

## SISTEME DE CRIPTARE

### I. Noțiuni introductive

#### CIFRURI DE TRANSPOZIȚIE

### II. Cifrul Rail Fence

1. Citiți despre modalitatea de criptare Rail Fence. Cripțați un mesaj oarecare și vedeți cum funcționează.
2. Decripțați mesajul următor:



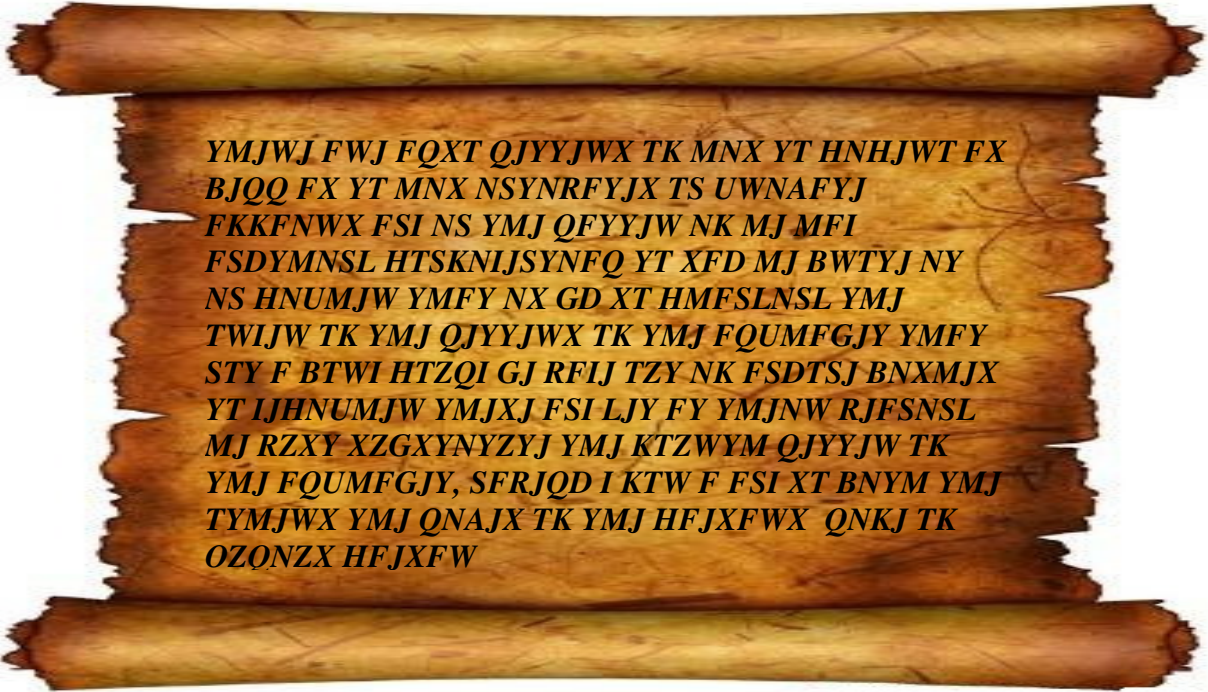
**CRROEIIAZFDNIRESTUTPI**

3. Care este cheia? Cum ați obținut-o?

#### CIFRURI DE SUBSTITUȚIE MONOALFABETICE

### III. Sistemul de criptare Cezar

1. Citiți despre sistemul de criptare Cezar. Cripțați un mesaj oarecare și vedeți cum funcționează.
2. Decripțați următorul mesaj:

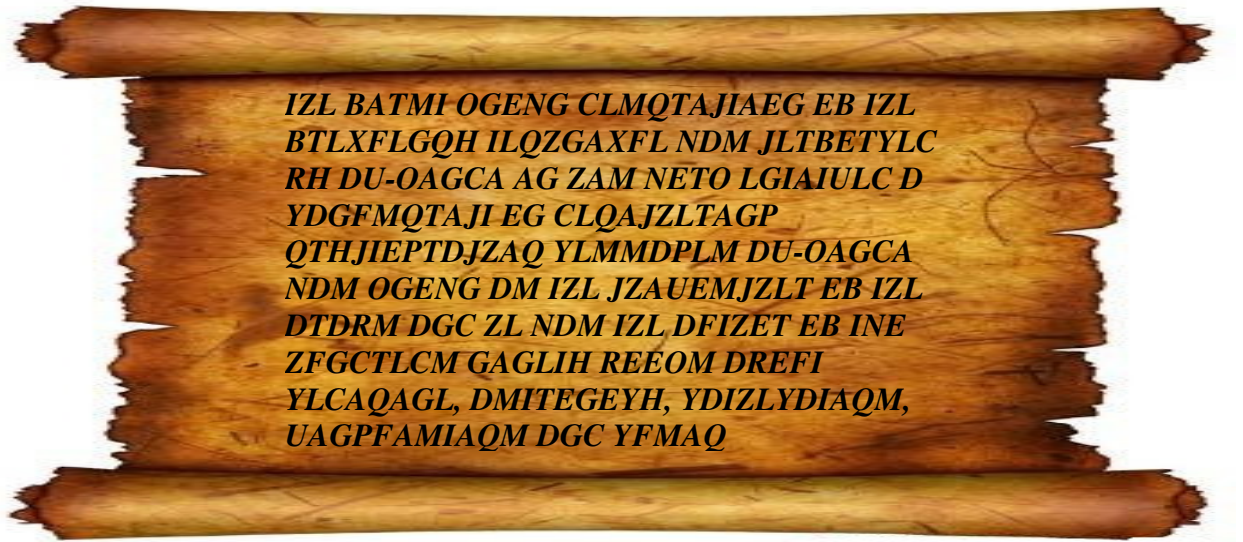


**YMJWJ FWJ FQXT QJYYJWX TK MNX YT HNHJWT FX  
BJJQ FX YT MNX NSYNRFYJX TS UWNIFYJ  
FKKFNWX FSI NS YMJ QFYJYJW NK MJ MFI  
FSDYMNSL HTSKNIJSYNFQ YT XFD MJ BWYJY NY  
NS HNUMJW YMFY NX GD XT HMFSLNSL YMJ  
TWIJW TK YMJ QJYYJWX TK YMJ FQUMFGJY YMFY  
STY F BTWI HTZQI GJ RFIJ TZY NK FSDTSJ BNXMJX  
YT IJHNUMJW YMJXJ FSI LJY FY YMJNW RJFSNSL  
MJ RZXY XZGXNYZYJ YMJ KTZWYM QJYYJW TK  
YMJ FQUMFGJY, SFRJQD I KTW F FSI XT BNYM YMJ  
TYMJWX YMJ QNAJX TK YMJ HFJXFWX QNKJ TK  
OZQNZX HFJXFW**

3. Ce ați obținut? Care este cheia?
4. Câte chei posibile există?

#### **IV. Analiza de frecvență**

1. Citiți despre metoda analizei în frecvență.
2. Folosiți metoda de analiză în frecvență pentru a decripta următorul mesaj:



### **CIFRURI DE SUBSTITUȚIE POLIALFABETICE**

#### **V. Sistemul de criptare Vigenere**

1. Citiți despre sistemul de criptare Vigenere.
2. Criați un mesaj oarecare și vedeți cum funcționează.
3. Decriați un mesaj utilizând o cheie cunoscută.

#### **VI. Criptanaliza sistemului de criptare Vigenere**

1. Citiți despre criptanaliza sistemului.
2. Folosiți metoda despre care ați citit pentru a decripta următorul mesaj:

**RFIVDDWCYKMGIJKUKAJTTSFZREHTFPGPLZSTOSLC  
OSSJFGZGVNQFACAFHATKABTYEHWGVNDSCZPTSR  
KHQYAJIEYIVXMAIEAFWOEAXGOTAXZEUTTSKRSUG  
KZTQGTKAWSSRDHONKASSOWTTSFRCFHHRTOSRKA  
UBCFMYCNNODRSCIWSTYEIWLCBKQHRNOSBVEZQR  
PPFSDLSUBGKHQGADEWSYCEFHEISXSAUIZUTFRQD  
ERTQRGIOGDSZNFVETIBVEITQLT**

## ALTE CIFRURI DE SUBSTITUȚIE

### VII. Cifrul Playfair

1. Citiți despre sistemul de criptare Playfair.
2. Criptați un mesaj oarecare și vedeți cum funcționează.
3. Decriptați mesajul următor:  
Indicație: I/J se consideră o singură literă  
Indicație: Mesajul clar conține cuvântul PLAYFAIR

**YA QA DK SM CI RF HA AB TC AG LI LR CA**

#### ① Mai multe informații:

1. S.Singh „Cartea Codurilor – Istoria secretă a codurilor și a spargerii lor” , Ed. Humanitas, București, 2005.  
<http://simonsingh.net/cryptography/crypto-cd-rom/>  
[http://www.simonsingh.net/The\\_Black\\_Chamber/index.html](http://www.simonsingh.net/The_Black_Chamber/index.html)
2. Laurent Joffrin „Istoria codurilor secrete”, Ed. Litera, București, 2010.
3. V.Maieran, D.Dulciu „O istorie a criptografiei românești”, Ed. Rao, București, 2010.
4. D.Kahn „The Codebreakers: The Comprehensive Story of Secret Communication from Ancient Times to the Internet”, 1967 (1996).
5. CrypTool Online  
<http://www.cryptool-online.org/>
6. Crypto Club  
<http://www.cryptoclub.org/>