

SISTEME DE CRIPTARE

I. Noțiuni introductive

CIFRURI DE TRANSPOZIȚIE

II. Cifrul Rail Fence

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



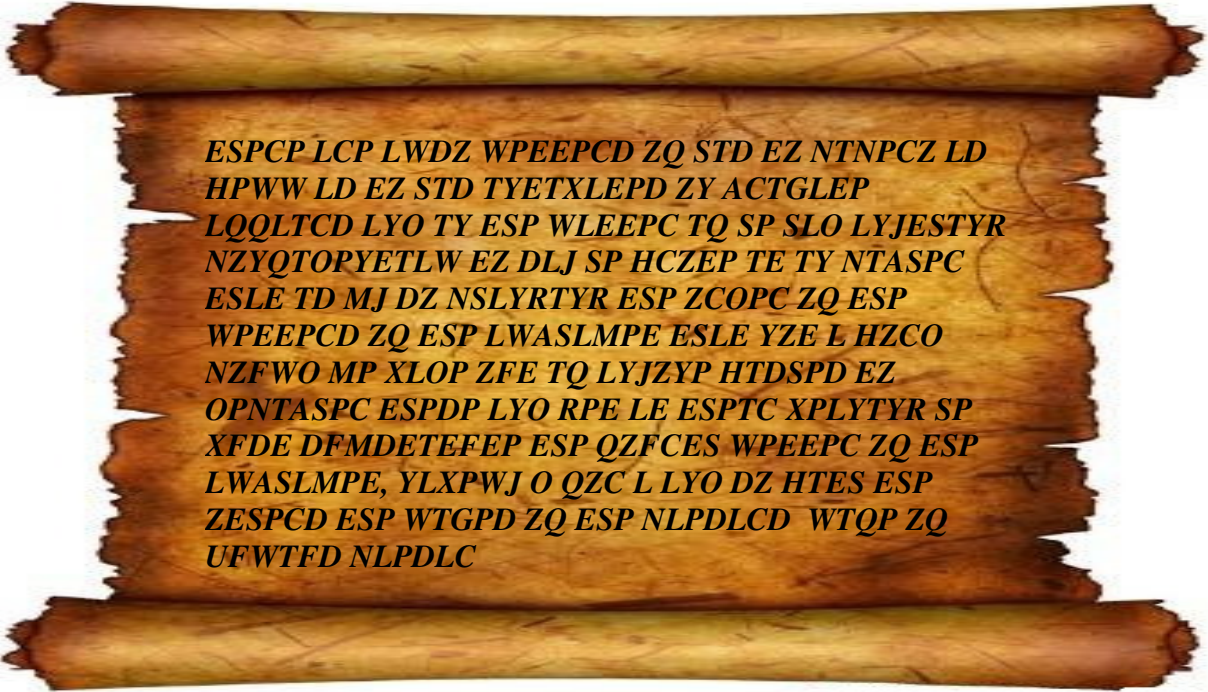
MAALEOOLOXDRIRTIDTDFIEHNRNCEET

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

CIFRURI DE SUBSTITUȚIE MONOALFABETICE

III. Sistemul de criptare Cezar

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

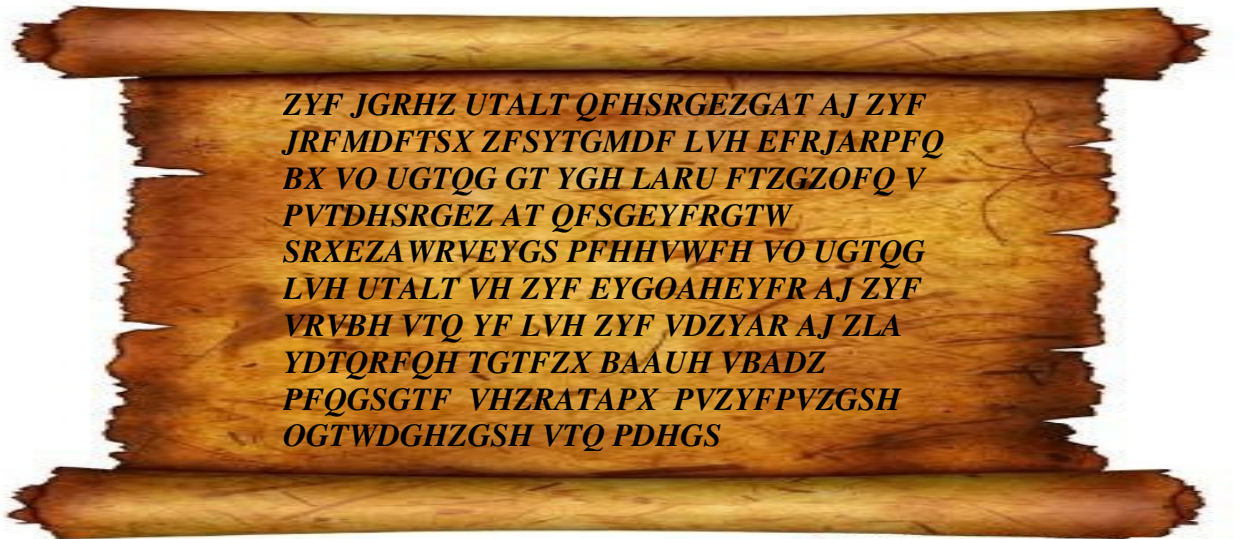


**ESPCP LCP LWDZ WPEEPCD ZQ STD EZ NTNPCZ LD
HPWW LD EZ STD TYETXLEPD ZY ACTGLEP
LQQLTCD LYO TY ESP WLEEPC TQ SP SLO LYJESTYR
NZYQTOPYETLW EZ DLJ SP HCZEP TE TY NTASPC
ESLE TD MJ DZ NSLYRTYR ESP ZCOPC ZQ ESP
WPEEPCD ZQ ESP LWASLMPE ESLE YZE L HZCO
NZFWO MP XLOP ZFE TQ LYJZYP HTDSPD EZ
OPNTASPC ESPDP LYO RPE LE ESPTC XPLYTYR SP
XFDE DFMDETEFEP ESP QZFCES WPEEPC ZQ ESP
LWASLMPE, YLXPWJ O QZC L LYO DZ HTES ESP
ZESPCD ESP WTGPD ZQ ESP NLPDLCD WTQP ZQ
UFWTFD NLPDLC**

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
KHQYAJIEYIVXMAIEAFWEOAXGOTAXZEUTTSKRSUG
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

SI YS BQ HU HQ AO UI QI ZU PC XG CA SW

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
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/>