RESEARCH ARTICLE OPEN ACCESS

Implementation of split based encryption technique for securing file transfer over a network

Mrs. Parul Rathor
Department of Computer Science & Engineering
Email.id: cparul2605gmail.com

Abstract
The main aim of this paper is to introduce the basic concept of cryptography. It will be demystify all such related terms in relation to cryptography in this paper. Here the essential concepts of cryptography are introduced first; we then proceed to revise three such algorithms/schemes that are RSA, Advanced Encryption Standard (AES) and RC6. A combination of algorithms is used to provide "Strong data protection". Combining splitting with standard encryption methods provides a very strong of data protection called " Master-frame" .A master – frame is a frame which we include all four mini frames each of 25KB data of algorithms RSA, AES & RC6.Then in each frame we store these three algorithms encrypted it and provide key. After that we provide security to these master frame by using proper key, its frame number and encryption type. A master frame is nothing but security of frame.

I. Introduction

At some stage in this time when the Internet provides fundamental communication between tens of millions of people and is being progressively more used as a tool for commerce, security becomes an enormously important issue to covenant with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential feature for secure communications is through cryptography. This dissertation has two major purposes the first is to define some of the terms and concepts behind basic cryptographic methods, and to offer a way to compare the numerous cryptographic schemes in use today. The second is to provide frame which is nothing but security of trace.

"Cryptography is the sculpture of achieve security by preparing encrypt message to make them non-readable."

The main aim of this topic is to provide a broad evaluation of cryptography. The Cryptography is a theme extensive ranging to coverage about how to protect information in digital form and to endow with security services.

II. Types of Cryptographic Algorithms

There are several customs of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. There are, in general, two types of cryptographic schemes typically used to accomplish these goals:-

1. Secret Key Cryptography (SKC): Only One single key is used for both encryption and decryption. It is also called as Symmetric Key. Here size of resulting encrypted text is usually same as or less than the original text. Also Key exchange is a very big problem
2. Public Key Cryptography (PKC): Two different keys are used. One for encryption another for decryption as well as for digital signatures. Another name of PKC is Asymmetric Key. The size of resulting encrypted text is more than the original plain text size. In contrast of SKC, key exchange having no problem at all.

In advance, we define some terms:-

1. Plain text → It is the simple text which are known to be anyone who get access to that message.
2. Cipher text → "When a plain text message is codified using such suitable scheme, resulting message is called as cipher text."
3. Encryption → It is the procedure of converting plain text into cipher text.
4. Decryption → It is the reverse procedure of encryption which converts the plain text from the cipher text.
5. Such schemes are known as a Cryptographic system or a Cipher.

;

III. Review of three schemes

A grouping of algorithms is used to provide well-built data protection. Let us revise the three such schemes that are RSA, Advanced Encryption Standard (AES) and RC6 one by one:-

1.1 RSA Scheme

One of the first, and perhaps best known public key scheme; It was developed in 1977 by R.Rivest, A.Shamir and L. Adleman; The RSA algorithm is the most fashionable & verified asymmetric key cryptographic algorithm. Let us have a quick summary of prime numbers as they form the basis of RSA algorithm.

1. Select any two large prime nos. A and B
2. Compute N = A * B
3. Choose encryption key E such that it is not a factor of (A-1)
   and (B - 1).
4. Pick decryption key D such that the following equation is true:
   (D * E) mod (A - 1) * (B - 1) = 1
5. For encryption, calculate cipher text CT from plain text PT as follows:
   CT = PT^E mod N
6. Send CT as the cipher text to the receiver.
7. For decryption, analyze plain text PT from cipher text CT as follows:
   PT = CT ^D mod N

The RSA algorithm is based on arithmetical fact that it is very simple to obtain and multiply large prime numbers together, but it is extremely difficult to factor their product. The two private and public key in RSA are based on large prime numbers. Conversely, the real challenge of RSA is the collection and creation of the private and public keys. This algorithm is fairly simple.

1.2 AES Scheme

In 1990's, the US government hunted to normalize a cryptographic algorithm, which was to be used universally by them. It was to be called as the Advanced Encryption Standard (AES).The necessity for inventing such new algorithm because of the supposed weakness in Data Encryption standard (DES). The 56-bit keys of DES were no longer considered safe beside attacks based on complete key searches and the 64-bit blocks were also considered as weak. AES was to be based on 128-bit blocks with 128-bit keys. In Oct 2000, Rijindael was declared final selection for AES and according to its designers the major features of AES are given as –

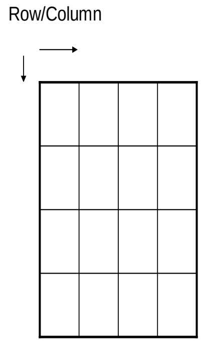
a. Symmetric & parallel structures-> this give the implementers of the algorithm a lot of elasticity. It also stands up well against cryptanalysis attacks.
b) Adapted to modern processors-> the algorithm works well with modern processors
c) Suited to smart cards-> the algorithm can work well with smart cards

Operations are:-
He was designed to have the following distinctiveness:

I. Resistance beside all known attacks.
II. Speed and code density on a wide range of platforms.
III. Design unfussiness

The algorithm starts with an Add round key stage followed four stages by 9 rounds and a three stages by tenth round. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm. The four stages are as follows:
1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

OPERATIONS -- >>



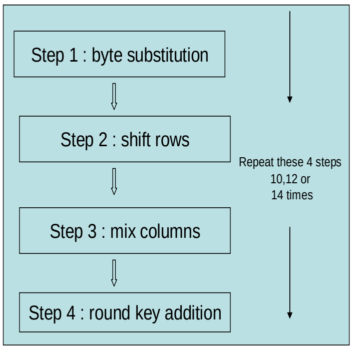

Step 1 : byte substitution
Step 2 : shift rows
Step 3 : mix columns
Step 4 : round key addition
Repeat these 4 steps 10,12 or 14 times

Fig 1.Initial plain text/key block

Fig 2. Steps in Rijindael

In this step 1, the S-box technique is used similar to the way it is done in DES. The input plain text passes by S-box & the resultant text is generated for the input to the next operation.

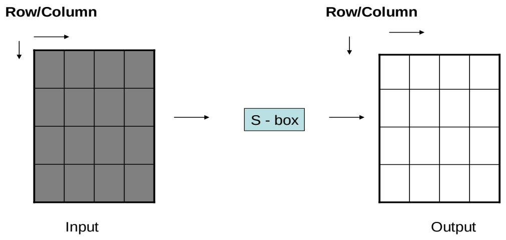


Fig 3. Step 1 Byte Substitution

In this step 2, the first row is safe. The other three rows are shifted like in second row letter H be shifted to right then in third row letter K be shifted and at last letter N be shifted. As a letter was shifted correspondingly all other letters beside it was also shifted. The logical view of this operation is shown below.

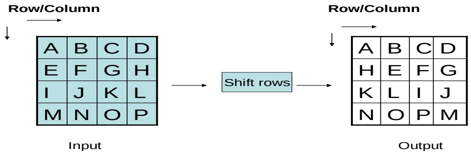


Fig.4 Step 2 Shift rows

In step 3, the four bytes of every column are mixed in a linear trend. It is not so easy that’s why he was not mentioned here.

In step 4, each key byte is XOR.He was XOR both input & output so that next output will be cipher text of this round as given in figure.

1.3 RC6 Schemes

RC6 is an advance of RC5; it was designed to meet the necessities of the Advanced Encryption Standard (AES). Our analysis demonstrates that RC6 is highly resistant to deferential and linear cryptanalytic attacks, which are currently the two most selective analytical attacks on block ciphers.

RC6 meets the necessities for the AES like it was easy, quick and safe.

IV. Methodology

As in above we revise all three schemes RSA, AES and RC6.Now if we want to provide security to this schemes and also if we want to merge it? Then here we introduced one frame, in this frame we encapsulate this three schemes. These frames is of 100kb which is split into four frames and each of 25kb then we encrypted it by using suitable schemes, providing key, after that again we send back to master frame which is of same as 100 kb. In this frame we provide security of each frame like frame nos. & encrypted type key.

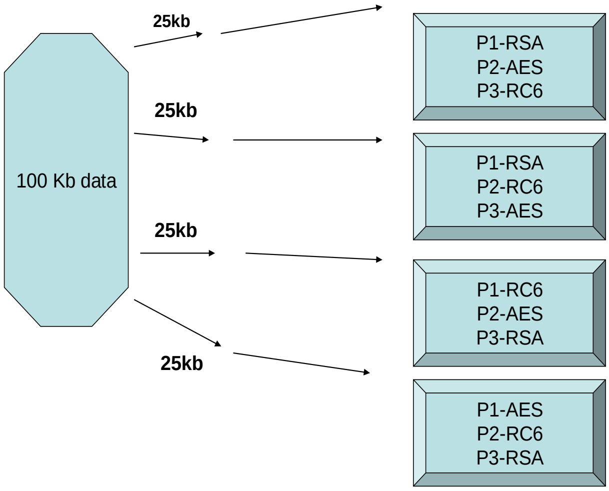


Fig.5 Storage of Frames

We will divide that master frame into four frames, first we will encrypt it and send back to the master frame. We will do these because it will increase randomization which will be difficult for decryption .Also here same key will be used for each algorithm but key type will be different.

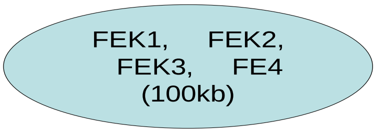


Fig 6 Master Frame

The software configuration is JAVA language, because object oriented language. It is platform independent, robust language and also support for networking. This frame is made on eclipse.

A storage appliance can be used to provide high availability.

A master frame is nothing but security of frame.

Hence we conclude this by combining splitting with standard encryption methods provides a very strong of data protection thats called "Master-frame".

V. Conclusion

This paper has described temporarily about how cryptography works. In spite of the mathematical theory behind an algorithm, the best algorithms are those that are familiar and well-documented. A permutation of algorithms is used to provide " A Strong data protection. "

The RSA algorithm is the most fashionable & verified asymmetric key cryptographic algorithm. The second one was to be called as the Advanced Encryption Standard (AES).And the third one is RC6,which is highly opposed to reverent and linear cryptanalytic attacks, which are currently the two most selective diagnostic attacks on block ciphers. Finally, all these three schemes are stored in one frame called " Master Frame " which will be secured by using frame numbers, encrypted type & key.

In this way it will make our master frame secure.

A storage machine can be used to provide high availability.

A storage appliance can be used to provide high availability.

A master frame is nothing but security of frame.

Hence we conclude this by combining splitting with standard encryption methods provides a very strong of data protection that called "Master-frame".

References

[1]. [1] E. Biham and A. Shamir. *Diferential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, New York, 1993.

[2]. [2] A. Biryukov and E. Kushilevitz. *Improved cryptanalysis of RC5*. In K. Ny-berg, editor, Advances in Cryptology | Eurocrypt '98, volume 1403 Lecture notes in Computer Science, pages 85{99, 1998. Springer Verlag.

[3]. [3] J. Daemen, R. Govaerts and J. Vandewalle. Weak keys for IDEA. In D. Stinson, editor, Advances in Cryptology | Crypto '93, volume 773 of Lecture Notes in Computer Science, pages 224{231, New York, 1994, Springer Verlag.

[4]. [4] M.H. Heys. *Linearly weak keys of RC5. IEE Electronic Letters*, Vol. 33, pages 836{838, 1997.

[5]. [5] T. Jakobsen and L.R. Knudsen. *The interpolation attacks on block ciphers.*

[6]. In E. Biham, editor, *Fast Software Encryption*, volume 1267 of Lecture notes in Computer Science, pages 28{40, 1997. Springer Verlag

[7]. [6] Trappe, W., & Washington, L.C. (2006*). Introduction to*

[8]. *Cryptography with Codin Theory*, 2nd ed. Upper Saddle River, NJ:

[9]. Pearson Prentice Hall.

[10]. [7] Denning, D.E. (1982). *Cryptography and Data Security*. Reading,

[11]. MA: Addison-Wesley.

[12]. [8] Ferguson, N., & Schneier, B. (2003). *Practical Cryptography*. NewYork: John Wiley & Sons.

[13]. [9] Electronic Frontier Foundation. (1998). Cracking DES: *Secrets of*

[14]. *Encryption Research*, Wiretap Politics & Chip Design. Sebastopol,

[15]. CA: O'Reilly & Associates.

[16]. [10] Schneier, B. (2000). Secrets & Lies: *Digital Security in a Networked World*. New York: John Wiley & Sons.

[17]. [11]*Network Security Essential*, William Staling, Pearson Publications Ltd.

[18]. [12] G. Abuaitah and B. Wang. Secvizer: A security visualization tool for qualnet-generated traffic traces. *In Proceedings of the 6th International Workshop on Visualization for Cyber Security (VizSec), VizSec '08,* pages 111–118, 2009.

[19]. [13] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless Sensor Networks: A Survey. Computer Networks, 38(4):393–422, Mar.2002.

[20]. [14]P. Bak, F. Mansmann, H. Janetzko, and D. Keim. Spatiotemporal analysis of sensor logs using growth ring maps. Visualization and Computer Graphics, IEEE Transactions on, 15(6):913–920, nov.-dec.2009.

[21]. [15]S. Card, J. Mackinlay, and B. Shneiderman. Readings in Information Visualization: Using Vision to Think. Morgan Kaufmann Publishers, San Francisco, 1999.

[22]. [16] X. Chen, K. Makki, K. Yen, and N. Pissinou. Sensor network security:a survey. IEEE Commun. Surveys Tuts., 11(2):52–73, 2009.

[23]. reference model. In Proceedings of the IEEE Symposium on Information Vizualization 2000, INFOVIS '00, pages 69–75, Washington, DC, USA,2000. IEEE Computer Society.