ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Mathematical RSA Algorithm in Network Security

Sujata Bala[1], Dr. Sahdeo Mahto[2]

Research scholar, Department of Mathematics, Ranchi University, Ranchi, Jharkhand, India[1]

Associate Professor, Department of Mathematics, Ranchi University, Ranchi, Jharkhand, India[2]

ABSTRACT: In day to day growing of larger and complex networks are needs to be a system to protect and secure the information on net. Aim of my paper is to describe a mathematical model for network security. This paper presents a design of data encryption and decryption in a network environment using RSA algorithm with specific coding of message.

KEYWORDS: encryption, decryption, RSA, algorithm,

I. INTRODUCTION

Network security controls and prevents the un-authorized access of data, misuse, refutation, of computer network and other network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. It covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security starts with authentication, commonly with a username and a password. Since this requires just one detail authenticating the user name i.e., the password—OTP NO. Digital signature etc. are require to secure our some secret data.[1]

In network security RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it.[2]

RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1978 and founded RSA Data Security in 1982.[3] Clifford Cocks, an English mathematician working for the UK intelligence agency GCHQ , had developed an equivalent system in 1973, but it was not declassified until 1997. In 2001 digital certificate, smart card biometric authentications are developed with RSA algorithm. In 2005 Cyota a private company specializing in online security and anti-fraud solutions for financial institutions.[4] In 2006 EMC corporation approved RSA stockholder.[5] In 2007 Hyderabad Company developed a RSA software that specialize a file and data security. In 2009, RSA launched the RSA Share Project. [6] In 2011, RSA introduced a new Cyber Crime Intelligence Service designed to help organizations identify computers, information assets and identities compromised by trojans and other online attacks.[7] In 2016, RSA was acquired by and became a subsidiary of Dell EMC Infrastructure Solutions Group through the acquisition of EMC Corporation by Dell Technologies in a cash and stock deal led by Michael Dell.[8]

II. RELATED WORK

THE RSA CRYPTOSYSTEM

RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers. The factoring

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

problem, It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

Suppose that I want to be able to receive secret messages from other people. The fundamental idea is the following. I find a "one-way function", call it E, such that everyone can compute E, but only I can compute the inverse of E. Then anyone can send me a secret message M, by computing E(M), and sending this value to me. Since I am the only one who can compute the inverse of E, I and no-one else can retrieve M.
I.e. M=D(E(M)) where D is inverse of E(M).
I.e. He writes the message as a sequence of integers M_1, M_2 , . . . as explained above. He then computes the numbers $E(M_1)$,$E(M_2)$, . . . and sends these numbers to me. Even if someone interrupts the message, he cannot compute the integers M_i, because he does not know the inverse function.
How I decrypt a message when I receive?
I receive the numbers $E(M_1)$,$E(M_2)$, . . …….and only I can compute this
$M_1=D(E(M_2))$, $M_2=D(E(M_2))$, ……..and so on. Then I translate these numbers into letters, and read the message. Because only I know the value of inverse function D.

THE RSA ALGORITHM involves four steps:
1. Key -generation,
2. Key distribution,
3. Encryption and
4. Decryption
The RSA Algorithm is Creating RSA Public and Private Key in Pair .It can be used for both key exchange and digital signatures. Although employed with numbers using hundreds of digits, the mathematics behind RSA is relatively straight-forward.

III. PROPOSED METHODOLOGY

RSA ALGORITHM
1. Choose two prime large numbers **p** and **q**. then calculate
n=p*q
2. We compute $\boldsymbol{\varphi(n) = (p-1)*(q-1)}$
3. We can Choose a third number ***e*** that is relatively prime to $\boldsymbol{\varphi(n)}$**(** i.e. it doesn't divide evenly into) and
$$\boldsymbol{\varphi(n) = (p-1)*(q-1)}$$
4. We calculate an integer d from the quotient $\frac{(e*d-1)}{(p-1)*(q-1)}$
i.e. $\boldsymbol{e*d \equiv 1\ mod\ \varphi(n)}$
5. The public key is the number pair ***(e,n)*** although these values are public known. It is computationally infeasible to determine **d** from **n,** and **e. if p** and **q** are large enough
6. To encrypt the message ***M*** with the public key creates the 'ciphertext' ***C*** using the equation
$$\boldsymbol{C \equiv M^e\ mod\ n}$$
7. A receiver decrypts the **'ciphertext'** ***C*** with the private key using the equation.
$\boldsymbol{M \equiv C^d\ mod\ n}$ **And private key is** ***(d,n)***

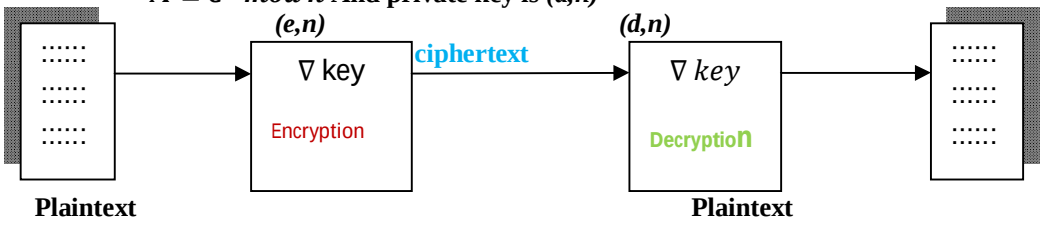

Fig1:encryption and decryption process of message

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

This fig. shows that in first step message is in the form of plaintext. After encryption and use of public key ***(e,n)*** the message changes into ciphertext. In ciphertext form no-body can read this message. After decryption and use of private key ***(d,n)*** in ciphertext it can be change in form of plaintext and then we can read this message.

EXAMPLE

Suppose two persons are communicating to each other and there are many persons between this open communication link, then how they send a secret message to each other through this open communication link and no one can be read this. So now we consider an example and proceeds the following steps.

KEY DISTRIBUTION

Suppose that Aliya wants to send a secret message to Akash. For this security they decide to use RSA Algorithm, Aliya must know Akash's public key to encrypt the message and, Akash use her private key to decrypt the message. To enable Aliya send his encrypted messages, and Akash transmits her public key (*e.n*) to Aliya via a reliable, but not necessarily secret route. Akash's private key (*d*), is never distributed.

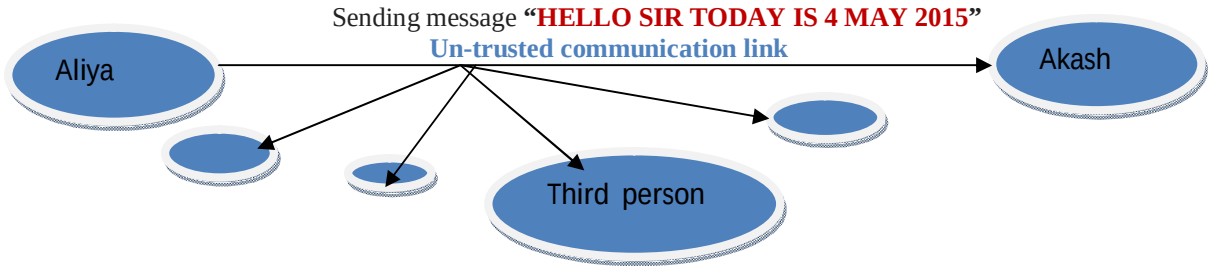

Fig:2 **A**liya send a message to Akash through open & un-trusted link

This fig. shows that Aliya wants to send a secret message to Akash through an open link where many person are there who hacked her message on the way. But Aliya wants only send a message to, Akash and no-body can read this message so Aliya and Akash use the RSA algorithm method to solve this problem.

PROBLEM: Aliya wants to send a message third (many) person to Akash (and only to Akash) through an un-trusted communication link.

ENCRYPTION

Aliya obtains Akash's public key, and he can send a message
"HELLO SIR TODAY IS 4 MAY 2015" to Akash.

She first turns ***"HELLO SIR TODAY IS 4 MAY 2015"*** (strictly speaking, the un-padded plaintext) into integer function .The message must be converted to a string of numbers. In practice, ASCII (American Standard Code of Information Interchange) numbers are usually used; we will use our usual code like A = 01, B = 02,…..,, Z = 26,& for numbers. 1-27, 2-28,3-29…….9-35 0-36 and 00 for space. So, "HELLO SIR TODAY IS 4 MAY 2015" would be converted to a string and it is plaintext as

M="080512120019091800201504012500099190030001301250028362731"

Aliya computed this message into ciphertext C using Akash public key.(e,n) This can be done reasonably quickly, even for 500-bit numbers, using modular exponentiation. Aliya then transmits *c* to Akash.

$$c \equiv M^e \pmod{n}$$

DECRYPTION

Akash can recover M="022523050024041700150549012000042400350007012052310326"
Before decryption the message can read as "**BYWWE XDEQ OE#AT DX 9 GAT *5CZ"**
Which has no meaning. And nobody can understand this message
Now, Akash only one who knows the inverse function. He creates the function so he knows the public encryption key and private decryption key both. He knows the value of e and d, so he computes this message as.
From *c* by using her private key exponent *d* by computing

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

$$M \equiv C^d \pmod n$$

Given M ,He can recover the original message *M* (Third person)by reversing the padding scheme.
"0805121200190918002015040125000991900300013012500283627 31"

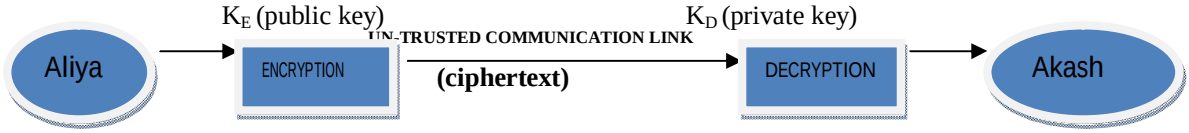

Fig:3 Aliya send a message to Akash through a public key K_E and private key K_D

This fig shows that In RSA Aliya use a public key K_E to send a message to Akash. Then after encryption the message will change in form of ciphertext and in this form nobody can read this message without using decryption key K_D. Akash knows the private key so only he can easily read this message.

Now Akash compute the message as
"HELLO SIR TODAY IS 4 MAY 2015"

- Should be easy to compute for Akash /Aliya (who know the key)
- Should be difficult to compute for third person(who does not know the key)

IV. SIMULATION AND RESULTS

MATHEMATICAL CALCULATION BEHIND ENCRYPTION AND DECRYPTION

Step 1 Choose two prime large numbers **p=5** and **q=11**. then calculate

$$n=p*q=55$$

Step 2 $\varphi(n) = (p-1)*(q-1)$

$$\varphi(n) = (5-1)*(11-1)=40$$

Step 3 we choose ***e=7*** i.e. relatively prime to 40

Step 4 calculating d

$$e*d \equiv 1 \bmod \varphi(n)$$

$$7*d \equiv 1 \bmod 40$$

Using Euclid's extension theorem and we get **d=23**

So our public key is **(7,55)** and private key is **(23,55)**

Here M= "0805121215001909180020150401250009190030001301250028362731"

This message is in plaintext and it change into "ciphertext" as

$C \equiv M_i^e \bmod n$ Where **e=7** and **n=55**

And the ciphertext change in to the plain text as

$M \equiv C_i^d \bmod n$ **Where d=23 and n=55**

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Here the plaintext as form i.e. (M)= "080512121500190918002015040125000919003000130125002836273 1"

Here M_1=8, $E(M_1)=8^7 \bmod 55=2$ M_{13}=04, $E(M_{13})=4^7 \bmod 55=49$

M_2=05, $E(M_2)=5^7 \bmod 55=25$ M_{14}=1, $E(M_{14})=1^7 \bmod 55=1$

M_3=12, $E(M_3)=12^7 \bmod 55=23$ M_{15}=25, $E(M_{15})=25^7 \bmod 55=20$

M_4=12, $E(M_4)=12^7 \bmod 55=23$ M_{16}=00 , $E(M_{16})=0^7 \bmod 55=00$

M_5=15, $E(M_5)=15^7 \bmod 55=5$ M_{17}=9, $E(M_{17})=9^7 \bmod 55=4$

M_6=00, $E(M_6)=00^7 \bmod 55=00$ M_{18}=19, $E(M_{18})=19^7 \bmod 55=24$

M_7=19, $E(M_7)=19^7 \bmod 55=24$ M_{19}=00, $E(M_{19})=00^7 \bmod 55=00$

M_8=09, $E(M_1)=9^7 \bmod 55=4$ M_{20}=30, $E(M_{20})=20^7 \bmod 55=35$

M_9=18, $E(M_9)=19^7 \bmod 55=17$ M_{21}=00, $E(M_1)=0^7 \bmod 55=00$

M_{10}=00, $E(M_{10})=00^7 \bmod 55=00$ M_{22}=13,$E(M_1)=13^7 \bmod 55=13$

M_{11}=20, $E(M_{11})=20^7 \bmod 55=15$ M_{23}=1, $E(M_{23})=1^7 \bmod 55=1$

M_{12}=15, $E(M_{12})=15^7 \bmod 55=5$ M_{24}=25, $E(M_{24})=25^7 \bmod 55=20$

Then message will change in ciphertext as

"022523230500240417001505490120000424003500070120523103 26" which is in the letter form as

"**BYWWE XDQ OE#AT DX 9 GAT *5CZ"**

Then ciphertext change in plaintext by inverse of these functions, and Akash only compute the inverse of this integer and read this message. He computes this message as this formula

$$M \equiv c^d mod n$$

M_1=2, $D(E(M))=2^{23} \bmod 55=08$

M_2=25, $D(E(M))=25^{23} \bmod 55=05$

M_3=23 $D(E(M))=23^{23} \bmod 55=12$……..

:

:……M_{24}=20, $D(E(M))=20^{23} \bmod 55=25$

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Table:1 calculation for encryption and decryption of the message

Message	M_i	$C \equiv M_i^7 \ mod \ n$		$M \equiv C_i^{23} \ mod \ n$	Integer converts in message
H	08	02	B	08	H
E	05	25	Y	05	E
L	12	23	W	12	L
L	12	23	W	12	L
O	15	05	E	15	O
00	00	00	00	00	00
S	19	24	X	19	S
I	09	04	D	09	I
R	18	17	Q	18	R
00	00	00	00	00	00
T	20	15	O	20	T
O	15	05	E	15	O
D	04	49	#	04	D
A	01	01	A	01	A
Y	25	20	T	25	Y
00	00	00	00	00	00
I	09	04	D	09	I
S	19	24	X	19	S
00	00	00	00	00	00
4	30	35	9	30	4
00	00	00	00	00	00
M	13	07	G	13	M
A	01	01	A	01	A
Y	25	20	T	25	Y

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

00	00	00	00	00	00
2	28	52	*	28	2
0	36	31	5	36	0
1	27	03	C	27	1
5	31	26	Z	31	5

In table 1 we calculate the encryption and decryption of message. i.e when message in form of alphabets and nos. its change to plaintext with certain coding then apply extension Euler theorem and change the message into ciphertext with formula $\boldsymbol{C \equiv M_i^7 \ mod \ n}$.and ciphertext message change into plaintext with $\boldsymbol{M \equiv C_i^{23} \ mod \ n}$ using the formula and the message can be readable as last columns of the table.

After encryption the cipher text change in the form of plaintext and the message

"0805121215001909180020150401250009190030001301250028362731"And it can be read as

"HELLO SIR TODAY IS 4 MAY 2015"

V. CONCLUSION

RSA algorithm is used for securing data transmission. It is works on public and private key both. When some one wants to send a secret message to me with a untrusted communication link then we should use RSA algorithm. From this example we see that when Aliya send a message to Akash. for security they made a function with two prime no .and its inverse function. First she computes this message in as a sequence of integer. Then she take a function E and message will be converted in function of E, i.e function E(M). Nobody can compute this message because they do not have the inverse of E. only Akash knows the inverse so he computes the message as D(E(M)) and he can read easily.
Cryptography is playing a major role in data protection in applications running in a network environment. It allows people to do business electronically without worries of deceit and deception in addition to ensuring the integrity of the message and authenticity of the sender. It has become more critical to our day-to-day life because thousands of people interact electronically every day; through e-mail, e-commerce, ATM machines, cellular phones, etc. This geometric increase of information transmitted electronically has made increased reliance on cryptography and authentication by users.

REFERENCES

[1] E. Eugene Schultz, " Windows NT/2000 Network Security," New Riders Publishing, August 2000, 375 pages.
[2]Steve Burnett and Stephen Paine. RSA Security's official guide to cryptographynla.gov.au/anbd.bib-an24051951
[3] Rivest; Ronald L. (Belmont, MA), Shamir; Adi (Cambridge, MA), Adleman; Leonard M. (Arlington, MA), **U.S. Patent 4,405,829** The Original RSA Patent as filed with the U.S. Patent Office by December 14, 1977, .
[4] "RSA buys Cyota for $145 million".
[5] "EMC Newsroom: EMC News and Press Releases". *Emc.com*. Retrieved 2012-05-12
[6]https://en.wikipedia.org/wiki/RSA_Security - cite_ref-15
[7]http://www.emc.com/security/rsa-identity-protection-and-verification/rsa-cybercrime-intelligence-service .htm
[7]"Dell Technologies Top FAQs" (PDF). Retrieved 11 September 2016.
[8] Matt Curtin Introduction to Network Security,.
[9] Sivakumar T, Gajjala Askok, k. Sai Venuprathap, August 2013, " Design and Implementation of Security Based ATM theft Monitoring system", International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 3, Issue 1 (August 2013) PP: 01-07
[10] Rijndael algorithm and 256-bit key sizes are specified in the AES standard. Key sizes of 128, 160, 192, 224, and 256 bits are supported by, but only the 128, 192,