*Zbornik radova Prirodno-matematičkog fakulteta-Univerzitet u Novom Sadu*
*knjiga 13 (1983)*
*Review of Research Faculty of Science-University of Novi Sad, Volume 13(1983)*

# ONE ELEMENT KEY CIPHER

*Mirko Stojaković*
*Matematički institut,*
*11000 Beograd, Knez Mihajlova 35, Jugoslavija*

**ABSTRACT**

From the 26-letter alphabet of the English language the letters x and z are dropped and replaced by the combination ks and cs. The remaining 24 letters are taken in some order as elements of the symmetric group $S_4$. An algorithm is described for changing the clear words (of a plain text) into the hidden ones. To make such a cipher only one letter as a key needs to be memorized (the group $S_4$ being automatically constructed starting with $S_1$). The encryption and decryption of this cipher is described and the measure of security of the cipher is given. A worked out example is also given.

1. Cryptography is usually not considered as a branch of the theory of formal languages. But there are many reasons to do so: There is a finite alphabet A and the set of "clear" words $w_1, w_2, \ldots$ over A is to be transformed into the set of "secret" words $u_1, u_2, \ldots$ (over the same alphabet A) by using some grammar g ("method of ciphering"). Usually the clear word w is transformed into the secret

---

*AMS Mathematics subject classification (1980): 94B99*

*Key words and phrases: Cipher, key, alphabet, symmetric group $S_4$, encryption, decryption, security measure, plain text, clear words, hidden words.*

word $u$ by replacing the letters of $w$ by the letters of $u$ starting with some key word $u$. This means that $u$ is some gramatical function of $w$ and of $u_o$:

$$u = f_g(w, u_o) \quad . \tag{1}$$

The key $u_o$ is, in fact, that part of the grammar $g$ which is "invertible" and which means that, given $u$, $u_o$ and $g$ one can reconstruct $w$

$$w = \phi_g(u, u_o) \tag{2}$$

2. We shall explain this by develloping an original group theoretic algorithm of ciphering in which the key is a letter $u_o$. As is always the case, and as it must be the case, deciphering is a very intricate job when the grammar $g$ and the key $u_o$ are unknown to the decoder.

3. We shall take the latin alphabet of 24 letters omitting the letters $x$ and $z$ which in the clear text have been previously replaced by the combinations "ks" and "cs" respectively.

4. In the symmetric group $S_4$ each element of the group is replaced by some letter out of our 24-letter alphabet A. We present here the table of composition of this group. This table can be automatically constructed by starting with $S_2$ or even with $S_1$ and therefore need not be memorized.

5. Let the clear word $w$ (we consider the sentence a word) be composed of the letters $a_1, a_2, a_3, \ldots$, let the key letter be $u_o$ and let the secret word $u$, corresponding to the word $w$, be composed of the letters $u_1, u_2, u_3, \ldots$ Then our ciphering grammar is given by the table

$$\begin{aligned} u_1 &= u_o a_1 \, , \\ u_2 &= u_1 a_2 \, , \\ u_3 &= u_2 a_3 \, , \\ &\cdots\cdots\cdots\cdots \\ &\cdots\cdots\cdots\cdots \end{aligned} \tag{3}$$

| | 1234 | 1243 | 1324 | 1342 | 1423 | 1432 | 2134 | 2143 | 2314 | 2341 | 2413 | 2431 | 3124 | 3142 | 3214 | 3241 | 3412 | 3421 | 4123 | 4132 | 4213 | 4231 | 4312 | 4321 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | A 1 | B 2 | C 3 | D 4 | E 5 | F 6 | G 7 | H 8 | I 9 | J10 | K11 | L12 | M13 | N14 | O15 | P16 | Q17 | R18 | S19 | T20 | U21 | V22 | W23 | Y24 |
| A 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| B 2 | 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 | 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 | 18 | 17 | 20 | 19 | 22 | 21 | 24 | 23 |
| C 3 | 3 | 5 | 1 | 6 | 2 | 4 | 9 | 11 | 7 | 12 | 8 | 10 | 15 | 17 | 13 | 18 | 14 | 16 | 21 | 23 | 19 | 24 | 20 | 22 |
| D 4 | 4 | 6 | 2 | 5 | 1 | 3 | 10 | 12 | 8 | 11 | 7 | 9 | 16 | 18 | 14 | 17 | 13 | 15 | 22 | 24 | 20 | 23 | 19 | 21 |
| E 5 | 5 | 3 | 6 | 1 | 4 | 2 | 11 | 9 | 12 | 7 | 10 | 8 | 17 | 15 | 18 | 13 | 16 | 14 | 23 | 21 | 24 | 19 | 22 | 20 |
| F 6 | 6 | 4 | 5 | 2 | 3 | 1 | 12 | 10 | 11 | 8 | 9 | 7 | 18 | 16 | 17 | 4 | 15 | 13 | 24 | 22 | 23 | 20 | 21 | 19 |
| G 7 | 7 | 8 | 13 | 14 | 19 | 20 | 1 | 2 | 15 | 16 | 21 | 22 | 3 | 4 | 9 | 10 | 23 | 24 | 5 | 6 | 11 | 12 | 17 | 18 |
| H 8 | 8 | 7 | 14 | 13 | 20 | 19 | 2 | 1 | 16 | 15 | 22 | 21 | 4 | 3 | 19 | 9 | 24 | 23 | 6 | 5 | 12 | 11 | 18 | 17 |
| I 9 | 9 | 11 | 15 | 17 | 21 | 23 | 3 | 5 | 13 | 18 | 19 | 24 | 1 | 6 | 7 | 12 | 20 | 22 | 2 | 4 | 8 | 10 | 14 | 16 |
| J10 | 10 | 12 | 16 | 18 | 22 | 24 | 4 | 6 | 14 | 17 | 20 | 23 | 2 | 5 | 8 | 11 | 19 | 21 | 1 | 3 | 7 | 9 | 13 | 15 |
| K11 | 11 | 9 | 17 | 15 | 23 | 21 | 5 | 3 | 18 | 13 | 24 | 19 | 6 | 1 | 12 | 7 | 22 | 20 | 4 | 2 | 10 | 8 | 16 | 14 |
| L12 | 12 | 10 | 18 | 16 | 24 | 22 | 6 | 4 | 17 | 14 | 23 | 20 | 5 | 2 | 11 | 8 | 21 | 19 | 3 | 1 | 9 | 7 | 15 | 13 |
| M13 | 13 | 19 | 7 | 20 | 8 | 14 | 15 | 21 | 1 | 22 | 2 | 16 | 9 | 23 | 2 | 24 | 4 | 10 | 11 | 17 | 5 | 18 | 6 | 12 |
| N14 | 14 | 20 | 8 | 19 | 7 | 13 | 16 | 22 | 2 | 21 | 1 | 15 | 10 | 24 | 4 | 23 | 3 | 9 | 12 | 18 | 6 | 17 | 5 | 11 |
| O15 | 15 | 21 | 9 | 23 | 11 | 17 | 13 | 19 | 3 | 24 | 5 | 18 | 7 | 20 | 1 | 22 | 6 | 12 | 8 | 14 | 2 | 16 | 4 | 10 |
| P16 | 16 | 22 | 10 | 24 | 12 | 18 | 14 | 20 | 4 | 23 | 6 | 17 | 8 | 19 | 2 | 21 | 5 | 11 | 7 | 13 | 1 | 15 | 3 | 9 |
| Q17 | 17 | 23 | 11 | 21 | 9 | 15 | 18 | 24 | 5 | 19 | 3 | 13 | 12 | 22 | 6 | 20 | 1 | 7 | 10 | 16 | 4 | 14 | 2 | 8 |
| R18 | 18 | 24 | 12 | 22 | 10 | 16 | 17 | 23 | 6 | 20 | 4 | 14 | 11 | 21 | 5 | 19 | 2 | 8 | 9 | 15 | 3 | 13 | 1 | 7 |
| S19 | 19 | 13 | 20 | 7 | 14 | 8 | 21 | 15 | 22 | 1 | 16 | 2 | 23 | 9 | 24 | 3 | 10 | 4 | 17 | 11 | 18 | 5 | 12 | 6 |
| T20 | 20 | 14 | 19 | 8 | 13 | 7 | 22 | 26 | 21 | 2 | 15 | 1 | 24 | 10 | 23 | 4 | 9 | 3 | 18 | 12 | 17 | 6 | 11 | 5 |
| U21 | 21 | 15 | 23 | 9 | 17 | 11 | 19 | 13 | 24 | 3 | 18 | 5 | 20 | 7 | 22 | 1 | 12 | 6 | 14 | 8 | 16 | 2 | 10 | 4 |
| V22 | 22 | 16 | 24 | 10 | 18 | 12 | 20 | 14 | 23 | 4 | 17 | 6 | 19 | 8 | 21 | 2 | 11 | 5 | 13 | 17 | 15 | 1 | 9 | 3 |
| W23 | 23 | 17 | 21 | 11 | 15 | 9 | 24 | 18 | 19 | 5 | 13 | 3 | 22 | 12 | 20 | 6 | 7 | 1 | 16 | 10 | 14 | 4 | 8 | 2 |
| Y24 | 24 | 18 | 22 | 12 | 16 | 10 | 23 | 17 | 20 | 6 | 14 | 4 | 21 | 11 | 19 | 5 | 8 | 2 | 15 | 9 | 13 | 3 | 7 | 1 |

where ab is the composition of the letters a,b in the group $S_4$.

The deciphering is naturally given by the table

$$a_1 = u_o^{-1}u_1 ,$$
$$a_2 = u_1^{-1}u_2 ,$$
$$a_3 = u_2^{-1}u_3 ,$$
$$\dots\dots\dots\dots$$

Recalling that $S_4$ is a group, we have

THEOREM 1. *The grammar* $g$, *defined by* (3), *is the one-to-one mapping* $w \to u$ *(and is therefore invertible).*

6. As an example let us take the clear sentence

w = "suspe ndthe attac kimme diate lyyyy"

Let the one letter key be given by the letter E so that

$$u_o = E .$$

The first letter $u_1$ of the secret word U is $u_1 = W = ES$ where S is the first clear letter S.

The new key letter is now $u_1 = W$ and proceeding as formulated in (3) we get the secret word u:

u = "wnlht jrosn nrooi svswk dccwo rgrgc"

7. The measure of complexity of this cipher is given by

THEOREM 2. *As the measure* $\mu$ *of the complexity of the cipher described by* (3) *can be taken the number*

$$\mu = 24!\cdot 23\cdot 2$$

P r o o f. There are 24! combinations of associating 24 letters to the elements of $S_4$. There are 23 possibilities to select the key (the neutral element of $S_4$ is omitted as the key for evident reasons) and there are 2 possibilities to use the key on the left or on the right side in the composition of elements of $S_4$. This measure is valid in the case that the grammar $g$, using $S_4$, is somehow known to the decoder. In the opposite case we do not know how to express the measure of complexity of our cipher (the upper limit for the complexity being here is $24^{\text{length } w}$ when $g$ is supposed to be behind the cipher).

## REFERENCES

[1] M. Stojaković, *O jednom uredjenju simetričnih grupa, Godišnjak Filozofskog fakulteta, Novi Sad, 1956, knjiga I, str. 281-292.*

[2] A.G. Konheim, *Cryptography, New York, 1981.*

[3] Helen F. Gaines, *Cryptanalysis, Dover, 1956*

Received by the editors January 30, 1984.

REZIME

ŠIFRA SA JEDNOELEMENTNIM KLJUČEM

Iz azbuke od 26 slova engleskog jezika dva slova x i z zamenjena su respektivno sa ks i cs. Preostala 24 slova uzeta su nekim redom za elemente simetrične grupe $S_4$. Opisan je algoritam za pretvaranje jasnog teksta u skriveni u koju svrhu treba kao ključ pamtiti samo jedno slovo (dok se tabela za $S_4$ automatski dobija iz $S_1$). Šifrovanje i dešifrovanje za ovu šifru je opisano i jedan primer naveden. Mera sigurnosti šifre takodje je procenjena.