SECURING DATA FROM CYBER CRIME USING COMBINATION OF SHA-1 AND RSA ALGORITHM

[1]Sana Bellary [2]ReshmaNadaf

[1]Electronics and Communication Department, SDM College of Engineering and Technology, Dharwad, Karnataka, India

[1]sanabellary@gmail.com [2]reshma.nadaf27@gmail.com

Abstract—*In this current world, there are more number of cyber crimes occurring nowadays. Our financial information, military information any many more information can be hacked very easily as the internet is the base of all the systems [1]. Even though there are many block cipher techniques used in the cryptography for securing the data, for example Elliptic Curve, RSA, ElGamal etc., but still the data is not highly secured. So to avoid this a novel technique of combining the RSA algorithm and HASH functions. By this technique, confidentail data can be more secured and even prevented from the cybercrimes.*

Keywords— *Cybercrime; RSA; Cryptography; Encryption; Decryption, Data security;*

I.INTRODUCTION

As the internet services are increasing in day today life cybercrimes are also increasing a lot. And security is the important factor in our day today life as he important that can be hacked very easily. For example the financial data which can be hacked during the online transactions by the frauds. Military information can also be hacked by the terrorists. To make the data more secure, the important data should not be disclosed anywhere except the authorized users.

Cryptography is the one of the best technique which provides the security in all the fields. We can specify that the cryptography is the key for data security. Cryptography has two main aspects symmetric key and asymmetric key. Symmetric key is also referred as secret key cryptography which uses single key for encryption and decryption of data [1]. Asymmetric key cryptography is also referred as public key cryptography which uses both public key and private for the encryption and decryption of data. There are several techniques used in the cryptography. Nowadays the most and commonly used symmetric cryptography is DES(Data Encryption Standard). In this DES, 64 bit data is encrypted with the help of 56 bit key. DES provides 64 bit cipher text. The same steps are followed in the reverse manner to get back the plain text. This technique was proved secured till 1988 as it was hacked and it was been proved that it has no much security. So after DES, AES(Advanced Data Encryption) was been introduced. AES uses 128 bits of data which can be encrypted with the help of 128,192 and 256 bits of key. Now the system is not secured as it is been hacked.

Public key cryptography came into existence in the year 1975. Public key cryptography uses both the keys i.e., private key and public key for encryption and decryption.

There are many more techniques used in the cryptography for securing data, to provide data confidentiality, data authenticity etc., RSA is one of those techniques. RSA is the Rivest Shamir Adleman technique, name itself indicates the name of inventors who introduced this technique. This is the technique which is public key cryptography which uses two keys public key and private key cryptography for more data security. But Diffie Hellman was the first public key cryptography which was introduced for the key exchange purpose. Hey the public key and private key are exchanged between User A and User B after that RSA was introduced. RSA provides more data security. Elliptic curve is one of the public key cryptography used for data security purpose.

But in this research we are only giving importance to RSA technique and HASH function. Hash functions are provides fixed amount of data values. Hash functions are the values which provides data integrity. Data integrity is nothing but it is a parameter where if the Sender A sends data to Sender B, and if the hacker hacks that data and changes the data and then send it to Sender B, then the Sender B can come to know that data received is been changed he can analyse that the data is been hacked.

In this paper we are trying to present the combination of HASH functions and RSA algorithm, so that we can achieve the data integrity and as well as the data security.

II.BLOCK DIAGRAM

1. HASH FUNCTIONS

A minor departure from the ,message confirmation code is the restricted hash work. Similarly as with the message authentication code, hash work acknowledges a variable measure message M as message and produces a fixed size yield, alluded to as a hash code[9]. Not yet all like a MAC code a HASH functions are the values which are generated with the help of plain text and the key. The HASH code is a component of the considerable number of bits of the message and gives a mistake location capacity change to any bits in the message brings a change in HASH code. There are many variations in HASH function. SHA 1, SHA2, SHA3 etc.,

In this research we are concentrating on SHA1 (Secured Hash Function-1). In cryptography, SHA 1 is a cryptographic hash work which takes an message and produces the 160 bit hash value known as message digest.

In this SHA 1, it consists of 80 rounds, at the 80th round the message digest or the hash value is been generated.

SHA1 is mainly used for the application such as data integrity, data security etc., the diagram shows one simple round of SHA 1, like this we should perform 80 rounds.

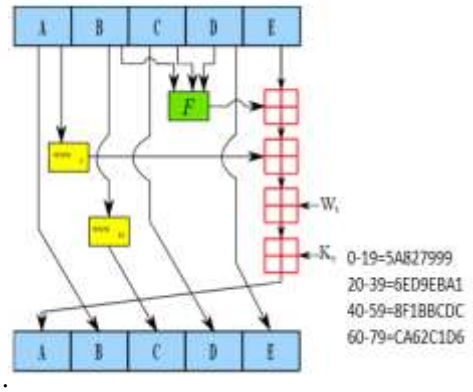

Figure 1-SHA 1 block for first round[9]

Here A,B,C,D,E defines 32 bit words

F is the non linear function which has several computations involved.

$<<<_5$ determines circular shift left for 5 times.

$<<<_{30}$ determines circular shift left for 30 times.

W_t is the variable of the message word for t^{th} round.

K_t is the round constant used for t round.

⊞ denotes modulo 2 addition.

2. RSA TECHNIQUE:

RSA is the public key cryptography technique. Here it is utilized by the computers to encrypt and decrypt the messages. It has two distinctive keys, public key and private key which are respectively use for the encryption and decryption process. Also called as open key cryptography as the one key is kept private and other key is been shared with an another user.

Here in RSA the user will create his own public key and forwards it to an another user, and the public key is based on the two prime numbers, and those prime numbers are kept secret.

RSA algorithm includes mainly four stages:

Key generation, Key distribution, Encryption and Decryption. An essential principle behind RSA is handy to discover three substantial integers e, d and n such that it should satisfy the condition with m i.e.,$0 \leq m < n$.

Steps involved in RSA[2].

1. Select two prime numbers p and q, and for security purposes prime numbers should be selected randomly.
2. Calculate n, n=p*q. n is utilized as the modulus for public and private keys.
3. Calculate $\Phi(n)=(p-1)(q-1)$ where $\Phi(n)$ is the Carmichael's totient function and it kept secret.
4. Choose an integer e, with the goal it should satisfy the conditions below that $1 < e < \Phi(n)$ and gcd(e, $\Phi(n)$)=1; means e and $\Phi(n)$ are co-prime numbers.
5. Decide $d \equiv e^{-1} \pmod{\Phi(n)}$, d is specified as the modular inverse of (modulo $\Phi(n)$).
6. Encryption can be done with the following formula $C=m^e \bmod n$, where m is the plain text or a message.
7. Decryption can be performed with the help of formula $M= C^d \bmod n$. and here the original message is ben retrieved back.

3. BLOCK DIAGRAM OF THE COMBINATION OF RSA AND SHA-1

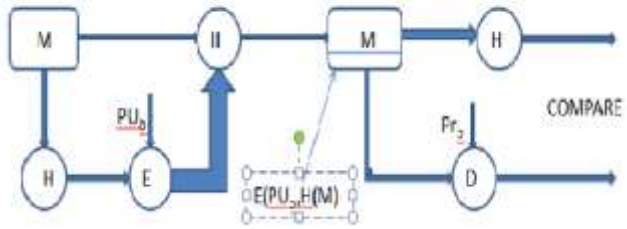

Figure 2- Block diagram for the combined SHA-1 and RSA algorithm.

In this above block diagram, it uses both RSA technique and SHA1 algorithm.

Here 'M' is the message of 512 bits.

'H' is the hash value or the message digest of 160 bits.

PU_b is the public key of user B

PR_b is the private key of user B.

When the message M of 512 bits is applied at the input of SHA1, after processing the 160 bit message digest or the hash values H are been generated. After generating the hash values, with the help of RSA algorithm, public key and private keys are generated which is used for the Encryption and Decryption of the 160 bit hash value. The main goal of using this technique is to achieve data integrity, data security, data confidentiality etc. When the message of 512 bit applied to the SHA1, the message digest or the hash value of 160 bits[9].

The Hash value is been added to the source when the message is known to be correct.

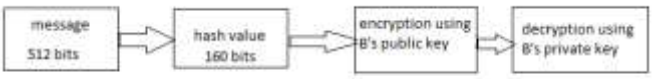

Figure 3-block for generation of hash values

III.USES OF USING HASH WITH RSA

There are many uses involved with RSA algorithm and Hash functions respectively. By using RSA algorithm already it is specified that the data security is been achieved. Data security means the exact amount of data transferring from sender to the receiver without any data leakage.

With the help of hash functions we can determine one specific application i.e., data integrity which is mostly and likely used in wide range in cryptography. Data integrity helps us to achieve the exact data from the user. If there is any change in data sent by the user, receiver can come to know that the data is been changed by the third party with the help of hash functions. Digital signature is also

another application which can be achieved by using hash functions.

With the combination of both hash and RSA algorithm bothdata security and data integrity is achieved. There are many applications which are been achieved such as data confidentiality, data encryption and data decryption, non repudiation at source and destination etc. Non repudiation is nothing but the denying of message after the receiving it or sending it. Source informs that the message has not been sent by that particular source even though the message was sent by the source this is called source non repudiation. Destination non repudiation says that the destination denies that the message is been not received even though the message is received by d destination[4].

IV.RESULTS

For this research we are using FPGA tool, Xillinx 14.7 is been used. and the coding is written in HDL language i.e., Verilog coding is been used.

After using the HASH functions, we can specify that the fine amount of data security and the data integrity is been achieved. Here are some of the screenshots of the outputs for reference purpose.

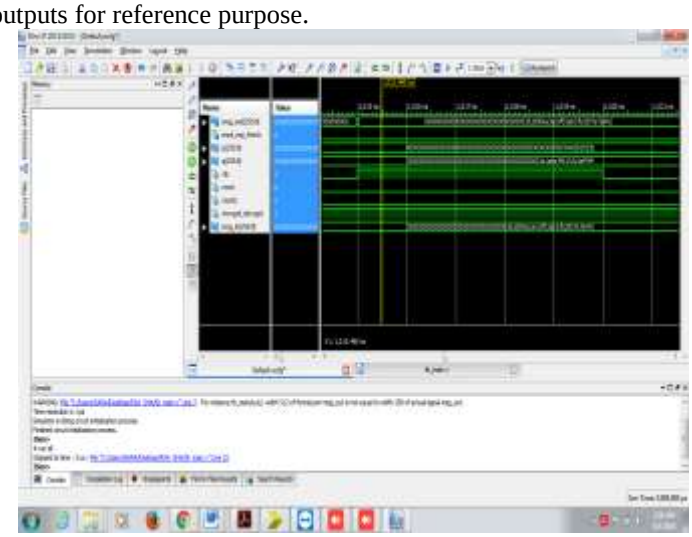

Figure 4- simulation result for the combined work of RSA and SHA-1 algorithm.

The result shows the output of 160 bit hash function, which is divided into 5, 32 bit words Ha, Hb, Hc, Hd, He. For convenient purpose we have divided the output in 32 but words. Actually it is a 160 bit hash value or the message digest.

After getting the hash value of 160 bits, it is encrypted using public key of user B and decrypted using B's private key with the help of RSA algorithm.

CONCLUSIONS

In this paper we have given a brief discussion of RSA algorithm and HASH functions. We have also came across with the result that by using the hash functions data integrity can be achieved accurately. The message 512 bits was given and we have achieved 160 bit message digest or the hash value properly. By using the HASH function data security as well as data integrity is achieved.

REFERENCES

[1] Preventing And Securing Data From Cyber Crime Using New Authentication Methods Based On Block Cipher Techniques.-Prakash Kuppuswamy, Nitya Rekha 2017.

[2]Implementation Of RSA-Lavanya K Galla 2016.

[3] X.Zhang; K.K.Parhi;"On the Optimum Constructions of Composite Field for the AES Algorithm"; IEEE Transactions on Circuits And Systems—II: Express Briefs, Vol. 53, No. 10, October 2006 pp. 1153-1157.

[4] William Stallings- 3rd Edition

[5] National Institute on Standards and Technology Computer Security Resource Center, NIST's March 2006 Policy on Hash Functions accessed September 28, 2012.

[6]A Hybrid Security Algorithm for RSA Cryptosystem Prabhat K. Panda 2017.

[7] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM vol. 21 (2) , pp.120–126, 1978.

[8]Analysis and design of enhanced Rsa algorithm to improve the Security Shikha Mathur 2017.