MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

The Josse Challenge – Part 1

Author: Nils Kopal

February 2023

Introduction (1/5) – The Cipher

The **Josse cipher** was recently discovered by Rémi Géraud-Stewart and David Naccache in historical documents from the late 19th century, written by Major H.D. Josse of the French Army. Details of the cipher and its discovery can be read in [GSN21].

The cipher is an auto-key cipher, with a mixed alphabet. Lasry showed in [Las21] that the Josse cipher can be broken either using isomorphs or with a heuristic attack based on simulated annealing.

CrypTool 2 contains an implementation of the Josse cipher:

https://www.cryptool.org/en/ct2/downloads

Introduction (2/5) – Lookup Table Generation

The first step of the cipher is the creation of a lookup table (based on another table) to convert the plaintext letters into numbers from 1 to 25. In the alphabet he used, Major Josse removed the letter W.

In the first table (see Table 1 on next page) a keyword (e.g., "SECRETKEY") is written in the first row. Here, any duplicate letters are omitted. After that, the remaining unused letters of the 25-letter alphabet are added in the rows below.

Finally, the lookup table (see Table 2 on next page) is generated by reading out the first table column-wise and assigning numbers from 1 to 25 to the read letters.

Introduction (3/5) – Generated Tables

S	E	C	R	T	K	Y
A	B	D	F	G	H	I
J	L	M	N	O	P	Q
U	V	X	Z			

Table 1: First table generated from the keyword "SECRETKEY"

S	A	J	U	E	B	L	V	C	D	M	X	R	F	N	Z	T	G	O	K	H	P	Y	I	Q
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 2: Second table for converting between letters and numbers

Introduction (4/5) – How Encryption Works

For encrypting a text, the plaintext is first converted into numbers using the lookup table: Example (Table 2 on previous page is used here):

H	E	L	L	O	V	V	O	R	L	D
21	05	07	07	19	08	08	19	13	07	10

Then, three encryption rules (see next page) are applied to compute the ciphertext numbers. In the last step, these numbers are converted to ciphertext letters using the same lookup table:

04	01	08	15	09	17	25	19	07	14	24
U	S	V	N	C	T	Q	O	L	F	I

Introduction (5/5) – Encryption rules

For encryption use the following three rules:

1. Compute first ciphertext letter: $C_1 = (25 - P_1)\ mod'\ 25$
2. Compute second ciphertext letter: $C_2 = (P_2 + P_1)\ mod'\ 25$
3. Compute i-th ciphertext letter: $C_i = (P_i + C_{i-1})\ mod'\ 25$

($mod'\ 25$ is: if $x\ mod\ 25$ is equal to 0 then use 25 instead of 0)

The decryption is the inverse process.

For a more detailed description of the cipher, you may watch a video of the "Cryptography for everybody" YouTube channel about the Josse cipher [Kop22].

Challenge

This is the **first challenge** in a series of **three challenges** with the Josse cipher.

With this challenge, we provide a **ciphertext with 207 letters**:

```
ROJBL GOVRB EAATO OVVES SOQIB AKFCJ JDFNU RVRNG JTEBA
TOOZJ AEBTA ONXXJ UQALV BBIPP FYXXO JIIBJ LDLEE XKUJJ
IRQSF YFFVE UYALZ YBFEC KKNNQ FLTKK OBBUL ZPGGL ZPRFY
LALLD AEBZD HCSJL YXXJB BQFZS CIORD HGOGF FCQLK GPPIX
HMPDN VYGSC OOKTP PDHII XFVGO XP
```

The solution are the **first 14 letters** of the plaintext.

References

- Rémi Géraud-Stewart and David Naccache, *A French cipher from the late 19th century*, Cryptologia **45** (2021), no. 4, 342–370.
- Nils Kopal, *Cryptography for everybody: A French Army Cipher from the late 19th Century, YouTube URL: https://www.youtube.com/watch?v=zKmNgR1-DJM*.
- George Lasry, *Analysis of a late 19th century french cipher created by Major Josse*, Cryptologia (2021), 1–15.