Analysis of Cryptographic Technique and Its Applications in Modern Human Life

MOHAMMED NIZAM UDDIN[1], DR. MUHAMMAD HANIF[2], JANNATUL NAIME[3]

[1] *Associate Professor, Department of Applied Mathematics, Noakhali Science and Technology University, Bangladesh*

[2] *Professor, Department of Applied Mathematics, Noakhali Science and Technology University, Bangladesh*

[3] *Masters Student, Department of Applied Mathematics, Noakhali Science and Technology University, Bangladesh*

Abstract- ***In present day Social systems administration framework Data security is the most extreme basic issue in guaranteeing safe transmission of data through the web. Web has turned out to be increasingly across the board, if an unapproved individual can gain admittance to this system, he can keep an eye on us as well as he can without much of a stretch chaos up our lives. System Security and Cryptography is an idea to ensure system and information transmission over remote system. Today information correspondence for the most part relies on computerized information correspondence. The insurance of sight and sound information, delicate data like charge cards, banking exchanges and interpersonal organization security numbers is winding up significant. The security of this classified information from unapproved access should be possible with numerous encryption strategies. Likewise organize security issues are presently getting to be significant as society is moving towards computerized data age. As an ever increasing number of clients associate with the web it pulls in a great deal of digital offenders. The errand of system security not just requires guaranteeing the security of end frameworks however of the whole arrange. In this paper, an endeavor has been made to present the different Network Security and Cryptographic ideas.***

I. INTRODUCTION

Security of information should be possible by a procedure called cryptography. Cryptography is a field in software engineering and science that involves methods of verifying correspondence between two gatherings within the sight of an outsider. It is a system utilized today concealing any secret data from the assault of a gatecrasher. Cryptography is the procedure that includes encryption and unscrambling of content utilizing different components or calculations. The stowing away of data is called encryption. Encryption is a procedure of coding data into a structure that is unintelligible without a disentangling key. This is a procedure wherein a plaintext is changed over to figure content. Plaintext is decoded information or data that speaks to just discernible character. Figure content is a content that comes because of encryption performed on plaintext utilizing a calculation called figure. This message is a good for nothing content and can't be comprehended by anybody. Figure content is otherwise called scrambled or encoded message as it is a non-discernible type of the first message. At the point when the data is unhidden, it is called decoding. Decoding is a turnaround procedure of encryption. It is a procedure of changing over figure content once more into a plaintext that the client can peruse. In cryptography, there utilize a key to unscramble message from encode message. A key is a worth that is a used to encode or unscramble a message. It is a numeric or alpha numeric content or might be uncommon images too. Cryptography named Symmetric cryptography and Asymmetric cryptography systems (1). In symmetric-key cryptography, a similar key is utilized by the two gatherings. The sender utilizes this key and an encryption calculation to scramble information; the recipient utilizes a similar key and the comparing unscrambling calculation to decode the information. In hilter kilter or open key cryptography, there are

two keys: a private key and an open key are utilized. The private key is kept by the recipient and open key is reported to the general population. Some usually utilized uneven cryptography methods are RSA (Rivest, Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm), ECC (Elliptic bend cryptography). Uses of cryptography incorporate ATM cards, PC passwords, and electronic trade.

II. RSA ALGORITHM

The first, and still most normal, open key cryptography execution, named for the three MIT mathematicians who created it — Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977 (2). RSA today is utilized in many programming items and can be utilized for key trade, advanced marks, or encryption of little squares of information. RSA Algorithm depended on the number hypothesis. RSA calculation is an awry cryptography calculation which implies, there ought to be two keys include while imparting, i.e., open key and private key. The possibility of RSA depends on the way that it is hard to factorize a huge whole number. The open key comprises of two numbers where one number is augmentation of two huge prime numbers. What's more, private key is additionally gotten from a similar two prime numbers. So in the event that someone can factorize the huge number, the private key is undermined. Along these lines encryption quality absolutely lies on the key size and on the off chance that we twofold or triple the key size, the quality of encryption increments exponentially. RSA keys can be ordinarily 1024 or 2048 bits in length, however specialists accept that 1024 piece keys could be broken sooner rather than later. Be that as it may, till now it is by all accounts an infeasible errand (3).

III. HOW RSA ALGORITHM WORKS

If we consider the alphabet as numerical value 0 to 25 which is figured out the below table:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Suppose we sent a message “CAT” which numerical value represents 2019.

Using encryption algorithm the cipher text becomes,

$C = M^e (mod\ n) = 2019^3 (mod\ 3127) = 2669.$

Also using decryption algorithm from the cipher text we again get the plain text message,

$M = C^d (mod\ n) = 2669^{2011} (mod\ 3127) = 2019.$

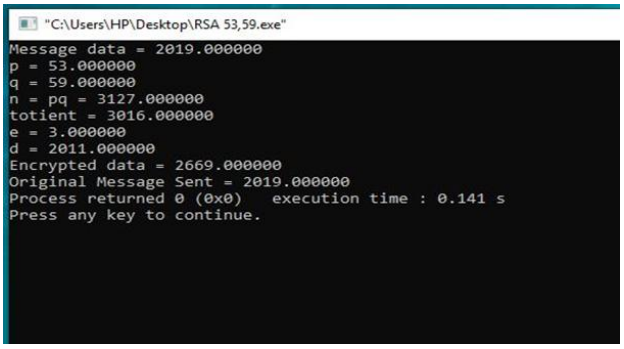
Write the above example using C Programming:

```
//Program for RSA asymmetric cryptographic algorithm
#include<stdio.h>
#include<math.h>
//to find gcd
intgcd(int a, int h)
{
int temp;
while(1)
   {
temp = a%h;
if(temp==0)
return h;
a = h;
      h = temp;
   }
}

int main()
{
   //2 random prime numbers
double p = 53;
double q = 59;
double n=p*q;
double count;
double totient = (p-1)*(q-1);
    //public key
   //e stands for encrypt
double e=3;
   //for checking co-prime which satisfies e>1
while(e<totient)
{
count = gcd(e,totient);
if(count==1)
```

```
break;
else
e++;
   }
   //private key
   //d stands for decrypt
double d;
   //k can be any arbitrary value
double k = 2;
  //choosing d such that it satisfies d*e = 1 + k * totient
   d = (1 + (k*totient))/e;
doublemsg = 2019;
double c = pow(msg,e);
double m = pow(c,d);
   c=fmod(c,n);
   m=fmod(m,n);
printf("Message data = %lf",msg);
printf("\np = %lf",p);
printf("\nq = %lf",q);
printf("\nn = pq = %lf",n);
printf("\ntotient = %lf",totient);
printf("\ne = %lf",e);
printf("\nd = %lf",d);
printf("\nEncrypted data = %lf",c);
printf("\nOriginal Message Sent = %lf",msg);
return 0;
}
```

Output:



IV. APPLICATIONS OF CRYPTOGRAPHY IN MODERN HUMAN LIFE

The importance of cryptography is increasing day by day at the rate of the use of computer security. The use of cryptography is encryption communications between us and another system. This is most commonly used for communicating between a client program and a server. The applications of cryptography in modern human lives are discuss below:

1. Secure Communication: the clearest utilization of cryptography and the one those we all utilization every now and again, is scrambling interchanges among us and another framework. This is most ordinarily utilized for conveying between a customer program and a server. Models are an internet browser and web server, or email customer and email server. Netscape has built up an open key convention called Secure Socket Layer (SSL) for giving information security layered between TCP/IP (Transmission Control Protocol/Internet Protocol) and application conventions, (for example, HTTP, Telnet, NNTP, or FTP) (4). SSL underpins information encryption, server verification, message honesty, and customer validation for TCP/IP associations. SSL utilizes the RSA open key cryptosystem for the confirmation steps. After the trading of keys, various distinctive cryptosystems are utilized, including RC2, RC4, IDEA, DES and triple-DES (5). The best model is web encryption, since here you can pick between a reasonable or encoded form of a site by exchanging among HTTP and HTTPS in the URL. Most huge organizations currently utilize the encoded structure of course, and you'll see that any visit to Google, Facebook and different locales will be to the HTTPS rendition of the site (6). This is gone with in ongoing programs by additional data, including a latch to demonstrate that it is HTTPS. Something you can attempt is to tap the lock on a scrambled page, and your program will disclose to you increasingly about the page security. It will likewise reveal to you the particularly applicable certainty of the genuine site name you're visiting. In this manner, in case you're entering a secret phrase in a page, kindly watch that it is HTTPS (7).

2. Network Security: Cryptography is the fundamental and productive fixing to the formula of security arrangements. With the entry of new age correspondence frameworks and rapid systems later on, cryptography will have a key task to carry out (8). Web security is a tree limb

of PC security explicitly identified with the Internet, frequently including program security yet in addition organize security on an increasingly broad level as it applies to different applications or working frameworks on an entirety. Various techniques have been utilized to secure the exchange of information over the system, including information encryption. Remote security is the avoidance of unapproved access or harm to PCs utilizing remote systems. The most widely recognized kinds of remote security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) (9). WAP security is fundamentally given by the Wireless Transport Layer Security (WTLS), which gives security benefits between the cell phone and the WAP passage to the Internet. Advanced marks are usually utilized for checking the validness of computerized records and messages (10). It guarantees the beneficiary that the got message has originated from a known sender and the respectability of the message has not been modified during its transmission procedure. In system security, advanced marks are generally utilized the paper reports in the association which are presently supplanted with the electronic archives. One can't deny their mark later on the off chance that they have marked the report. Consequently, computerized marks ought to be considered as one of the safety efforts while arranging information security in this association. Advanced marks depend on open key cryptography, otherwise called topsy-turvy cryptography. Utilizing an open key calculation, for example, RSA and DSS (11). The computerized mark utilizes a hash code or message digest calculation and an open key mark calculation. The arrangement is as per the following:

- The sender makes a message.
- The sending programming creates a hash code of the message.
- The sending programming produces a mark from the hash code.
- Using the sender's private key.
- The twofold mark is appended to the message.
- The getting programming keeps a duplicate of the message signature.

These days, Digital Signatures are utilized in Government, (for example, expense forms, confirming business-to-government exchanges), medicinal services industry, Manufacturing organizations and budgetary administrations. In system security the other significant subjects is Password. Passwords today are very important because access to a very large number of portals on the Internet, or even your email account, is restricted to those who can produce the correct password.

Secure Money Transferring: We can utilize cryptography to give a way to guarantee that information isn't adjusted during transmission, for example its uprightness is protected. In electronic subsidizes move, it is significant that honesty be kept up. A bank can lose millions if an exchange is illegally blocked. Electronic banking-which gives different financial administrations through web, changed the methods for business directed in banks radically. Additionally called as web based banking (12; 4). To verify the moving cash through the electronic banking, ATM (Automatic Teller Machine) cards are generally significant. An implanted Crypto-Biometric verification conspires for ATM banking frameworks has been proposed. The client's unique mark is required during an exchange. The unique finger impression picture is encoded through 3D clamorous guide when it is caught, and afterward transmitted to the focal server utilizing symmetric key calculation. The encryption keys are separated from the irregular pixel conveyance in a crude picture of unique mark, some stable worldwide highlights of unique finger impression and from pseudo arbitrary number generator. Various rounds of emphasess utilize diverse keys. The decoding happens at the financial terminal utilizing a similar key. Prior the exchanges in ATMs were encoded with DES; however the exchange processors required the utilization of the more secure Triple DES (13). The Advanced Encryption Standard (AES) calculation includes support for the new encryption standard AES, with Cipher Block Chaining (CBC) mode, to IPSecurity (IPSec). AES has a variable key length- - the calculation can determine a 128-piece key (the default), a 192-piece key, or a 256-piece key. Probably the most developed encryption innovations are utilized to ensure the ATM Cards. Further

cryptographic calculations are utilized in platinum cards, Visas and ace cards. Attractive stripes were presented on check cards during the 1970s when the ATM cards came in. The attractive stripe could store card information which could be perused by physical contact and by swiping on the machine.

V. CONCLUSION

With the rapid growth in the Internet, network data security has become an inexorable concern for any individual or organization whose internal private network is connected to the Internet. For secure personal information the importance of cryptographic techniques are increasing day by day. In the future world becomes cryptographic world. In future, the more mankind dependent on the technology they will connect to the cryptography. In this paper, we have presented the idea of cryptography, world's most popular technique of cryptography which is RSA Algorithm with its example and the applications of cryptography in modern human life.

REFERENCES

[1] Ruohonen, Keijo. MATHEMATICAL CRYPTOLOGY. 2014.

[2] RSASIGNATURE:BEHIND THESCENES. Dragan Vidakovic1, Dusko Parezanovic1, Olivera Nikolic2 and Jelena Kaljevic2. 2, 2013, Advanced Computing: An International Journal (ACIJ), Vol. 4.

[3] Number Theory and Public-Key Cryptography. Pointcheval, David. s.l. : World Scientific Publishing, New Jersey, 2001, 2000, Combinatorial and Computational Mathematics.

[4] Review on Network Security and Cryptography. Kumar, Shyam Nandan. 2015, International Transaction of Electrical and Computer Engineers System, pp. Vol. 3, No. 1, 1-11 .

[5] Review: Network Security Mechanisms and Cryptography. Khan, Mohammad Tanveer. 7, 2017, Vol. 6. ISSN.

[6] A research Paper on Cryptography Encryption and Compression Techniques. Kumari, Sarita. 4, 2017, Vol. 6, pp. 20915-20919 . ISSN.

[7] A Review on Cryptography, Attacks and Cyber Security. Anu and Divya Shree, Seema Ahlawat. s.l. : International Journal of Advanced Research in Computer Science, 2017, Vol. 8. ISSN.

[8] A Research Paper on New Hybrid Cryptography Algorithm. Prof. Swapnil Chaudhari1, Mangesh Pahade2, Sahil Bhat3, Chetan Jadhav4,Tejaswini Sawant5. 5, 2018, INTERNATIONAL JOURNAL FOR RESEARCH & DEVELOPMENT IN TECHNOLOGY , Vol. 9. ISSN.

[9] HARDWARE SECURITY IN CASE OF SCAN-BASED ATTACK ON CRYPTO-HARDWARE. Mehta2, Jayesh Popat1 and Usha. April 2018, International Journal of VLSI design & Communication Systems (VLSICS, Vol. 9.

[10] Network Security with Cryptography. Prof. Mukund R. Joshi, Renuka Avinash Karkade. 1, January 2015, International Journal of Computer Science and Mobile Computing, Vol. 4, pp. 201 – 204 . ISSN.

[11] Review: Network Security Mechanisms and Cryptography. Khan, Mohammad Tanveer. 7, s.l. : ISSN, July 2017, International Journal of Computer Science and Mobile Computing,, Vol. 6, pp. 138 – 146 .

[12] Cryptography – Security in E-Banking. Dixit, Uma. s.l. : e-ISSN: 2278-487X, p-ISSN: 2319-7668 , IOSR Journal of Business and Management (IOSR-JBM), pp. 33-37 .

[13] Review on Network Security and Cryptography. Kumar, Shyam Nandan. 2015, International Transaction of Electrical and Computer Engineers System, Vol. 3.