MBNA Publishing House Constanta 2026

Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

Automatic Polybios Encryption and Decryption

To cite this article: Vasiliu Paul, Deliu Florenţiu, Pazara Tiberiu, Proceedings of the International Scientific Conference SEA-CONF 2026, pg. 8-13.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-26-001

SEA-CONF© 2025. This work is licensed under the CC BY-NC-SA 4.0 License

Automatic Polybios encryption and decryption

Paul Vasiliu[1], Florenţiu Deliu[2], Tiberiu Pazara[3]

[1,2,3] "Mircea cel Bătrân" Naval Academy, Constanţa, România

E-mail: [1] paul.vasiliu@anmb.ro, [2] florentiu.deliu@anmb.ro ,[3] tiberiu.pazara@anmb.ro

Abstract. In this paper, Matlab implementation of the Polybios encryption system is presented. An example of encoding/decoding solved manually and automatically using the proposed Matlab implementation is presented.

Keywords: affine**,** encryption, system

1. Polybios encryption system

The Polybios encryption system was originally a maritime torch signaling system. It was later given a cryptographic meaning. The Polybios system was used for centuries, being considered one of the most secure encryption systems. This system was used in Russian prisons, and later by American prisoners in Vietnam.

The alphabet used by Polybios is the set of all uppercase letters of the alphabet. In this paper, we have extended this alphabet. We have considered that the alphabet over which messages are defined is the set of all uppercase and lowercase letters, the digits of the decimal number system, the space separator and comma:

$$\mathcal{M} = \{A\ B\ \cdots Z\ 0\ 1\ \cdots\ 9\ a\ b\ \cdots\ z\ _\ ,\} \quad (1)$$

Obvious $card(\mathcal{M}) = 64 = 8^2$. This set can be expanded by adding other characters to the alphabet.

The alphabet $\mathcal{M}$ is put in one-to-one correspondence with a square matrix C with 8 rows and 8 columns. The elements of the matrix C are the elements of the alphabet written in the order of their appearance in the alphabet. The rows and columns can be numbered with any distinct elements from the set $\mathcal{M}$. Let be $c_i \in \mathcal{M}, i = 1,2,\cdots,8$ with the property $c_i \neq c_j$ for $i \neq j$. The elements $c_i \in \mathcal{M}, i = 1,2,\cdots,8$ are called coordinates. Each character in the matrix C from line i and column j is well defined by the coordinate pair (c_i, c_j). For example, the character g is defined by the coordinate pair (c_6, c_3).

Coordinate vector:

$$k = (c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7\ c_8)\ c_i \in \mathcal{M},\ i = 1,2,\cdots,8, c_i \neq c_j\ \forall\ i \neq j \quad (2)$$

it is called encryption / decryption key. Thus the set of keys for the Polybios encryption system is:

$$K = \{k = (c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7\ c_8) \mid c_i \in \mathcal{M},\ i = 1,2,\cdots,8, c_i \neq c_j\ \forall\ i \neq j\} \quad (3)$$

Each character c will be encrypted by the pair $c_{linie}c_{coloană}$. For example, the character R will be encrypted with the pair (c_3, c_2).

Decryption involves dividing the message to be decrypted into blocks of two characters and determining the character corresponding to that block.

The Polybios encryption system is a monoalphabetic substitution.

There are various variants of the Polybios system. The system can be applied using various symbols as coordinates (numbers, points, figures, acoustic signals, lights, etc.).the sets of plaintexts.

Table 1. Alphabet character table $\mathcal{M}$ (C matrix) and the key k

	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8
c_1	A	B	C	D	E	F	G	H
c_2	I	J	K	L	M	N	O	P
c_3	Q	R	S	T	U	V	W	X
c_4	Y	Z	0	1	2	3	4	5
c_5	6	7	8	9	a	b	c	d
c_6	e	f	g	h	i	j	k	l
c_7	m	n	o	p	q	r	s	t
c_8	u	v	w	x	y	z		,

Let $a = a_1 a_2 \cdots a_n,\ a_p \in \mathcal{M},\ p = 1,2,\dots,n,$ be the message to be encoded. To encode the message, each character a_p is searched in the character table and the line c_i and column c_j on which this element is found are determined. The character a_p is encoded with the characters $c_i c_j$. For decoding, the character on line c_i and column c_j is searched in the character table. Let this character be a_p. Thus, the characters $c_i c_j$ are decoded with the character a_p.

2. Example 1

We consider the keyword May,0514 of length $p = 8$.

We will encrypt the message Sea Conf 2026 using the key k =(May,0514) of length 8.

Table 2. Alphabet character table $\mathcal{M}$ (C matrix) key k = (May,0514)

	M	a	y	,	0	5	1	4
M	A	B	C	D	E	F	G	H
a	I	J	K	L	M	N	O	P
y	Q	R	S	T	U	V	W	X
,	Y	Z	0	1	2	3	4	5
0	6	7	8	9	a	b	c	d
5	e	f	g	h	i	j	k	l
1	m	n	o	p	q	r	s	t
4	u	v	w	x	y	z		,

Table 3. Message encoding

S	e	a		C	o	n	f		2	0	2	6
yy	5M	00	41	My	1y	1a	5a	41	,0	,y	,0	0M

Thus, the character string yy5M0041My1y1a5a41,0,y,00M encodes the message Sea Conf 2026 using the key (May,0514).

For decoding, the character table is used and the decoding table is created:

Table 4. Message decoding

yy	5M	00	41	My	1y	1a	5a	41	,0	,y	,0	0M
S	e	a		C	o	n	f		2	0	2	6

The result of decoding the message yy5M0041My1y1a5a41,0,y,00M with the key Mai,0514 is the message: Sea Conf 2026.

3. Automatic Polybios encryption and decryption

For automatic encryption and decryption, the author wrote a program in Matlab. The program has the following functions:

The function with the signature function polybios(key,pt) is the main function.

The function has the input arguments: key string containing the key for encryption/decryption, pt string containing the plaintext to be encrypted and then decrypted. The function performs encryption and decryption of the plaintext mess using the key key using the Polybios encryption system.

The function with signature function c=genmatcar(key)

The function has the input argument: key string of characters containing the key for encryption / decryption. The function has the output argument: c the character array. The function generates the matrix c.

The function with the signature function write(c)

The function has the input argument: c is the character array. The function display c matrix.

The function with the signature function ct=polybioscod(c,key,pt)

The function has the input arguments: c is the character array, key is the encryption/decryption key, pt the message in plain text to be encoded. The function has the output argument: ct the coded message. The function encodes the pt message.

The function with the signature function dt=polybiosdecod(c,key,ct)

The function has the input arguments: c is the character array, key is the encryption/decryption key, ct the coded message. The function has the output argument: dt the decoded message. The function decodes the message ct.

The function with the signature function i=index(c,key)

The function has the input arguments: c is the character array, key is the encryption/decryption key. The function has the output argument: i the index of character c in key.

The source program is written in the appendix of the paper.

4. Running example

To run the program, we used the data from example 1.

```
>> key='May,0514'
key =
May,0514
>> pt='Sea Conf 2026'
pt =
Sea Conf 2026
>> polybios_E(key,pt)
The encoding/decoding key is: May,0514
Character matrix:
     M  a  y  ,  0  5  1  4
 M   A  B  C  D  E  F  G  H
 a   I  J  K  L  M  N  O  P
 y   Q  R  S  T  U  V  W  X
 ,   Y  Z  0  1  2  3  4  5
 0   6  7  8  9  a  b  c  d
 5   e  f  g  h  i  j  k  l
 1   m  n  o  p  q  r  s  t
 4   u  v  w  x  y  z     ,
The result of encoding with the key May,0514 is:
yy5M0041My1y1a5a41,0,y,00M
The result of decoding with the key May,0514 is:
Sea Conf 2026
```

>>

5. Conclusions and further developments

In this work, the author generalized the Vigenere encryption system by extending the alphabet over which the messages are defined. The author wrote a Matlab program that performs the encryption and decryption operations of the messages defined on this extension. The examples presented prove the correctness of the algorithm implementation and the correctness of the results generated by the program. In the future, the author will extend the alphabet and develop the program by adding punctuation characters and other separators.

Author contributions:

- Conceptualization: P.V., F.D. and P.T.
- Writing original draft: P.V.
- Writing review and editing: P.V.
- Supervision: F.D. and P.T.

Funding: This research received no external funding.
Conflict of interest: The Author declare no Conflict of interest.

Appendix
In this section we will present the Matlab function codes written by the author of the paper.

```
% Polybios encryption/decryption system
% Main function
% key is the encryption/decryption key
% pt the message in plain text to be encoded
function polybios(key,pt)
if length(key) == 8 mesaj=['The encoding/decoding key is: ',key]; disp(mesaj);
c=genmatchar(key); write(c);
ct=polybioscod(c,key,pt);
mesaj=['The result of encoding with the key ',key,' is:']; disp(mesaj); disp(ct);
dt=polybiosdecod(c,key,ct);
mesaj=['The result of decoding with the key ',key,' is:']; disp(mesaj); disp(dt);
else mesaj=['The key is not 8 characters long. ']; disp(mesaj); end end
% Function for generating the character matrix
% key is the encryption/decryption key
% c is the character array
function c=genmatchar(key)
for j=2:9 c(1,j)=key(j-1); end
for i=2:9 c(i,1)=key(i-1); end
for i=2:9
   for j=2:9
      if i*3+j<=34
      c(i,j)=char(65+(i-2)*8+(j-2));
      else
      c(i,j)=char(32);
      end
   end
end
k=48;
i=5;
```

```
for j=4:9
   c(i,j)=char(k);
   k=k+1;
end
i=6;
for j=2:5
   c(i,j)=char(k);
   k=k+1;
end
k=97;
for j=6:9
   c(i,j)=char(k);
   k=k+1;
end
for i=7:9
   for j=2:9
      c(i,j)=char(k);
      k=k+1;
      end
end
c(9,8)=' ';
c(9,9)=',';
end

% Function for displaying character array
% c is the character array
function write(c)
fprintf('Character matrix: \n');
for i=1:9
   for j=1:9
      fprintf(' %c ',c(i,j));
   end
   fprintf('\n');
end end
% Function for Polybios encoding
% c is the character array
% key is the encryption/decryption key
% pt the message in plain text to be encoded
% ct the coded message
function ct=polybioscod(c,key,pt)
[m n]=size(pt);
col=1;
for k=1:n
   for i=2:9
      for j=2:9
         if pt(k)==c(i,j)
            ct(col)=key(i-1);
            col=col+1;
            ct(col)=key(j-1);
            col=col+1;
         end
```

```
      end
   end
end
end

% Function for Polybios decoding
% c is the character array
% key is the encryption/decryption key
% ct the coded message
% dt the decoded message
function dt=polybiosdecod(c,key,ct)
[m n]=size(ct);
p=1;
k=1;
while k<=n
   i=index(ct(k),key); k=k+1;  j=index(ct(k),key); k=k+1; dt(p)=c(i+1,j+1); p=p+1;
end end

% Function for determining the index i
% c is the character array
% key is the encryption/decryption key
function i=index(c,key)
for i=1:8
   if c==key(i) break; end end end
```

References

1. Atanasiu, A. (2008). Securitatea informaţiei Vol. 1 (Criptografie), Editura Infodata, Cluj.
2. Konheim A.(2007). Computer Security and Cryptography, Wiley Interscience.
3. Vasiliu P. (2015). Programare în Matlab, Ed. ANMB, Constanţa.