ISSN: 2321-7782 (Online)
Volume 3, Issue 10, October 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Digital Security Using Cryptographic Message Digest Algorithm

Disha Shah
Asst. Professor, TMES, College of Computer Application,
Mandvi, Surat,Gujarat, India

Abstract: ***In recent years, with the incredible maturity of data exchange in network environments and increasing the attacker's capabilities, information security has turned into the most significant procedure for data storage and communication. In order to offer such information security the confidentiality, data integrity, and data origin authentication must be certified based on cryptography. This paper presents cryptographic algorithm named as Message Digest Algorithm. It generates digital signature to protect the information.***

Keywords: Cryptography, Security, Message Digest Algorithm, Encryption, Decryption.

I. INTRODUCTION

Cryptography is the science of writing in secret code so that only those for whom it is proposed can read and process it. Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, hidden or meaningless all the way through transmission or storage is termed Encryption. The main persistence of cryptography is to take care of data secure from invaders. The contradictory procedure of getting back the original data from encrypted data is Decryption, which restores the original data.

Security goals of data cover three points namely: Availability, Confidentiality, and Integrity. Cryptography, in modern days is considered grouping of three types of algorithms. They are

(1) Symmetric-key algorithms

(2) Asymmetric-key algorithms

(3) Hash functions

Symmetric algorithms use the same key for encryption and decryption. This is termed as secret key. With the same key messages are encrypted by the sender and decrypted by the receiver. It contains algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), Ron's Code (RCn), and Triple DES. Asymmetric algorithms use different keys. One key (public) is used for encryption and other (private key) is used for decryption. This is named as public key. Public key is known to public and private key is known to the user. It comprises various algorithms like Rivest, Shamir, & Adleman (RSA), Elliptic Curve(EC), Diffi-Hillman(DH). The Hash functions use a mathematical transformation to irreversibly "encrypt" information. It contains algorithms like Message Digest, Secure Hash Algorithm.

II. LITERATURE REVIEW

The work in [4], it has been proposed a new security architecture which implements RSA for both encryption and secure communication purposes, whereas MD5 hashing is used for digital signature and hiding key information. The work in [7], a new cryptography algorithm is identified which is based on block cipher concept. In this algorithm logical operation like XOR and shifting operation are used. Experimental results show that proposed algorithm is very proficient and secured. In [5], the security provided for the message from the third party. So the Digital signature, PRNG (Pseudo Random Number Generator),

Message Digest algorithms are used for encryption of the message and sending to the receiver. The work in [2], the application of MD5 algorithm is implemented for the stream controlled transfer messages in the network. This would be a high security algorithm for data transfer in mobile networking with stream controlled logic. There may a huge number of applications for this algorithm in data transfer in several types of networks.

III. MESSAGE DIGEST ALGORITHM

MD5 was developed from MD, MD2, MD3 and MD4. The MD5 message digest algorithm, developed by Ron Rivest, accepts a message input of various lengths and produces a 128-bit hash code. It has been one of the most widely-used hash algorithms. Message digest functions which are also entitled as hash functions, used to produce Digital Signature of the information which is known as message digest. MD5 algorithm is used to implement integrity of the message which produce message digest of size 128 bits. These are mathematical functions that process information to create different message digest for each unique message.

Message digest algorithm revenues two benefits. Identical messages always generate the same message digest and even if one of the bits of the message changes, then it produce different message digest. The other advantage is that message digests are much shorter than the document from which digests are generated. It processes the message and generates 128- bits message digest. The algorithm involves of the following steps:

1. Append the padding bits
2. Append the length
3. Initialize MD buffer
4. Process message in 512 bit blocks
5. Output generation

IV. PROPOSED ALGORITHM

Here, n is the modulus, e is the encryption exponent and d is the secret exponent or decryption exponent. The algorithm is divided into 5 steps: Key Generation, Digital Signing, Encryption, Decryption and Signature Verification with their working functions are discussed as under:

Step-1: Key Generation

Randomly generate two large prime numbers: p and q.

Calculate n=p * q

Calculate the totient: $\Phi(n)= (p-1) * (q-1)$

Select an integer ‘e’ such that $1< e < \Phi(n)$ and $\gcd(e, \Phi(n)) = 1$

Calculate d, such that $d * e = 1 \bmod \Phi(n)$

The public key is (n, e) and the private key is (n, d).

Step2: Digital Signing

Generate message digest of the document to be sent by using MD5 algorithm.

The digest is represented as an integer m.

Digital Signature S is generated using the private key (n, d), $S= m^d \bmod n$.

Sender sends this signature S to the recipient.

Step 3: Encryption

Sender represents the plain text message as a positive integer m.

It converts the message into encrypted form using the receiver's public key (e, n).

$C= m^e \bmod n$

Sender sends this encrypted message to the recipient.

Step 4: Decryption

Recipient does the following operation:

Using his private key (n, d); it converts the cipher text to plain text 'm'.

$m= C^d \bmod n$

Step 5: Signature Verification

Receiver does the followings to verify the signature:

An integer V is generated using the sender's public key (n, e) and signature S

$V= S^e \bmod n$

It extracts the message digest M1, from the integer V using the same MD5 algorithm.

It then computes the message digest M2 from the signature S.

If both the message digests are identical i.e. M1= M2, then signature is valid.

V. EXPERIMENTAL OBSERVATIONS

Step 1: Key Generation:

1. We have chosen two distinct prime numbers p=23 and q=53.

2. Compute n=p*q, thus n=23*53 =1219.

3. Compute Euler's totient function, Ø(n)=(p-1)*(q-1), thus Ø(n)=(23-1)*(53-1) = 22*52 = 1144.

4. Choose any integer e, such that 1 < e < 1144 that is gcd (e, 1144) =1. Here, we chose e=3.

5. Compute d, d = e-1(mod Ø(n)), thus d=3-1(mod 1144) = 763.

6. Thus the Public-Key is (e, n) = (3, 1219) and the Private- Key is (d, n) = (763, 1219). This Private-Key is kept secret and it is known only to the user.

Step 2: Encryption:

1. The Public-Key (3, 1219) is given by the Cloud service provider to the user who wishes to store the data.

2. Let the message to be send is "hello" which is converted to integer in the following manner:

A=0, B=1 ,a = 27, b=28,c=29 and so on .

So the message "welcome" is encoded to m= 49313829413931

3. Data is encrypted now by the Sender using the corresponding Public-Key which is shared by both the sender and the receiver.

$C=m^e \bmod n$ $C=49313829413931^3 (\text{mod}1219) = 625535179657807535.$

4. This encrypted data i.e., cipher text is send to the recipient.

Step 3: Digital Signature and signature verification:

1. First using MD5 algorithm the message gets converted to message digest i.e. to hexadecimal form.
2. MD1=H(m)= 0x000c00f0000000f0426f00f0726000f0.
3. Message digest in decimal form M1= 012024000024066111024011410802 40.
4. Next digitally signed the message digest MD1 using its own private key d to generate digital signature S.
5. S = (MD1)dmod n= 088702580002588392960258850124 0258.
6. Sender then sends the digital signature S to the recipient.
7. Receiver then computes the integer V using S, e and n.
8. V= S^e mod n= 012024000024066111024011410802 40.
9. Receiver the computes the message digest from S using MD5 algorithm
10. MD2 = 012024000024066111024011410802 40.
11. Since V = MD2, so the Signature is verified.

Step 4: Decryption:

The receiver decrypts the data by computing, m = C^d(mod n) = 49313829413931.

Once the m value is obtained, user will get back the original message using the same encoding technique.

VI. Conclusion

This paper has briefly described the concept of cryptography and its algorithms. There are different types of algorithms which are used to provide the security of the information. In this paper Message Digest algorithm is defined which is divided into 5 steps: Key Generation, Digital Signing, Encryption, Decryption and Signature Verification. This would be a high security algorithm for data transfer. Hash algorithms are key components in many cryptographic applications and security protocol suites.

Acknowledgement

I would like to express my very first thank to my inspiration to make me write this paper and carrying out this work, guiding and motivating with patience throughout the research work and also for getting me in the door at ICRJET. I am also thankful to the ICRJET for providing the opportunity to publish this paper.

References

1. Deepika Sharma, Pushpender Sarao, Sunita Dudi,"Implementation of Md5- 640 Bits Algorithm", International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 5, May 2015.
2. Priyanka Walia Vivek Thapar. "Implementation of New Modified MD5-512 bit Algorithm for Cryptography", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163, Volume 1 Issue 6 (July 2014).
3. Anjula Gupta, Navpreet Kaur Walia, "Cryptography Algorithms: A Review", 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939.
4. Sudhansu Ranjan Lenka, Biswaranjan Nayak," Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm" International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, June-2014.
5. Sreekanth Anyapu, G. Aparna, R., Manognya, D. Ravi Kumar, "Message Security Through Digital Signature Generation and Message Digest Algorithm", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 3, March 2013.
6. AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012.
7. Vishwa Gupta, Gajendra Singh, Ravindra Gupta, "Advance cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012.

8. Rashmi Nigoti, Manoj Jhuria, Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing", International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS).
9. Ronald Rivest, "MD5 Message-Digest Algorithm", rfc 1321, April 1992.
10. Computer Networks 5th Edition by Andrew S. Tanenbaum.

AUTHOR(S) PROFILE

Disha Shah, is presently working as an Asst. Professor in The Mandvi Education Society, College Of Computer Application, Mandvi, Surat, Gujarat. She has teaching experience of 4 years. She has completed her Master Degree in MSc-ICT from VNSGU, Surat in the year 2011. She has participated many National Conferences and Workshops.

