypts the cipher text and generates the signatures, more computation capacity and time will be required. Reducing modules in modular exponentiation is a technique to speed up the RSA decryption. The security of RSA comes from integer to find. Generation of random prime numbers gives the algorithm extra strength and efficiency.

Following steps are followed in RSA to generate the public and private keys [10]:

Step 1: Choose large prime numbers p and q such that

p not equal to q.

Step 2: Compute n=p*q

Step 3: Compute φ (pq) = (p-1)*(q-1)

Step 4: Choose the public key e such that

gcd (φ (n), e) =1; 1<e< φ (n)

Step 5: Select the private key d such that

d*e mod φ (n) =1

In RSA algorithm encryption and decryption are performed as-

Encryption:

Calculate cipher text C from plaintext message M such that

C=M ^e mod n

Decryption:

M=C^d mod n=M^ed mod n

HYBRID ALGORITHM

The hybrid algorithm using BLOWFISH-RSA is as follows:

Step 1: Input image

Step2: Encrypt original image using Blowfish algorithm.

Step 3: Encrypt encrypted image using RSA algorithm.

Step 4: Decrypt encrypted image using RSA algorithm

Step 5: Decrypt using Blowfish algorithm

Step 6: Stop.

5. EXPERIMENTAL RESULTS

The BLOWFISH and RSA algorithm is implemented using MATLAB 2013a. The time required for encryption and decryption is shown in the following table. The image files are taken from SVT dataset.

Table1: Encryption and decryption time using hybrid algorithm

Image File	Encryption Time for BLOWFISH	Encryption Time for RSA	Encryption Time for Hybrid algorithm
simg_1	6.7298	2.604	5.6928
simg_2	3.522	1.4834	2.79687
simg_3	4.4263	1.3884	3.5156
simg_4	4.3395	1.7571	3.5681
simg_5	2.4764	1.1496	3.4883
simg_6	4.7778	2.0446	3.9234
simg_7	4.4189	1.1389	6.8565
simg_8	4.7858	1.3789	6.2526
simg_9	3.9494	1.6731	3.5707
simg_10	4.7381	1.8306	3.4811

RSA algorithm is implemented using MATLAB2013a. The time required for encryption and decryption is shown in the following table with p=19 and q=23. The image files are taken from SVT dataset.

Table 2: Encryption and decryption time using RSA algorithm

Image File	Decryption Time for BLOWFISH	Decryption Time for RSA	Decryption Time for Hybrid algorithm
simg_1	4.1683	41.9616	3.9883
simg_2	3.984	19.1139	1.757
simg_3	4.4798	25.2828	2.3772
simg_4	4.5421	25.0157	2.3959
simg_5	2.56084	22.5839	2.32
simg_6	4.5084	27.6251	2.50723
simg_7	4.6812	26.5331	2.5698
simg_8	5.2663	31.3381	3.0367
simg_9	4.3673	24.3389	2.4913
simg_10	4.6239	25.5949	2.4673

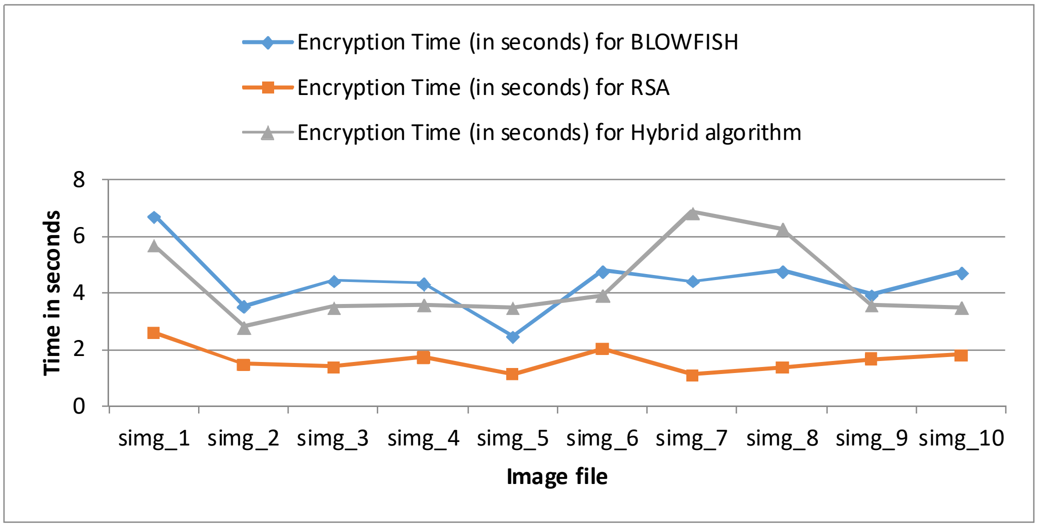

Figure 2: Encryption time for BLOWFISH, RSA and Hybrid algorithm

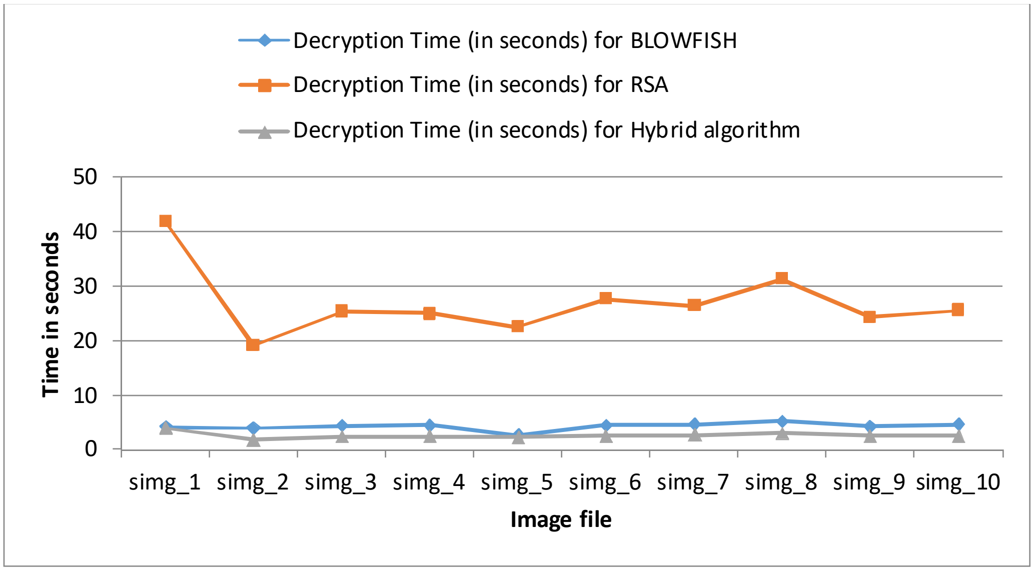

Figure 3: Decryption time for BLOWFISH, RSA and Hybrid algorithm

6. CONCLUSION

In this paper we have implemented the BLOWFISH and RSA algorithms and a hybrid algorithm (BLOWFISH-RSA) using MATLAB R2013a for different image files of increasing sizes, keeping key constant and it is observed that the time required for encryption for hybrid algorithm is less than BLOWFISH and greater than RSA but the time required for decryption for hybrid algorithm is less than both the algorithms. Therefore the hybrid algorithm is efficient in terms of time.

REFERENCES

[1] Behrouz A. Forouzan, “Cryptography and Network Security”, Tata McGraw-Hill, 2nd edition, 2008.

[2] Anand Kumar M and Dr. S. Karthikeyan, "Investigating the Efficiency of Blowfish and Rejindael Algorithms", International Journal of Computer Network and Information Security, pp. 22-28, 2012.

[3] Ashwak Alabaichi, Faudziah ahmed and Ramlan Mahmod, "Security Analysis of Blowfish algorithm", IEEE, pp. 12-18, 2013.

[4] Annapoorna Shetty, Shravya Shetty K, Krithika K "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm" International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 5, October 2014, ISSN (Print): 2320-9798.

[5] Ritu Tripathi, Sanjay Agrawal Comparative Study of Symmetric and Asymmetric Cryptography Techniques International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853.

[6] Vikrant M. Adki, Prof. Shubhanand S. Hatkar A Survey on Cryptography Techniques International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 6, June 2016 ISSN: 2277 128X.

[7] Neha, Mandeep Kaur, "Enhanced Security using Hybrid Encryption Algorithm" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297:2007 Certified Organization) Vol. 4, Issue 7, July 2016 ISSN(Online): 2320-9801 ISSN (Print) : 2320-9798.

[8] Saikumar Manku1 and K. Vasanth, "BLOWFISH ENCRYPTION ALGORITHM FOR INFORMATION SECURITY" ARPN Journal of Engineering and Applied Sciences VOL. 10, NO. 10, JUNE 2015, ISSN 1819-6608.

[9] AnnapoornaShetty, Shravya Shetty K, Krithika K A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 5, October 2014 ISSN(Online): 2320-9801 ISSN (Print): 2320-9798.

[10] Aman Kumar, Dr. Sudesh Jakhar, Mr. Sunil Makkar Comparative Analysis between DES and RSA Algorithm’s International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X.