ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

COMPARISON OF RSA AND MD5 ALGORIHM

Navaneethan C*, Meenatchi S , Kumar P J, Suganya P
VIT, University, Vellore.
Email: pjkumar@vit.ac.in

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

Abstract

Nowadays hackers hack the message while it is being send. To overcome this problem there are many algorithm. In our paper we are going to take a deep survey and compare two algorithms: RSA and MD5 in terms of speed, key size, block size, rounds, execution time, security to find which algorithm works better.

Introduction

1. Hiding the message with a Symmetric key cryptography is defined as private key cryptography where encryption and decryption can be made with the use of one secrete key. The transformation of plain text to cipher text and cipher text to the plain text is made with the use of the same secrete key.

2. Asymmetric Key Cryptography is called as public key cryptography. Here, by using the secret key the data is converted into cipher text then at receiver end same data is decrypted using another key. RSA algorithm uses asymmetric key.

3. Hash Function is a one way cryptography because we don't use keys here. "This is also known as message digest". It is widely used in password encryption.

4. In RSA algorithm consist of two keys. One is used for doing encryption and another is used for doing decryption .Two large prime numbers are taken and it is multiplied. E is kept as private key and d is kept as public key.

5. MD5 algorithm uses checksum for 128 bit value of a file. Some time there is a chance of same has value can be generated from two different files

MD5 requires minimum of 8 bits as a message. MD5 is fast and it takes large amount of data to be processed.MD5 function gives a 32 digit hexadecimal number.

Literature Survey: Inpaper [1].It mainly focuses on attacks on RSA. RSA algorithm doesn't work arbitrary value but if e value is small than RSA algorithm works. In RSA algorithm arbitrary value doesn't work. So to overcome this problem factoring modulus is used.

In paper[2].Discussesabout collision rates of MD5. Maximum collision rate occurs in MD5 because it has only 128 bits.

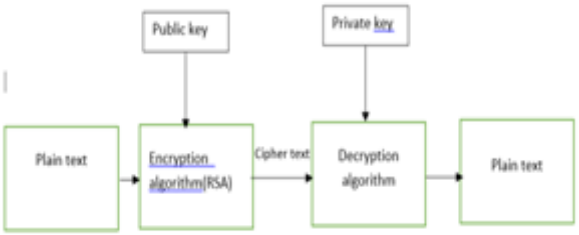
In paper[4]. Itis based on the survey of MD5 algorithm. By the usage of source codes and they have analysed about the comparative measures of MD5.

In this paper[5].They discussed about the recovery of the password in encrypted form of pdf file. This recovery operation decreases the instruction quantity which is processed in the hashing operation.

Working of RSA

First, randomly two prime numbers are selected, P and Q, then we should find N value i.e N=P*Q and we have to find M=(P-1)(Q-1). The next step is encryption process, encryption key is "e" where "e" value should be lesser than M and it should be greater than one. Then find gcd(e,M)=1. Decrpytion process is the next phase the decryption key is "d". Where e.d=1 mod M. Public key encryption is KU={e,N} then the secret private decryption key KR={d,P,Q}. RSA has public key and private key

1. randomly select two prime number say p & q
2. find N =p*q note m=(p-1)(q-1)
3. encryption key e where (1<e<m) gcd(e,m)=1
4. decryption key d where e.d=1mod m 0<d<N
5. public encryption key KU=(e,N)
6. private decryption key KR=(d,p,q)



Advantage of RSA

- RSA uses public key encryption that makes the data to be more secured.

- RSA uses private key decryption which plays a vital role in security where only the receiver knows the key to decrypt the message so it can't be hacked my hackers, the message is kept secured.
- If large prime number is taken it is hard for the hacker to crack the message

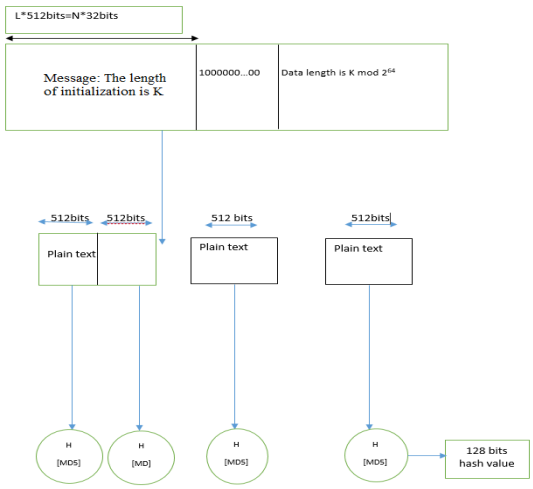
Disadvantage of RSA

- RSA encryption and decryption needs lots of calculation so it becomes slower.
- RSA is thousand time slower when it is compared to symmetric cryptographic algorithm.
- To increase the security we use the key size as 4096 the data is also kept secured but the calculation becomes more slower.

Working of MD5

This algorithm uses hash function to produce the hash value of 128 bit. This transformation of hashvalue into message digest form is also known as "finger print" or "hash value "of plain text.md5 algorithm is a one way hash function it is hard to invert (i.e) we cannot able to get the original text back once it has been converted but in RSA algorithm it is possible .in other word we can say md5 is irreversible .

- Append the padding bits.
- Length of the bits are joined.
- Get input from user.
- The given bits are separated into 512 bit blocks.
- Initialization of MD5 buffer.
- 16 basic operation is performed by taking 4 MD5 buffer.
- The result should be in the form of hash value. To generate 128 bit hash value four operations are performed.



Advantages of MD5

- Calculation is very fast than RSA.
- Provides from data collision.
- The main advantage is it uses one way hash technique.

Disadvantage of MD5

- Less secure than SHA-1 algorithm

4. Comparison of RSA and MD5

A. Compare OF Key Size

Compared to MD5, RSA has large number of bits.RSA bits ranges between 1024 to 2048 and it generates 309 digits code that is regarded as strong for all applications md5 has 128 bit and it generates digits .

B. Attacks On RSA Exceeded BY MD5

We have to two main attacks in RSA algorithm are,

- Mathematical Attacks
- Implementation Attacks

Mathematical Attack

Structure of RSA function is attacked .Decryption can be done easily if one knows the factor i.e mod N which helps to find the D value easily.

a. **ELEMENTARY ATTACK:** The purpose of this attack is to misuse the RSA algorithm and it done openly.
b. **SMALL PRIVATE KEY ATTACK:** If the private key value is taken small then the performance will be increased but if the small the problem is hacker can easily decrypt the small value. By using the Large private key value hackers cannot decrypt the data but the calculation becomes slow.
c. **SMALL PUBLIC KEY ATTACK:** If the public key value is small then it can be easily attacked by hacker. The reason to use small public key is to increase the performance of encryption in RSA.

Implementation Attack

This is called as time attack. This attack happens when hidden cryptosystem is implemented. MD5 over comes all these attacks because there is no use of public or private keys in MD5.

Attacks involved in MD5

Dictionary attack: Is an attack in which the hacker tries all the possible passwords in a complete list called as dictionary. From the dictionary the hackers combines all the passwords and they perform binary search on the combined password. This can be done even faster by pre calculating the hash values of these possible passwords and storing them in a hash table.

Rainbow table: Rainbow tables are constructed with hash chains and they are more effective and efficient than the hash tables they optimize the storage requirements, rainbow table completely varies from hash table. Reduction is the process of converting hash value into plain text. Here the plain text is not the text which is generated by the hash value but it is another text. Hash values are formed by alternating reduction function and has function. The chain's start point and end point (i.e) first and last plain text is generated and it is stored in the table in the case of decipher the hashed password we should take that chains start point and regenerate the entire hash chain and the original plain text to the hashed password must be found. This rainbow table plays a vital role in the password cracking system. Now a days many cracking system and websites uses rainbow table.

C. Comparison of Execution Time

In RSA two large prime numbers are taken then it will be converted into 1024 bits. To encrypt and decrypt it takes more time but in MD5 there is no use of keys so it is faster than RSA

D. Comparison of Utilization OF CPU

MD5 utilizes CPU better than RSA because of fast calculation algorithm while RSA utilizes CPU anuses more computer resources and hence its speed goes down.

E. Comparison of Security

MD5 is more secure than RSA because RSA gives more secure to small files but in the case of large it is not compared well.MD5 gives more secure to small and large files. MD5 is much better in securing the files.

F. Complete Comparison

FACTORS	RSA	MD5
Key size	1024,2048,4096 bits	56,128,256,512 bits
Rounds	4	1
Block size	1024 bits	128 bits
Security	Works good but slow when the data is large	Works really good than RSA
Execution time	More time	Less time

Acknowledgement

We are highly thankful to our parents and we are really happy and glad to thank Prof. Navaneethan C for his support and his excellent guidance to complete this paper .

Conclusion

In this paper we have compared RSA and MD5 algorithms. We compared the working standard of twoalgorithm. We conclude that md5 is more secure than RSA because md5 is a one way cryptography and it has randomness characteristics so that it has been widely used in data integrity. Our future work, is to find how MD5 is more secure while comparing to other algorithms.

References

1. Sattar J Aboud, "An Efficient method for Attack RSA Scheme," Iraqi Council of Representatives, pp. 587-591, 2009.
2. Ming Hu, Yan Wang, "The Collision Rate Test of Two Known Message Digest Algorithms," International Conference on Computational Intelligence and Security, pp. 319-323, 2009.
3. Hancheng LIAO, "Image Retrieval based on MD5,"International Conference on Advanced Computer Theory And Engineering, pp. 987-991, 2008.
4. Zhao Yong-Xia, Zhen Ge, "MD5 Research," Second International Conference on Multimedia and Information Technology, pp. 271-273, 2010.
5. Keonwoo Kim, Un Sung Kyong, "Efficient Implementation of MD5 Algorithm in Password Recovery of a PDF File," Cyber Convergence Security Division, ETRI, Daejon, Korea, pp. 1080-1083.
6. AnakAgungPutriRatna, Ahmad Shaugi, Prima DewiPurnamasari, Muhammad Salman, "Analysis and Comparison of MD5 and SHA-1 Algorithm Implementation in Simple –O Authentication Based Security System," Universitas Indonesia, IEEE, pp. 99-104, 2013.
7. Xiaoling Wei, "MD5 Encryption Algorithm and Application," Yan'an University Computing Center, 2010.
8. Quist-Aphetsi Kester, Lauret Nana, Anca Christine Pascu, Sophie Gire, "A New Encryption Cipher for Securing Digital Images of Video Surveillance Device using Diffle-Hellman-MD5 Algorithm and RGB pixel shuffling, "European Modelling Symposium, pp. 305-311, 2013.
9. Wang Xiayoun, "How to Break MD5 and other Hash Functions," 2005.

10. Kasgar A.K., Agrawal Jitendra, Sahu Santosh, "New Modified 256-bit MD5 Algorithm with SHA Compression Function," International Journal ofComputer Applications, pp. 47-51, 2012.
11. A. Sinha, K. Singh, "A technique for image encryption using digital signature," Optics Communication", pp. 229-234, 2003.
12. Kahate, Atul, 2003, "Cryptography and Network Security," Tata McGraw-Hill, India.
13. William Stallings, "Cryptography and Netwok Security: Principles & Practice," 5th EditionPrentice Hall; 5 edition (January 24, 2010).
14. R. Rivest, "The MD5 Message-Digest Algorithm," Network Working Group, 1992.
15. Zhengi Wang, Lisha Cao, "Implementation and Comparison of Two Hash Algorithms," International Conference on Computational and Information Sciences, pp. 721-725, 2013.
16. X. Wang, D.Feng, X.Lai and H.Yu, "Collisions for Hash Functions," in Crypto, 2004.
17. Bonteh S, "Twenty years of Attacks on the RSA Cryptosystem," Notices of the American Mathematical Society, 46(2):203-213, 1999.
18. Rashmi P.Sarode, Piyush Gupta, NeerajManglani, "A Comparative analysis of RSA and MD5 Algorithm," Journal of Computer Science and Applications, pp. 25-33,2014.
19. Itoh, K., Kunihiro N.,KurosawaK., "Small secret key attack on a variant of RSA,"volume 4964 of Lecture Notes in Computer Science , pp. 387-406, 2008.
20. ShahzadAlam, Amir Jamil, AnkurSaldhi, Musheer Ahmad, "Digital Image Authentication and EncryptionUsing Digital Signature," International Conference on Advances in Computer Engineering & Applications, pp. 332-336, 2015.