International Journal of Engineering, Science and Mathematics
Vol. 7Issue 1, January 2018,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Kursa Short Message Encryption Technique

Dr.A.Vijay Kumar*
Mr.K.Srininvas**

Abstract (10pt)

In the present paper we made an effort to propose a short message encryption technique named KURSA. The present encryption technique can be used successfully for the encryption of very short messages as well as secret keys. We believe the present encryption technique will be very useful for secure secret key distribution because the technique adapted is very strange. Data is protected against known cipher text, plain text and brute force attacks. Data is in safe hands till the secret key taken is unknown.

Keywords:
Plaintext,
Cipher text,
Encryption,
Decryption
Secret Key.

Author correspondence:

Dr.A.Vijay Kumar,
Ph.D(CSE)
Professor and HOD of MCA,Sree Chaintanya College of Engineering, Karimnagar,Affiliated to JNTUH

1. Introduction

Providing security to the information is enforced in now-a-days, so every care should be taken to protect the information. Here we are proposing a **block cipher technique** called KURSA. The word kursa is a Telugu language word, kursa means very short. The present encryption technique can be used for success full encryption of the very short and sensitive information or secret keys. The encryption technique is robust against known plain text, cipher text and brute force attacks because length of the plain text is very short, so there will be less scope for experimenting on it. The secret key which is used in the encryption and decryption process should be exchanged via a secure communication channel or it should be send to the receiver after encrypting it with public key encryption technique. The encryption technique strength is based on the secrecy of the secret key.

[*] Dr.A.Vijay Kumar, Ph.D(CSE), Professor and HOD(MCA) , Sree Chaitanya College of Enineering.JNTUH.
[**] Mr.K.Srinivas,BE,ME, Associate Professor and HOD(CSE), Sree Chaitanya College of Enineering.JNTUH.

2. Encryption Algorithm

Step 1: Divide the plain text into blocks of 5 letters.
Step 2: Convert the plain text block into cipher text block as follows.
Ci = (Pi + Ki) mod 26 *for all* 0<= i <=4 ---- (1)
Where

Ci	i th cipher text letter
Pi	i th plain text letter
Ki	i th keyword letter

Step 3: Perform a left circular shift on the key to get the key for the next block.
Step 4: Repeat step 2 and 3 till entire blocks of the plaintext is converted into cipher text.

3. Decryption Algorithm

Step 1: Divide the cipher text into blocks of 5 letters.
Step 2: Convert the cipher text block into plain text block as follows.
Pi = (Ci - Ki) mod 26 *for all* 0<=i<=4 --- (2)
where

Ci	i th cipher text letter
Pi	i th plain text letter
Ki	i th keyword letter

Step 3: Perform a left circular shift on the key to get the key for the next block.
Step 4: Repeat step 2 and 3 till entire blocks of the plaintext is converted into cipher text.

4. Encryption Process

The encryption algorithm is a block cipher technique in which each time it converts 5 successive letters of the plaintext into cipher text using a keyword. The plain text and cipher text's are strings or phrases in English. The letters of the English alphabet *a to z* are used for preparing the keyword. Assume, each letter in the alphabet is assigned a numerical value starting from zero such that a=0, b=1, c=2 ... z=25 and the letters are arranged in a circular passion. In the first step the original message will be divided into blocks of 5 letters then in the second step the individual blocks will be converted into cipher text in a sequential order. At the recipient end the receiver should use the decryption algorithm which takes same key for re conversion of cipher text into plain text.

For example consider the plaintext, prepareforthewar and key aeiou . The original text now will be divided into four blocks, prepa-refor-thewa-r and this blocks will be converted into cipher text blocks, pvmdu-vmtir-bvywe-f. The process involved in the encryption of the message prepareforthewar is illustrated below.

First Block	prepa
Keyword	aeiou

C 0 = (P0 + K0) mod 26 = (15+0)mod 26 =15 mod 26 = 15 =p
C 1 = (P1 + K1) mod 26 = (17+4)mod 26 =21 mod 26 = 21 =v
C 2 = (P2 + K2) mod 26 = (4+8)mod 26 =12 mod 26 = 12 =m
C 3 = (P3 + K3) mod 26 = (15+14)mod 26 =29 mod 26 = 3 =d
C 4 = (P4 + K4) mod 26 = (0+20)mod 26 =20 mod 26 = 20 =u

Second Block	refor
Keyword	eioua

C 0 = (P0 + K0) mod 26 = (17+4)mod 26 =21 mod 26 =21 =v
C 1 = (P1 + K1) mod 26 = (4+8)mod 26 =12 mod 26 = 12 =m
C 2 = (P2 + K2) mod 26 = (5+14)mod 26 =19 mod 26 = 19 =t
C 3 = (P3 + K3) mod 26 = (14+20)mod 26 =34 mod 26 = 8 =i
C 4 = (P4 + K4) mod 26 = (17+0)mod 26 =17 mod 26 = 17 =r

Third Block thewa
Keyword iouae

C 0 = (P0 + K0) mod 26 = (19+8)mod 26 =27 mod 26 = 1 =b
C 1 = (P1 + K1) mod 26 = (7+14)mod 26 =21 mod 26 = 21 =v
C 2 = (P2 + K2) mod 26 = (4+20)mod 26 =24 mod 26 = 24 =y
C 3 = (P3 + K3) mod 26 = (22+0)mod 26 =22 mod 26 = 22 =w
C 4 = (P4 + K4) mod 26 = (0+4)mod 26 =4 mod 26 = 4 =e

Forth Block r
Keyword ouaei

C0 = (P0 + K0) mod 26 = (17+14)mod 26 =31 mod 26 = 5 =f

5. Decryption Process

Decryption algorithm takes the cipher text as input and converts it into plaintext using a keyword. Decryption process is opposite to the encryption process where plaintext blocks were converted into cipher text here the cipher text blocks will be converted into plaintext using the same 5 letter keyword. The decryption logic is very simple; the cipher text letter's numeric value needs to be subtracted from the keyword letter's numeric value. And over the result mod 26 should be performed in a sequence one after another using the following linear equation 2.

For example consider the cipher text in the above example pvmduvmtirbvywef which will be divided into four blocks as, pvmdu- vmtir-bvywe-f and these four blocks will be converted into plaintext prepareforthewar using the same key aeiou. The entire process involved in the decryption of the cipher text is illustrated as follows.

First Block pvmdu
Keyword aeiou

P 0 = (C0 - K0) mod 26 = (15 - 0) mod 26 = 15=p
P 1 = (C1 - K1) mod 26 = (21 - 4) mod 26 = 17=r
P 2 = (C2 - K2) mod 26 = (12 - 8) mod 26 = 4 =e
P 3 = (C3 - K3) mod 26 = (3 - 14) mod 26 = -11 mod 26=15=p
P 4 = (C4 - K4) mod 26 = (20 -20) mod 26 = 0=a

Perform left circular shift for one character on the keyword aeiou then it becomes eioua, use it as keyword for second block processing.

Second Block vmtir
Keyword eioua

P 0 = (C0 - K0) mod 26 = (21 - 4) mod 26 = 17=r P 1 = (C1 - K1) mod 26 = (12 - 8) mod 26 = 4=e
P 2 = (C2 - K2) mod 26 = (19 - 14) mod 26 = 5 mod 26 =5=f
P 3 = (C3 - K3) mod 26 = (8 - 20) mod 26 = -12 mod 26=14=o

P 4 = (C4 - K4) mod 26 = (17 -0) mod 26 = 17=r

Perform left circular shift for one character on the keyword eioua then it becomes iouae use it as keyword for third block processing.

Third Block	bvywe
Keyword	iouae

P 0 = (C0 - K0) mod 26 = (1 - 8) mod 26 = -7mod26=19=t
P 1 = (C1 - K1) mod 26 = (21 -14) mod 26 = 7=h
P 2 = (C2 - K2) mod 26 = (24 - 20) mod 26 =4 mod 26 =4=e
P 3 = (C3 - K3) mod 26 = (22 - 0) mod 26 =22 mod 26=22=w
P 4 = (C4 - K4) mod 26 = (4 -4) mod 26 = 0=a

Perform left circular shift for one character on the keyword iouae then it becomes ouaei use it as key for forth block processing.

Fourth Block	f
keyword	ouaei

P 0 = (C0 - K0) mod 26 = (5 -14) mod 26 = -9mod26=17=r

Plaintext:	prepareforthewar
Ciphertext:	pvmduvmtirbvywef

6. Implementation

The Kursa block cipher technique is implemented in C language. The method **void encrypt(char p[], char k[] , char c[])** is used for encryption of the key and **void decrypt(char c[] , char k[] , char p[])** is used for the decryption of the cipher text into plain text. The character arrays p,c and k are used for storing plain text, cipher text and secret key. To the encryption function we have to pass 3 character array parameters, p, k and c, in which first two p and k are input parameters used to pass plain text and secret key, and third one is output parameter used to store cipher text.

The method **void getblock(char s[] , char block[] , int i)** is used to get a fresh block from the plain text or cipher text. The character array **s** and **block** are used to store plain text and present block. The integer variable i represents the block number. A **void rotate (char k[])** is used to perform left rotation on the key to get the key for the next block. The functions **void encrypt_b(char p[] , char k[] , char c[])** and **void decrypt_b(char c[] , char k[] , char p[])** are used to encrypt and decrypt the individual blocks of the plain text and cipher text.

```
void encrypt(char p[], char k[] , char c[])
{
  char key[5] ,b[5] ;
  int i ;
  int len = strlen(p) ;

  strcpy(key,k) ;
  for(i=0 ; i< len/5 + 1 ; i++)
  {
    getblock( p , b , i) ;
    encrypt_b(b,key,c+i*5) ;
    rotate(key) ;
  }
  c[len] = '\0' ;
}

void decrypt(char c[] , char k[] , char p[])
{
  char key[5] , b[5] ;
  int i ;
  int len = strlen(c) ;
  strcpy(key,k) ;
  for(i=0 ; i< len/5 + 1 ; i++)
  {
    getblock( c , b , i) ;
    decrypt_b(b,key,p+i*5) ;
    rotate(key) ;
  }
  p[len] = '\0' ;
}

void getblock(char s[] , char block[] , int i)
{

  int j = i*5 , k ;

  for(k=j ; k<j+5 && s[k] != '\0'; k++)
    block[k-j] = s[k] ;
  block[k-j] = '\0' ;
}

void encrypt_b(char p[] , char k[] , char c[])
{
  int i ;

  for(i=0 ; i<5 && p[i] != '\0' ; i++)
    c[i] = ((p[i]+k[i]-194)%26) + 97 ;
}

void decrypt_b(char c[] , char k[] , char p[])
{
  int i ;

  for(i=0 ; i<5 && c[i] != '\0' ; i++)
    p[i] = ((c[i]-k[i]+26)%26) + 97 ;
}

void rotate(char k[])
{
  char first = k[0] ;
  int i;
  for(i=0 ; i<4 ; i++)
    k[i] = k[i+1] ;
  k[i] = first ;
}
```

7. Strength and weakness

The data encrypted with the kursa encryption algorithm is highly confidential because it is safe against known cipher text, plain text and brute force attacks. The procedure we have adapted for the encryption and decryption of the messages is unique and for each letter of the plaintext and cipher text we are using a different key letter. If there are no repeated letters in the plain text the encryption algorithm will be extremely stronger. If the letters in the plain text are repeated there may be a bit of chance to identify the secret key.

8. Conclusion

Data is secure till the secret key is confidential. So, every precaution should be taken to protect the secret key. The secret key should be given to the receiver through secure communication channel and in the cipher text form so that unauthorized persons do not get the secret key. The encryption technique is suitable for exchanging the secret keys and very short messages.

References

[1]. Ari Juels is a professor at Cornell Tech, Thomas Ristenpart Univ. of Wisconsin, Madison, WI, USA, Honey Encryption: Encryption beyond the Brute-Force Barrier, IEEE Security & Privacy (Volume: 12, Issue: 4, July-Aug. 2014), Page(s): 59 – 62**,** Print ISSN: 1540-7993.

[2]. Abhishek Bhardwaj; Subhranil Som, Study of different cryptographic technique and challenges in future 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 Pages: 208 – 212, IEEE Conference Publications.

[3]. Dania Qara Bala; Soumyadev Maity; Sanjay Kumar Jena, Mutual authentication for IoT smart environment using certificate-less public key cryptography, Third International Conference on Sensing, Signal Processing and Security (ICSSS), 2017, Pages: 29 – 34, IEEE Conference Publications.

[4]. Jaewon Noh; Jeehyeong Kim; Giwon Kwon; Sunghyun Cho, Secure key exchange scheme for WPA/WPA2-PSK using public key cryptography, 2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), 2016 , Pages: 1 - 4, IEEE Conference Publications.

[5]. Jeffrey H. Shapiro, Quantum illumination: From enhanced target detection to Gbps quantum key distribution, 2017 Conference on Lasers and Electro-Optics (CLEO), Pages: 1 – 1, IEEE Conference Publications.

[6]. N. Venkatadri; K. Ramesh Reddy, Secure TORA: Removal of Black Hole Attack Using Twofish Algorithm, 2016 IEEE 6th International Conference on Advanced Computing (IACC), Pages: 239 – 244, IEEE Conference Publications.

[7]. Tapan Kumar Hazra; Anisha Mahato; Arghyadeep Mandal; Ajoy Kumar Chakraborty, A hybrid cryptosystem of image and text files using blowfish and Diffie-Hellman techniques, 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), Pages: 137 – 141, IEEE Conference Publications.

[8]. Vaibhav Poonia; Narendra Singh Yadav, Analysis of modified Blowfish algorithm in different cases with various parameters, 2015 International Conference on Advanced Computing and Communication Systems 2015, Pages: 1 – 5, IEEE Conference Publications.

[9]. V. C. Dongre; S. G. Shikalpure,Ensuring privacy preservation in wireless networks against traffic analysis by employing network coding and Blowfish encryption, 2016 International Conference on Signal and Information Processing (IConSIP), 2016, Pages: 1 – 5, IEEE Conference Publications.

[10]. Zhou Yingbing; Li Yongzhen, The design and implementation of a symmetric encryption algorithm based on DES, 2014 IEEE 5th International Conference on Software Engineering and Service Science , 2014,Pages: 517 - 520 , IEEE Conference Publications.