Criptografie clasica utilizand cuburile Enigma

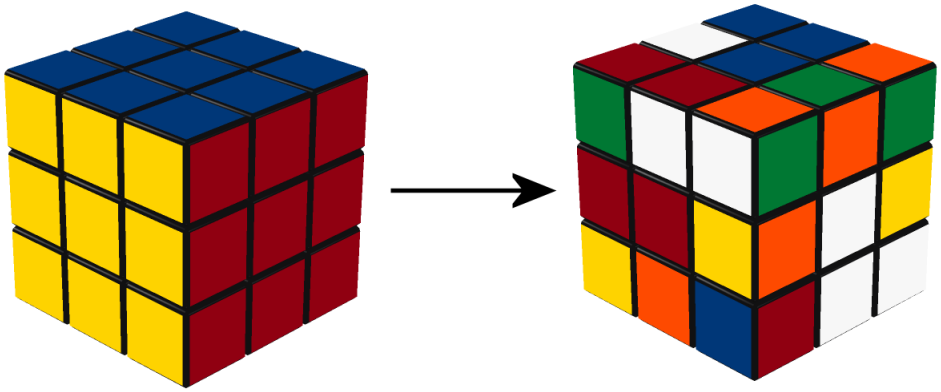
Criptografia este stiinta codificarii mesajelor, astfel incat acestea sa nu poata fi intelese de catre persoane neautorizate.

a) criptografia clasica – bazata pe dispozitive mecanice sau electro-mecanice

Masina Enigma

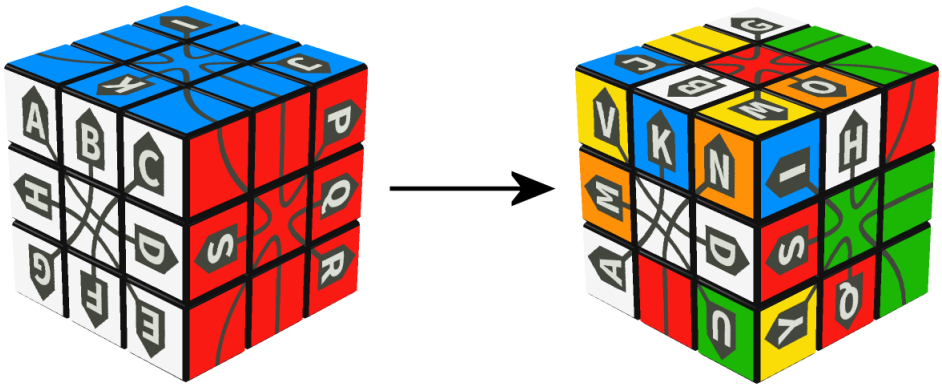
b) criptografia moderna – bazata pe algoritmi implementati pe calculator

Cubul Rubik este un dispozitiv mecanic tridimensional capabil sa genereze un numar impresionant de permutari distincte.



Cubul Rubik

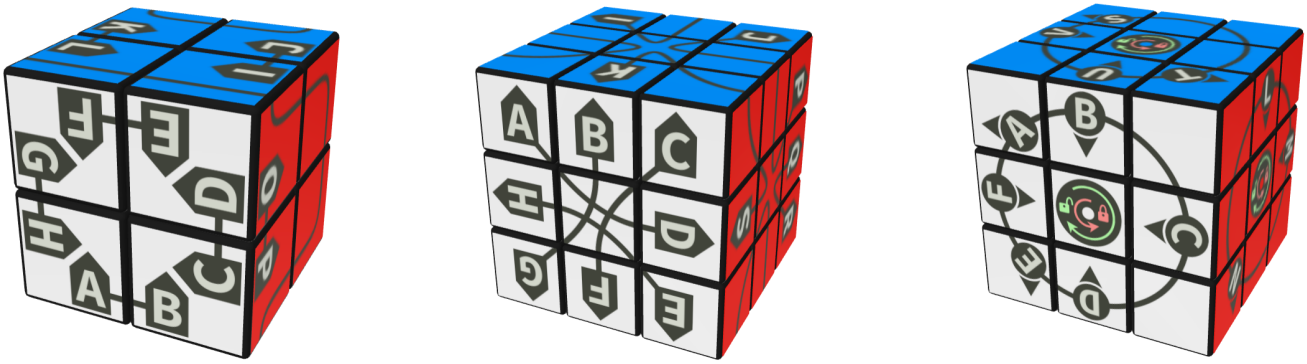
Pentru a utiliza Cubul Rubik in criptografie avem nevoie de litere si legaturi plasate pe fatetele cubului. Legaturile dintre litere sunt folosite pentru a realiza corespondente (numite substitutii).



Litere si legaturi plasate pe fatetele cubului

Introducem in continuare trei configuratii de litere si legaturi ce dau nastere la trei cuburi distincte

- *Enigma Pocket Cube* (cubul de buzunar Enigma)
- *Enigma Rubik's Cube* (cubul Rubik Enigma)
- *Non-reciprocal Enigma Rubik's Cube* (cubul Rubik Enigma nereciproc)



De la stanga la dreapta: Enigma Pocket Cube, Enigma Rubik's Cube si Non-reciprocal Enigma Rubik's Cube

In cazul cubului nereciproc, corespondenta dintre litere se realizeaza astfel. Pentru codificare urmarim legatura dintre litere in sens anti-orar, iar pentru decodificare sensul este cel orar.

De remarcat ca fiecare litera are definita o orientare data de varful pentagonului circumscris, respectiv de sageata alaturata. Rotirea feliei pe care se afla litera respectiva cu 90 de grade, in sensul indicat de orientarea sa, este un pas esential in tehnica de codificare si decodificare. Acest pas se numeste *amestecare incrementala*.

Cum decodificam un mesaj? Vom da un exemplu.

Avem nevoie de mesajul codificat, dat sub forma unei secvente de litere scrise in grupuri de cate cinci, in care diacriticele si semnele ortografice se ignora.

```
DTGGC LXWKE HOBWW UBWBJ AAKEJ BOKNS VHADH DDCWK PTZGS BMBSV BRSOB OKFIQ
```

De asemenea, avem nevoie de o cheie secreta, sub forma unei secvente de litere, ce va fi utilizata la initializarea cubului si care trebuie cunoscuta doar de catre persoanele autorizate in descifrarea mesajului.

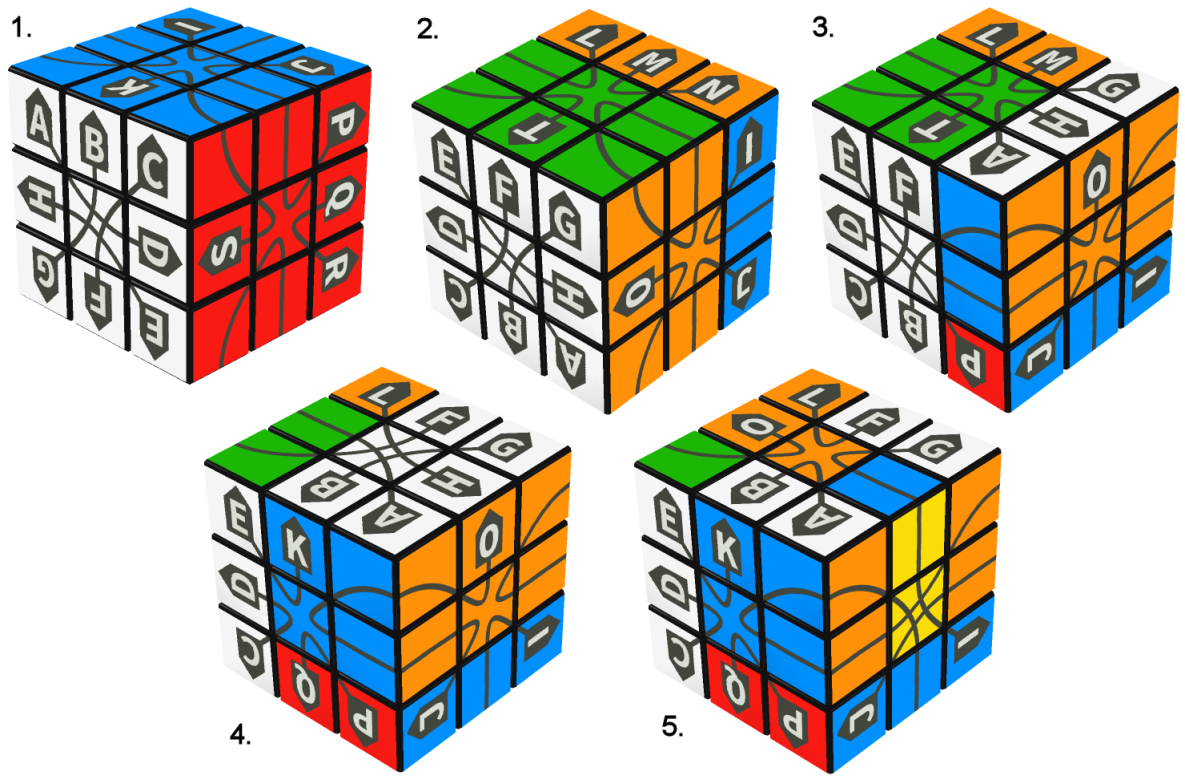
```
INFO
```

Trebuie precizat si dispozitivul folosit, in cazul de fata Enigma Rubik’s Cube.

Etapele decodificarii sunt urmatoarele

a) aplicarea cheii

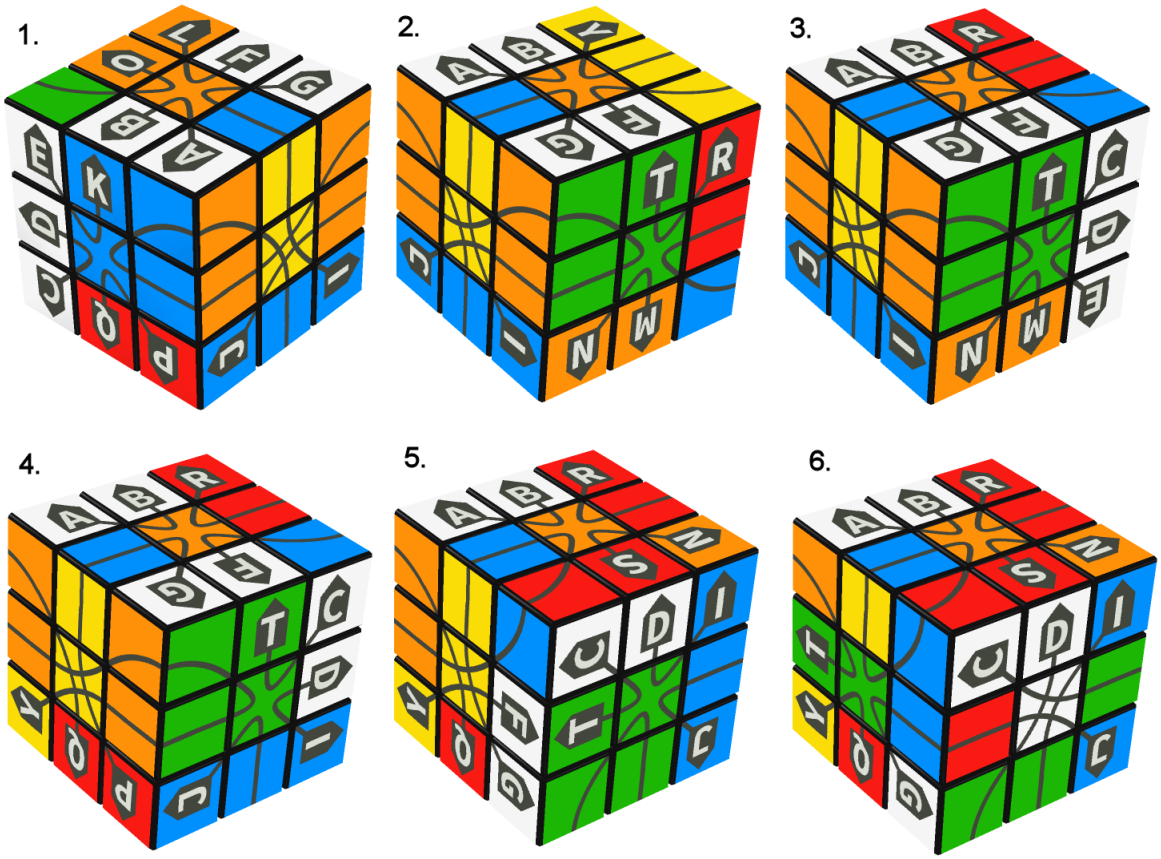
Identificam pe cub prima litera din cheie, I, si efectuam amestecarea incrementala asociata ei. Continuam apoi cu urmatoarea litera, N, s.a.m.d. Aducem astfel cubul intr-o stare amestecata initiala de la care vom incepe decodificarea mesajului propriu-zis.



Aplicarea cheii INFO

b) decodificarea mesajului litera cu litera

Identificam pe cub prima litera din mesaj, D, si cautam litera aflata in corespondenta, C. Aplicam amestecarea incrementala corespunzatoare acestei ultime litere. Identificam pe cub urmatoarea litera din mesaj, T, si cautam litera aflata in corespondenta, R. Aplicam amestecarea incrementala corespunzatoare acestei ultime litere, s.a.m.d. De remarcat, cubul continua sa se amestece cu fiecare litera parcursa, generandu-se astfel noi substitutii.



Decodificarea primului grup de cinci litere DTGGC

Pentru prima grupa de litere obtinem corespondenta

```
D-C
T-R
G-I
G-P
C-T
```

Urmatoarele corespondente sunt

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

Mesajul decodificat este

```
CRIPT OGRAF IAEST ECONS ECINT AMATE MATIC AAPRE SUPUN ERILO RPARA NOICE
```

care se citeste “Criptografia este consecinta matematica a presupunerilor paranoice”.

Tema. Decodificati urmatoarele mesaje, folosind dispozitivele indicate si cheia secreta furnizata la curs.

a) dispozitiv: Enigma Pocket Cube

```
WIUNU DFZJO VOWNB JYYWX XOXUE CSHPS LUJTQ F
```

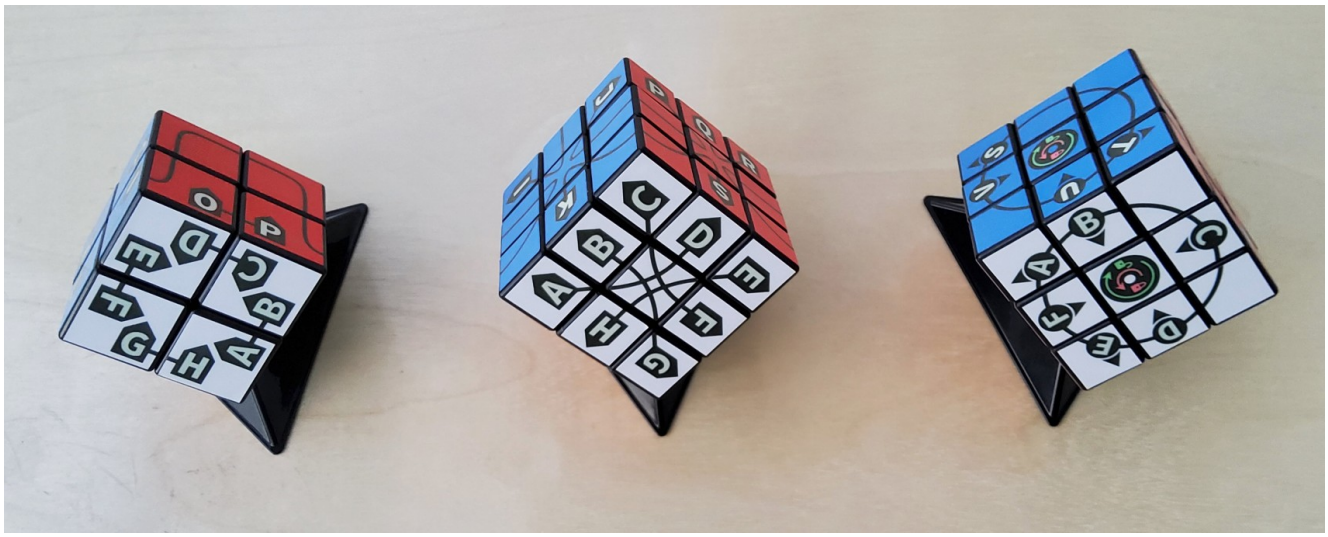
b) dispozitiv: Enigma Rubik’s Cube

```
CXGKY XTJDK HDTYQ VKFQT ZQYFE BZYIO AGLMD IGLVR ETCNZ FEDYQ WBPRW ASOTL
BBNM
```

c) dispozitiv: Non-reciprocal Enigma Rubik’s Cube

```
DHFWB DEPCJ GCBJQ CCNHT YHJWX MRBVR OTSJW AFVFY BGGXH LMWBL VOHAT RDEON
HJJUZ XPTJU HRKV
```

Cuburile Enigma nu sunt inca disponibile in format fizic.



Cuburile Enigma in format fizic

Ele sunt insa accesibile in format virtual la adresele de mai jos.

Enigma Pocket Cube
http://www.randelshofer.ch/rubik/virtual_cubes/pocket/picture_cubes/2x_enigma_cube.html

Enigma Rubik's Cube
http://www.randelshofer.ch/rubik/virtual_cubes/rubik/picture_cubes/enigma_cube.html

Non-reciprocal Enigma Rubik's Cube
http://www.randelshofer.ch/rubik/virtual_cubes/rubik/picture_cubes/enigma_cube_nr.html

Utilizati aceste adrese pentru a rezolva tema si pentru a afla detalii suplimentare legate de Cuburile Enigma.