Enhancing the Communication Channel Through Secure Shell And Irrational DES

S.R.M.Krishna,Paradeep singh jamwal,K.padma priya,P.Hema Vishnu

Abstract:--- As the internet grows in popularity and therefore also in size more and more transmission takes place mainly because the technology is more readily available and applications have become more user friendly allowing entry to less sophisticated user over a broad spectrum.most data transfer are mainly text based not secure and vulnerable to various forms of security risks. So the model that uses SSH for securing channel like intranet/internet which provides client authentication encryption and decryption with high degree of security by transferring the data in an encrypted format, up on this model enhances the efficiency of data transmission by encrypting or decrypting the data with irrational DES.

DES is a cryptographic standard however,the applications of it limited because of small key space based on irrational number.Moreover the permutation controlled by data can be performed at high speed in generic cpu.this scheme also expands the key space without costing more to run.and also finally through the combination of secure shell(ssh) and irrational DES not only enhances the security of communication channel.it also provides varius applications like remote user creation,remote user deletion,remote command execution,remote system shutdown ,remote file transfer applications in an highly secure manner.

Index Terms – remote ssh, irrational DES, remote Administration.

INTRODUCTION

This paper addresses the problem of providing a secure means of client to client or server to server or client to server over an insecure channel like internet.The paper aims to use the SSH and irrational DES which is the which is the enhanced DES algorithm for securing the transmission channel between any two remote computers.

A.SECURE SHELL

SSH™ (or *S*ecure *Sh*ell) is a protocol which facilitates secure communication between two systems using a client/server architecture and allows users to log into server host systems remotely. Unlike other remote communication protocols, such as FTP or Telnet, SSH encrypts the login session, making it impossible for intruders to collect unencrypted passwords.

SSH is designed to replace older, less secure terminal applications used to log into remote hosts, such as telnet or rsh. A related program called scp replaces older programs designed to copy files between hosts, such as rcp. Because these older applications do not encrypt passwords transmitted between the client and the server, avoid them whenever possible. Using secure methods to log into remote systems decreases the risks for both the client system and the remote host. This increasing the remote file transfer solutions and it also increases the popularity has been fueled by the broader availability of commercially developed and supported client and server applications for windows,Unix and other platforms and by the effort of the OPENSSH[1] project to develop an open source implementation.

Features of ssh:

The SSH protocol provides the following safeguards:

- After an initial connection, the client can verify that it is connecting to the same server it had connected to previously.
- The client transmits its authentication information to the server using strong, 128-bit encryption.
- All data sent and received during a session is transferred using 128-bit encryption, making intercepted transmissions extremely difficult to decrypt and read.

The client can forward X11[10] applications from the server. This technique, called *X11 forwarding*, provides a secure means to use graphical applications over a network. Because the SSH protocol encrypts everything sends and receives, it can be used to secure otherwise insecure protocols. Using a technique called *port forwarding*, an SSH server can become a conduit tosecuring otherwise insecure protocols, like POP, and increasing overall system and data insecurity.

According to Shannon[3] claims that SSH has three main capapabilities.Secure command shell: such as those available to Linux,UNIX,Windows or the familiar DOS prompt,provide the ability to execute programs and other commands,usually with character input and output.port farwarding:allows a TCP/IP applications data to be securely transmitted over insecure channels.

Secure file transfer:SFTP is an interactive file transfer protocol which performs all operations over the SSH transport layer and is replacement for the original SCP protocol existed in SSH.it is highly recomonded that SFTP is used to perform the file transfer in preference to the legacy FTP protocol. As in the latter,authentication details are transmitted in plain text format and such may be compromised through “password sniffing” attacks.The former also uses the same port as the SSH server,eliminating the need to open another port on the firewall of the router.

According to the van Shannon[3] the SSH protocol provides four basic security benefits.which are user authentication,data encryption, and data integrity.

Authentication : public based and host based authentication .of these,public key authentication is one of the most secure methods to authenticate using SSH.public key authentication uses a public/private key pair,generated typically by using key generation utility.

Data Encryption:when a client establishes a connection with SSH server or independent servers they must agree with cipher they will use to encrypt and decrypt data.The server generally supports the list of ciphers it supports.and the client then selects the first cipher in its list that matches one on the server’s list.session keys are the “shared keys described above and are randomly generated.both the client and server uses the same key for both encryption and decryption.

Data Integrity : Even with SSH encryption,the data being sent over the network could still be vulnerable to some one inserting unwanted data into the data.SSH uses HMAC algorithms to greatly improve up on SSH’s simple 32-bit CRC data integrity checking method.

SSH enabled applications are gaining popularity because of the security they supply for the task carried out over the network.some of the popular one are putty,SSH client for windows and VNC over SSH [5].As a security protocol,SSH has not been as popular as SSL[9].

B.THE REALIZATION OF DES ALGORITHM

According to the figure 1, it transforms a block (L,R) according to the following invertible formula:

$Li=Ri-1$ and $Ri=Li-1(+) f(Ri-1,Ki)$, where E is a fixed expansion permutation which maps Ri-1 from 32 to 48 bits.The 16 sub-keys are produced by key table which details shown in figure 2.S is an selection function including 8 groups.there are 8 boxes which map Ri-1 from 48 to 32 bits.P is other 32-bit permutation.they are all fixed.as can be seen from figure 2,the 64 bit key produces 16 sub-keys through the fixed permutation and shift.therefore16 sub keys are same in each group.This will lead to the insecurity of information,and some improved sheme are proposed to overcome these defects which on is the new algorithm irrational DES.

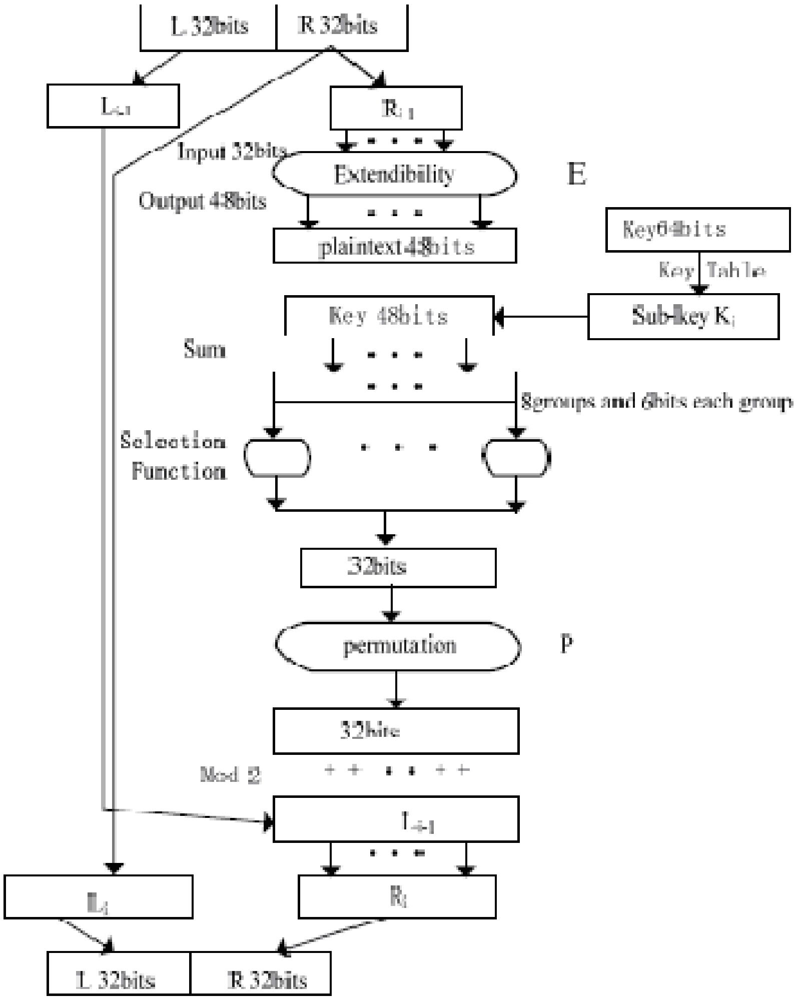


Figure 1. The existing DES

C. DES BASED ON IRRATIONAL NUMBER

In order to solve the problem that the 16 sub keys are same in each group and the key space is too small,the improved scheme based on irrational number is proposed.it not only increases the randomness of the sub-keys of each group,but also extends the key space.which shown in Figure 2.

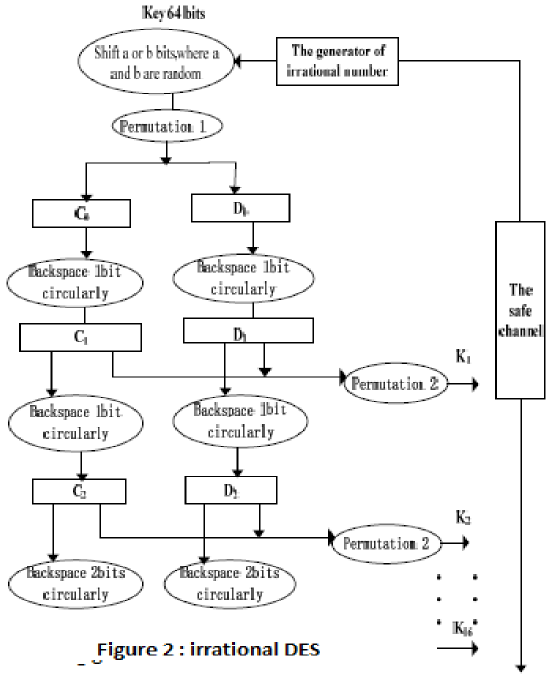

Key 64 bits
Shift a or b bits,where a and b are random
The generator of irrational number
Permutation 1
C0
D0
Backspace 1bit circularly
Backspace 1bit circularly
C1
D1
Permutation 2
K1
The safe channel
Backspace 1bit circularly
Backspace 1bit circularly
C2
D2
Permutation 2
K2
Backspace 2bits circularly
Backspace 2bits circularly
K16

Figure 2 : irrational DES

As can be seen from Figure 2, the 64-bit key controlled by irrational number to shift before the -sub-key being produced.Therefore the key is not directly invoved in the production of the sub keys.

In order to increase the randomness of sub-key,the production and selection of 'a' and 'b' used for shifting, is transmitted to the receiver through the safe channel.For example, selecting two 2-digit decimal numbers after the decimal point of the irrational number squart(2) or π randomly,then let 'a' equal to the first number, and 'b' be equal to the other number.another two number which are selected in the same way are made XOR(exclusive or).if the result is odd there will be 'a' bits shifted,otherwise 'b' bits will be shifted.

II CONTRIBUTION

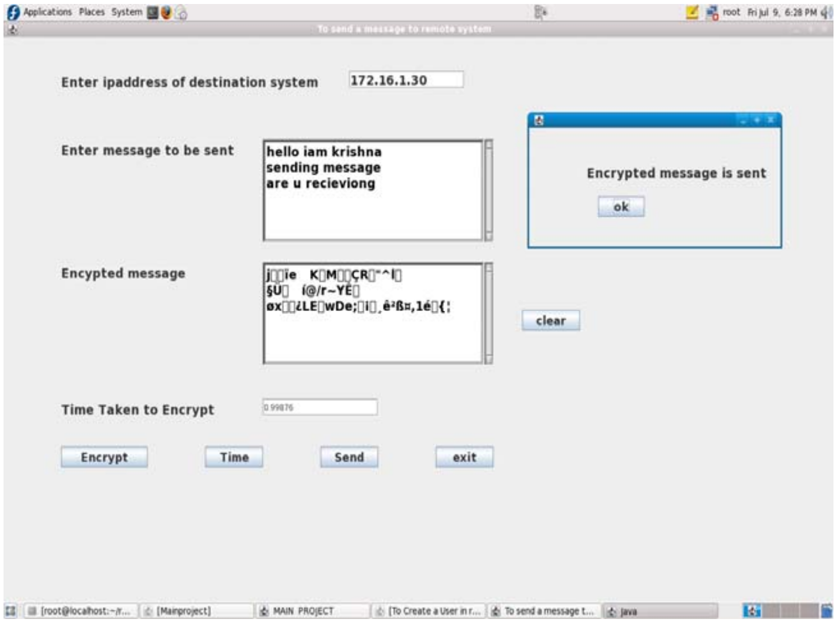
The running time that DES took as much as irrational DES. Ie the confidentiality of the key is enhanced without spending more time,secondly based on the same plain text and key, the cipher text of DES after several simulation is the same,but it is random about the DES with irrational numbers. i.e the key space is expanded through increasing the randomness of sub-keys. And it is combined with secure shell protocol the proposed model provides maximam amount of security to an insecure communication s link between remote clients and servers.This model enhances the security of communication channel.in which some of the following aspects are unique.The system offers supreme security due to double encryption.i.e once with irrational DES and once with RSA in builtness of SSH protocol.SSH is normally used to secure applications like Telnet,and FTP but in this model it is used very similar to SSL.Like SSL, it runs over TCP/IP and secures the data sent between TCP/IP or client/server applications,retaining all the security benefits of SSH.not only that SSH also provides various administration applications like remote command execution,remote user creation or deletion or remote shutdown or reboot or file transfer application in an highly secure manner.

III DESIGHN AND IMPLEMENTATION

Figure 3 shows the arrangement of high level secure communication of clients to server or clients to clients.

A. SSH Server Application Implementation

The GUI is where the user interact s with the system.it receives data input from user and displays displays received information in both encrypted formate and sent data also.



Enter ipaddress of destination system 172.16.1.30

Enter message to be sent
hello iam krishna
sending message
are u recieviong

Encypted message
j□□ïe K□M□□ÇR□ˉ^l□
§U□ í@/r~YÈ□
øx□□¿LE□wDe;□i□¸ê²ß¤,1é□{¦

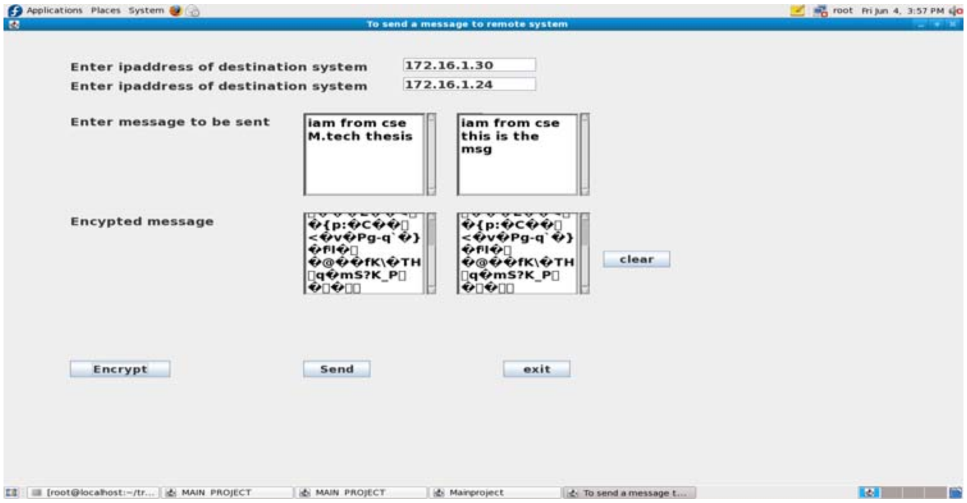
Time Taken to Encrypt 0.99876

Encrypted message is sent

Figure 3:Server application GUI

B.SSH Client Application Implementation

The process of setting up an SSH secured communication channel is as follows :- configure the encryption algorithms for use from client to server and from server to client, - configure the hash algorithm used in both directions,-use this properties(containing the configurations) object and use this as parameter for establishing a SSH connection and subsequently returning a handle on the connection by means of an object .- use the toolkit's password authentication method s-instantiate the channel class , and use the channel object as a parameter for the open channel method (of SSH connection object).through SSH connection and with irrational DES the multiple messages also can be passed to the various client to servers.



Enter ipaddress of destination system 172.16.1.30
Enter ipaddress of destination system 172.16.1.24

Enter message to be sent

iam from cse
M.tech thesis

iam from cse
this is the
msg

Encypted message

�{p:�C��□
<�v�Pg-q`�}
�fl�□
�@��fK\�TH
□q�mS?K_P□
�□�□□

�{p:�C��□
<�v�Pg-q`�}
�fl�□
�@��fK\�TH
□q�mS?K_P□
�□�□□

Figure 4:SSH client application GUI

C SSH Administration

Automatic login remote host

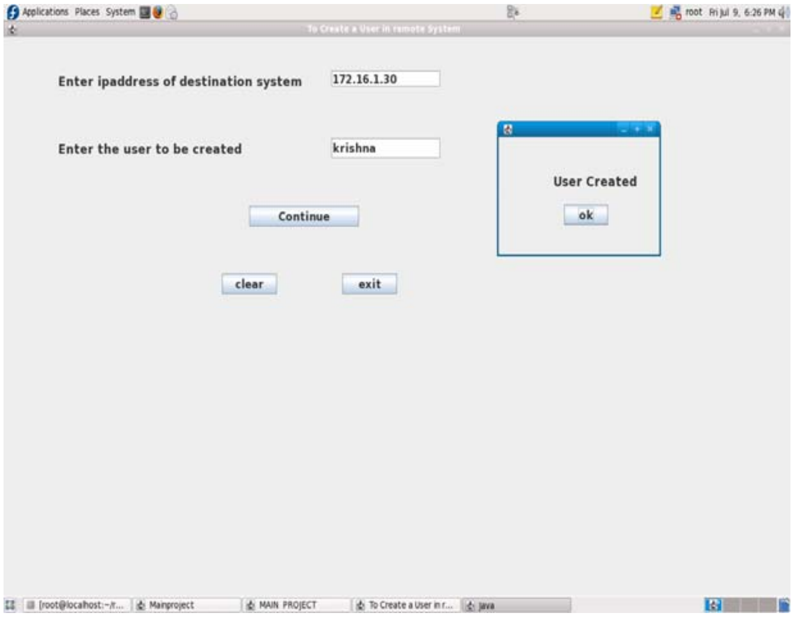
The person under consideration is the system administrator. He has different responsibilities while working in a network. He may have a requirement to login to client systems and do the necessary modifications. For this, if he is coerced to key in the password then there is a high probability for the password to be sniffed and intruders attacking the system? To overcome these hurdles we have provided the feature, automatic login to remote host.

Creating users/Deleting users

The system administrator has the responsibility of supervising the network. In this effort, he might be required users in the system. So, this feature allows him to create users.

Steps:

Connect to the remote host through secure shell
Provide proper password through secure shell
crate the users through command “user add” by sending command in encrypted format using secure shell.



Enter ipaddress of destination system: 172.16.1.30

Enter the user to be created: krishna

User Created

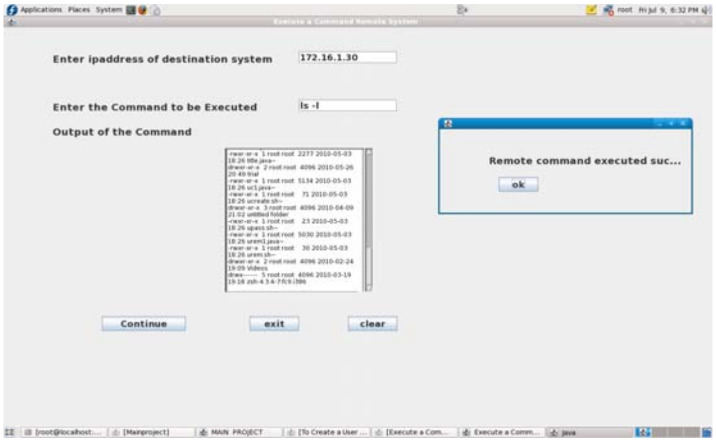
Figure 5:SSH remote user creation or deletion

Execution of command(eg. ls, cat, finger, find)

Unix supports commands like cat, finger, find etc. each command is a file. The commands are executed to accomplish different functionalities. For example, ‘ls’ command is used to list all the files. So, this feature allows administrator to execute the different commands.

Steps:

1. Connect to the remote host through secure shell
2. Provide proper password through secure shell.
3. Execution of any command will be done by passing corresponding executable command



Enter ipaddress of destination system: 172.16.1.30

Enter the Command to be Executed: ls -l

Output of the Command

```
-rwxr-xr-x  1 root root  2277 2010-05-03
18:26 title.java~
drwxr-xr-x  2 root root  4096 2010-05-26
20:49 trial
-rwxr-xr-x  1 root root  5134 2010-05-03
18:26 uc1.java~
-rwxr-xr-x  1 root root    71 2010-05-03
18:26 ucreate.sh~
drwxr-xr-x  3 root root  4096 2010-04-09
21:02 untitled folder
-rwxr-xr-x  1 root root    23 2010-05-03
18:26 upass.sh~
-rwxr-xr-x  1 root root  5030 2010-05-03
18:26 urem1.java~
-rwxr-xr-x  1 root root    30 2010-05-03
18:26 urem.sh~
drwxr-xr-x  2 root root  4096 2010-02-24
19:09 Videos
drwx------  5 root root  4096 2010-03-19
19:18 zsh-4.3.4-7.fc9.i386
```

Remote command executed suc...

Figure 6:SSH remote command execution

<u>Rebooting / shut down of remote system</u>

In some cases, after installing the software the system may be required to reboot. In this regard, the system administrator can reboot the remote system after the software has been installed.

<u>Steps:</u>

1. Connect to the remote host through secure shell
2. Provide proper password thorough secure shell.
3. Reboot or shut down of the remote system will be done through the “power off” command

IV TESTS & RESULTS

This section provides some of the tests carried out and presents their results.

Channel confidentiality :

Verifying whether tha data can be transmitted between client and server is in fact encrypted both with irrational DES and SSH protocol which protecting the system against passive attacks which is shown in figure 7

```
Data: hello iam a professor sending paper to ieee
SSH with irrational DES:.
    Encrypted data:WRPP$%&&@@#ji**^%%!!pp
Data:Basically iam implemtning paper through SSH
SSH with irrational DES:
    Encrypted data:QI&&^ttECGhp&^^5%#$$$!(R.
```

Figure 7 : encrypted data ssh with irrational DES

SSH with irrational DES time comparisons:

The following table describes the comparison of encryption or decryption time periods with existing DES and ssh with irrational DES.

EDESt --- encryption time period for existing DES.
EIDESt – encryption time period for ssh with irrational DES.
DDESt – decryption time period for existing DES.
DIDESt -- decryption time period for ssh with irrational DES.

EDESt	EIDESt	DDESt	DIDESt
0.66789	0.66709	0.65779	0.64709
0.78699	**0.798669**	**0.98699**	**0.798669**
0.62346	0.614408	0.72346	0.694408
0.88789	**0.87445**	**0.88789**	**0.87445**

Table 1: time comparisons for Des vs Sshides

SSH with irrational DES cipher text comparisons :

The following table describes about the cipher text generation for existing DES and ssh with irrational DES.in which the cipher text for the same plain text is always same with existing DES whereas differ in ssh with irrational DES which causes a high security of protection against the attacks for the message

CDES ---- cipher text for existing Des
CIDES ---- cipher text for ssh with irrational DES.
PDES --- plain text for existing DES
PIDES --- plain text for ssh with irrational DES.

PDES	CDES	PIDES	CIDES
Implementing a paper	ERT@7&&rwhhn^%%	Implementing a paper	wwPP%&&jut%%wrt
Implementing a paper	ERT@7&&rwhhn^%%	Implementing a paper	pRt$$@@eerTTyuj
Publishing paper from enngg	ytpssf@@qqwrtypp	Publishing paper from enngg	Ss#^&&ERTwzkl@12Pp

Table 1: cipher text comparisons for Des vs Sshides

V. CONCLUSION

The results presented in section iv are extremely good.They clearly showed that: - the data being transmitted between client and server is in fact encrypted, protecting the system against passive attacks.and not only that the running time that existing DES took as much as that of SSH with irrational DES.and the confidentiality of the key is enhanced without spending more time.and the based on the same plain text and the key the cipher text of DES after several simulation is the same but it is random about the SSH with irrational DES.

VI REFERENCES

[1] Open SSH , 2002 The Open SSH project[Online].Avaialable From http://www.openssh.org.
[2] SSh 2003 .Secure shell client for windows 2003 [Online].Available from http://www.ssh.com
[3] Shannon C E.Communicalion Theory of Secrecy Sytems[J].bell Systems Technical Journal,1949:28:656-715
[4] Feng Guodeng, Pei Ding Cryptography introduction [M].BeiJing ▪ Science Press ▪ 1999
[5] SSH tools 2003.Open sourse SSH toolkit for java [online] Available from http://www.sshtools.com.
[6] Sun Microsystems, inc 2002 . Java card Toolkit 2.1[Online] Available from http://www.sun.com
[7] C.GU “Dynamic DES algorithm” Computer Applications And software. VOL .24 No 7, pp.164-166, jul.2007.
[8] F.Y. Wang “Dynamic key 3DES Algorithm of Descrete System Based on Multi-Dimension Chaos”, Microelectronics & Computer, Vol.22 No.7,pp.120-123,2005.
[9] Joan Daemen and Vincent Rijmen 2002, ” AES – The Advanced Encryption Standard”, Springer.
[10] Alfred J. Menezes 1993, ” Elliptic curve public key cryptosystems”, Kluwer Academic publishers, I Edition.
[11] R. Enns, “NETCONF Configuration Protocol,” Juniper Networks, RFC4741, Dec. 2006.
[12] Neil Koblitz 1994, ” A Course in Number Theory. and Cryptography”, Springer, II Edition.
[13] Joan Daemen and Vincent Rijmen 2002, ” AES – The Advanced Encryption Standard”, Springer.