A New Color based Symmetric Encryption Algorithm

Ajit Singh[1], Kamal Sardana[2]
Assistant Professor[1] , Assistant Professor[2]
Department of Computer Engineering[1]
Department of Electronics and Communication Engineering[2]
The Technological Institute of Textile & Sciences, Bhiwani[1,2], India[1,2]

Abstract:- In today's environment, an electronic security being an important aspect for high performance communication networks. Therefore a secure policy need to assure the security and privacy of information that is sent over the electronic communication media is in great need. So in this paper, we have introduced a newer a color based symmetric cryptographic approach which is being implemented in secure and reliable path selection based policy system to achieve security in ISP's networks.

Keywords:-Policy Based Routing, BGP (Border Gateway Protocol), ISP (Internet Service Provider), Encryption, Decryption.

INTRODUCTION

Cryptography is the way to achieve security by secret writing message to make them non-readable. Secret writing enables you to store sensitive data or transfer it across insecure networks so that it cannot be masqueraded by an attacker. In today's world, most of the means of secure data, code storage and transmission depend on cryptographic techniques.

There are two basic types of cryptography: Symmetric key cryptography (Secret key cryptography) and Asymmetric key cryptography (Public key cryptography). In secret key cryptography, a single key is used by both sender and receiver. For this type of cryptography, it is obvious that the secret key must be known to both the sender and the receiver. The cumbersome problem with this approach is key distribution through a highly unsecured channel. There are few well known examples are DES, RC2, IDEA etc. Asymmetric key cryptography is mainly used to solve the problem of key distribution. In this, two keys are used; private and public keys. Public key is used for encryption and private for decryption purpose. Because users tend to use two keys: public key which is known to public and private key which is known only to the user. There is no need for key distribution through insecure channel, but due to it's relying on mathematical function and large scale computationally it is not efficient for small devices. RSA and Digital signature are well known asymmetric key cryptography.

According to TACIT[8], a cryptographic algorithm consider to be secured if the cost required to break an algorithm is greater than the value of encrypted data then we consider safe. Several cryptanalyst has carried out the study of the requirements for secure use of encryption algorithm.

- It requires a strong encryption algorithm. Moreover, the attacker who knows the algorithm and has access to one or more cipher text would not be able to interpret the plain text from the cipher text.
- Sender and receiver must interchange the private key via a secure fashion.

Realizing the importance of securing the information in communication media, at most care is taken to propose a cryptographic algorithm which produces color cipher rather than text cipher on the basis of hexadecimal color value and some suitable mathematical logic concept, which is being applied on BGP routers to achieve secure and reliable path selection based policy system. In this policy, administrator can implement a policy which defines certain administrative rules and service level agreements corresponding to different characteristic path selection mechanism. When BGP routers receive a packet, it can check the nature of packet against the policy. If it matches, then secure and reliable path selection based policy determine which path to follow rather than pre-defined path. So, this new introduced policy will be helpful to enhance the security, network performance and to meet the customized routing services.

II. ENCRYPTION ALGORITHM

Step 1. Read the character from the text file and get their ASCII value.
Step 2. Convert the ASCII value into 8-bit binary string as $\boldsymbol{b_0b_1b_2b_3b_4b_5b_6b_7}$.
Step 3. A 16-bit binary string is formed by applying binary string expansion method as $\boldsymbol{b_4b_5b_6b_7b_0b_1b_2b_3b_4b_5b_6b_7\ b_0b_1b_2b_3}$.
Step 4. Perform XOR operation on binary string with 16-bit specific key k.
Step 5. Now perform reverse operation on binary string.
Step 6. On the nature of key, an 8-bit specific number and specified operation is chosen from a key specific look-up table and perform that specified operation on the binary string with that number.
Step 7. Convert the resultant binary string into decimal equivalent number.
Step 8. Now convert the decimal value into hexadecimal equivalent number.
Step 9. Then corresponding to hexadecimal value, color cipher is to be generated.
Step 10. Continue step (1) to (10) for the next character of file until EOF is not encountered.

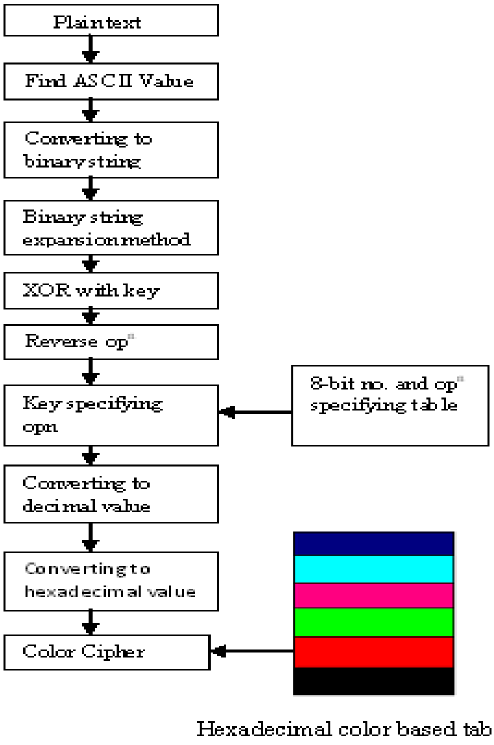

Plain text
Find ASCII Value
Converting to binary string
Binary string expansion method
XOR with key
Reverse op^n
Key specifying opn
8-bit no. and op^n specifying table
Converting to decimal value
Converting to hexadecimal value
Color Cipher
Hexadecimal color based table

Fig1: Flow Chart of color based Encryption technique

III. DECRYPTION ALGORITHM

Step 1. Scan the first color from the color cipher and get the corresponding hexadecimal value.
Step 2. Convert the hexadecimal value into decimal equivalent number.
Step 3. Corresponding binary value is evaluated.
Step 4. On the nature of key, an 8-bit specific number and specified reverse operation is chosen from a key specific look-up table and perform that specified reverse operation on the binary string with that number.
Step 5. Now perform reverse operation on binary string.
Step 6. Perform XOR operation on binary string with 16-bit specific key k.
Step 7. Apply binary string reduction method by truncating 4-bit from front and rear end of string.
Step 8. Corresponding decimal value is calculated.
Step 9.The ASCII character corresponding to it is determined i.e. plain text.
Step 10. Repeat the step (1) to (9) till the EOF.

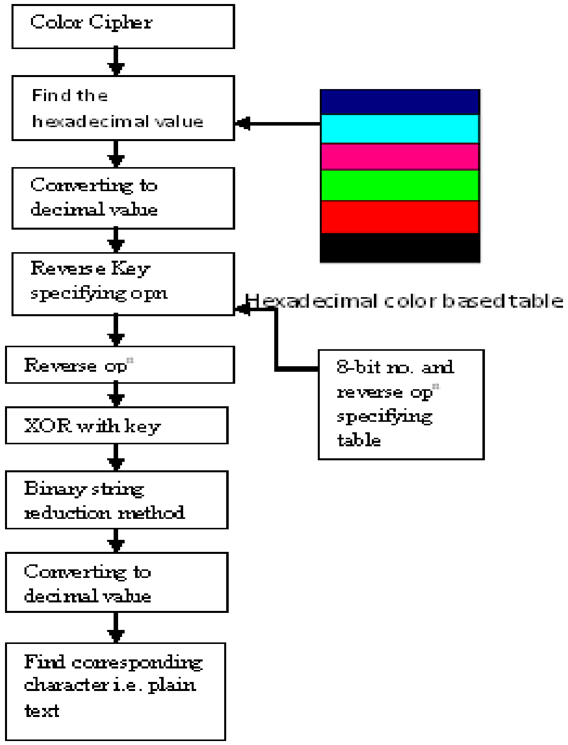

Color Cipher
Find the hexadecimal value
Converting to decimal value
Reverse Key specifying opn
Reverse opn
XOR with key
Binary string reduction method
Converting to decimal value
Find corresponding character i.e. plain text
Hexadecimal color based table
8-bit no. and reverse opn specifying table

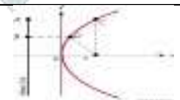
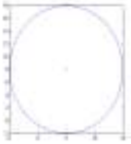
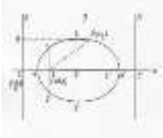
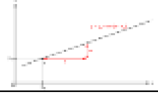
Fig 2: Flow Chart of color based Decryption technique

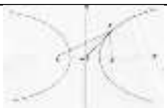
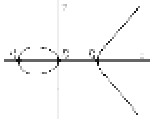
IV. KEY DISTRIBUTION TECHNIQUE

In secret key cryptography, a single key is used by both parties. So, it is obvious that the secret key must be known to both the sender and the receiver. But the cumbersome problem with this approach is key distribution through a highly unsecured channel. Here we have introduced a new key distribution system which is based on geometrical co-ordinate system in which sender and receiver will generate a key k by using the following procedure as:

- Sender will generate a coordinate point (X_1, Y_1) and similarly receiver (X_2, Y_2), then both exchange between them.
- Now both sender and receiver familiar with (X_1, Y_1) and (X_2, Y_2). From this we calculate m, where m = $\lceil(|Y_2-Y_1|/|X_2-X_1|)\rceil$.
- Then we can calculate g, where g = $\lceil(m^{X1* Y2} + m^{X2* Y1})\rceil$.
- On the nature of m, we can randomly choose a geometric image from a pre-defined geometric image table , i.e. Table 1.
- Generate functional equation corresponding to image and calculate p, where p = $|f(X_2, Y_2)|$.
- Finally, generate 16-bit key as k = (p(specified operation)g)mod65536.

Table 1: Geometrical Image Table

Nature of "m"	Geometric Images
m ϵ prime no. & m ϵ (1, 1000)	
m ϵ non-prime no. & m ϵ (above 65536)	
m ϵ prime no. & m ϵ (1000, 9999)	
m ϵ non-prime no. & m ϵ (1, 1000)	

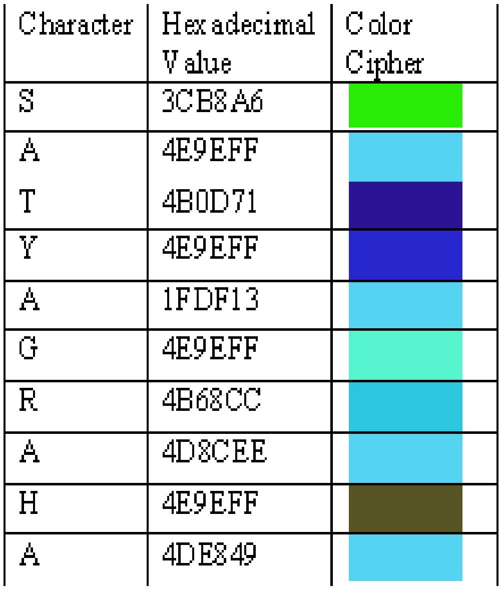
m ϵ non-prime no. & m ϵ (1000, 65536)	
m ϵ prime no. & m ϵ (above 9999)	

V. CASE STUDIES

Let we encrypt the character ‘S’ from the text file having content “SATYAGRAHA”. So first, we generate the 16-bit secret key by following procedure as:
Sender and receiver generates (19, 37) and (27, 51) coordinates points, and exchange between them.
Then sender calculates m = 1.75, and g = 59871413.
On the nature of m, sender choose a line image from a pre-defined table and get their corresponding equation i.e. f(X, Y) = Y – X + 1.
Finally, sender will generate k = 31387 by performing k = (15*59871413)mod65536.

For Encryption

Step 3. Apply the algorithm on first character of the file having the content “SATYAGRAHA” i.e. “S”, ASCII value of “Y” is 83.
Step 4. Corresponding 8-bit binary string is 01010011.
Step 5. Generate 16-bit binary string by applying expansion method as 0011010100110101.
Step 6. Perform XOR operation on resultant string of step (5) with the key (k = 31387) i.e. 0100111110101110.
Step 7. Reversing the binary string i.e. 0111010111110010.
Step 8. Perform a specified operation (multiplication here) with a specific number (91 here) i.e. 1010011110110100000110.
Step 9. Corresponding decimal value is 2747654.
Step 10. Now convert the 2747654 into hexadecimal value i.e. 29ED06.
Step 11. Finally the color corresponding to the character “S” is “🟩”. That is our secure color cipher.
Similarly other character will be treated and the resultant color cipher of “SATYAGRAHA” will be



Character	Hexadecimal Value	Color Cipher
S	3CB8A6	🟩
A	4E9EFF	🟦
T	4B0D71	🟪
Y	4E9EFF	🟦
A	1FDF13	🟦
G	4E9EFF	🟩
R	4B68CC	🟦
A	4D8CEE	🟦
H	4E9EFF	🟫
A	4DE849	🟦

Color Cipher of “***SATYAGRAHA***”

Fig 3: Encrypted Plain Text

VI. SECURE AND RELIABLE PATH SELECTION BASED POLICY ROUTING

In today’s networking environment, ISPs play a crucial role in keeping the Internet well-connected and stable, as well as providing network services that meet the needs of other networks. All the services offered by ISPs fundamentally rely on routing, the process of discovering paths in a network along which to send traffic to reach other destinations. Managing routing through some policies is essential in ISPs’ to achieve high performance. By configuring many routers in its network, an ISP implements policy that reflect its business relationships with neighboring networks, and adjusts routing protocols to select paths with desirable properties. In spite of its obvious importance, today’s ISP routing management practices follows policy based routing which are surprisingly primitive. For example, even though different networks today may have very different preferences for the kinds of paths they would like to use (e.g., a financial institution may prefer the most secure and reliable paths that do not traverse any untrusted networks, whereas a provider of video conferencing, live information broadcasting or voiceover-IP service may prefer paths with the lowest latency and fast data transmission while an advertising agency prefer path having low cost or normal data transmission), today's ISPs simply are not capable of providing such customized routing services a router is only allowed to select a single best path and only that path may be offered to its neighbors. By using secure and reliable path selection based policy, customer can implement a policy on a BGP decision router which defines certain rules and parameters corresponding to different characteristic path selection mechanism. When BGP routers receive a packet, it can check the nature of packet against the policy. If it matches, then secure and reliable path selection based policy determine which path to follow rather than pre-defined path.

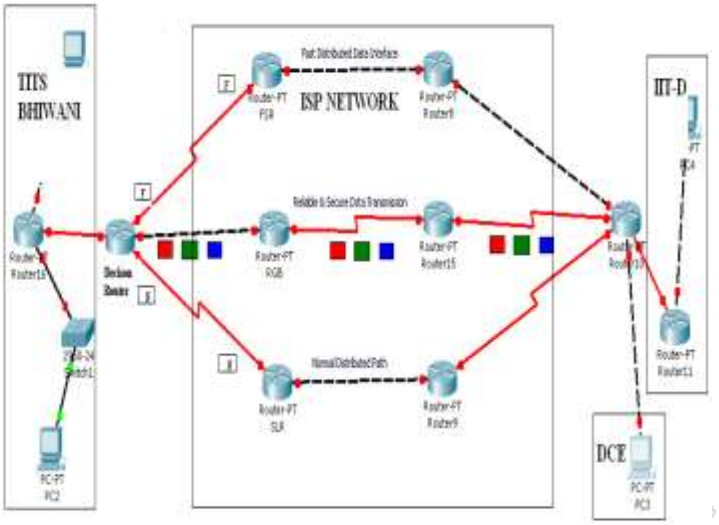


Fig 4: Secure and reliable path selection based policy System

In above ISP network, we have implemented a secure color based encryption and decryption algorithm on BGP decision router and router-10 to meet the importance of electronic security to the information that is sent over highly vulnerable and untrusted electronic communication media. Beside this, we have also imposed a secure and reliable path selection based policy on BGP decision router with the help of network simulator packet tracer which will provide the path on the nature or priority of incoming packet that violates the traditional path vector routing. Now if we need to have a secure and reliable data transmission or packet comes from IP address class 2, then BGP will provide a secure and reliable path to that packet. Also if nature of traffic demands fast transmission or comes from IP address class 1, then it will follow the fast distributed data interface path. Finally, normal distributed path will be available for slow transmission; low priority and IP address class 3 packets. So, this new introduced policy will be helpful to enhance the network performance and to meet the customized routing services. In this, we have discussed about three traffic classes which are categorized as:

Class 1: Traffic that demands services like video-conferencing, client meetings, live support etc.
Class 2: Traffic that demands services like secure transaction with the client will be categorized in this class except video-conferencing.
Class 3: This class mainly supports extranet services for the unauthorized clients.

VII. ROUTER CONFIGURATION

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z
Router(config)#interface fa 0/0
Router(config-if)#ip address 192.168.122.2 255.255.255.0
Router(config-if)#description line Fast Distributed Data Interface Line
Router(config-if)#no shut
LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#interface s 0/1
Router(config-if)#ip address 192.168.124.5 255.255.255.0
Router(config-if)#clockrate 500000
Router(config-if)#description line Reliable and secure data transmission Line
Router(config-if)#no shut
LINK-6-CHANGED: Interface serial 0/1, changed state to up
Router(config-if)#exit
Router(config)#interface s 0/0
Router(config-if)#ip address 192.168.128.3 255.255.255.0
Router(config-if)#description line Normal Destributed Path
Router(config-if)#no shut
LINK-7-CHANGED: Interface serial 0/0, changed state to up
Router(config-if)#exit
Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ?
  log Log matches against this entry
```

```
   <cr>
Router(config)#route-map PBR permit 10
Router(config-route-map)#match ip address 1
Router(config-route-map)#match fastEthernet
Router(config-route-map)#set interface fa 0/0
Router(config-route-map)#end
Router# show route-map
route-map PBR, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
    fastEthernet
  Set clauses:
    interface fa 0/0
Router(config)#route-map PBR permit 10
Router(config-route-map)#match ip address 2
Router(config-route-map)#match RelialeSecure
Router(config-route-map)#set interface S 0/1
Router(config-route-map)#end
Router# show route-map
route-map PBR, permit, sequence 10
  Match clauses:
    ip address (access-lists): 2
   RelialeSecure
  Set clauses:
    interface S 0/1
Router(config)#route-map PBR permit 10
Router(config-route-map)#match ip address 3
Router(config-route-map)#match NormalPath
Router(config-route-map)#set interface S 0/0
Router(config-route-map)#end
Router# show route-map
route-map PBR, permit, sequence 10
  Match clauses:
    ip address (access-lists): 2
   NormalPath
  Set clauses:
    interface S 0/0
```

VIII. CONCLUSION

The paper has demonstrated a color based symmetric encryption algorithm which is more secure as compared to existing ones and to the best of our concern it would be difficult to intruders for cryptanalysis. Morever, we have also implemented this newer approach on secure and reliable policy based routing which will provide different characteristics path on the basis of nature, priority, type of service (ToS) or defined class of incoming packet. The main emphasis of this policy is to provide a secure and reliable path, and that will be provided by applying the encryption and decryption techniques on BGP routers and also by configuring them. So, this new introduced policy will be helpful to enhance the security, network performance by partitioning the single link load into three link, and also helpful to meet the customized routing services by providing the required services to the customers. And the proposed direction for the future work would be to analyze the following factors:

1. Hardware implementation of this algorithm using VLSI techniques on BGP router.
2. Compression technique could be implemented along with encryption procedure to achieve high performance in terms of security and bandwidth utilization.
3. Introduce time and location dependent encoded look-up tables.
4. Performance analysis of this one with existing ones in terms of throughput, memory requirement, power consumption and security towards intruders.
5. Introduce the enhanced one or more complex policy in network traffic like ISP.
6. Introduce modified form of this one which can be efficiently used in small devices.

REFERENCES

[1] P.Gope, "Multi Operator Delimiter based Data Encryption Standard (MODDES)", ICCNT 2009.

[2] P.Gope ,"A comparative study of performance based crypto analysis features for standard Data Encryption Algorithms with (MODDES)", ICCNT 2009.

[3] Twenty Second National Radio Science Conference (NRSC 2005), RDEA Algorithm.

[4] Daemen, Jjmen, V.: "AES Proposal: Rijndael", Banksys/Katholieke, R Universiteit Leuven, Belgium, AES submission, June 1998.

[5] W.Stallings "Cryptography and network security principles and practice," Fourth edition, Prentice hall, 2007.

[6] Computer Networks by Andrew S. Tanenbaum, Fourth Edition, Prentice hall, 2004.
[7] P.Gope,” Extended Multi Operator Delimiter Based Data Encryption Standard(X-MODDES),” ICFN, 2010, China.
[8] P. Gope, A. Singh, “An Efficient Cryptograpic Approach for Secure Policy Based Routing”, ICNCS, 2011, Kanyakumari, India.
[9] A. Singh “An Improved Two-factor Authenticated Key exchange Protocol in Public Wireless LANs”, IEEE Xplore Digital Library, ACCT2012, India.
[10] A. Singh “A Novel Approach towards Mutual Authentication and Key Exchange Protocol based on Elliptic Curve”, IEEE Xplore Digital Library, ACCT2012, India.
[11] http://www.cisco.com.
[12] http://thepackettracer.blogspot.com.
[13] http://watchguard.com/.../policy_based_routiro ro_configure_f.html.
[14] D. R. Stinson, “Cryptography Theory and Practice”, CRC Press, Inc., 2002.
[15] E. Crawley et. al. “A framework for QoS based Routing in the Internet”, RFC 2386, Aug 1998.