Laborator 1 Criptografie si Securitate

February 2021

1. **Noţiuni introductive**

Cifruri de transpoziţie

2. **Cifrul Rail Fence**

   (a) Citiţi despre cifrul Rail Fence. Criptaţi un mesaj oarecare şi vedeţi cum funcţionează.

   (b) Decriptaţi mesajul următor:
   BLISITARPIENICCTSCENUEOEUEAERDGIRTTVSLRFIAIUAT

   (c) Care este cheia? Cum aţi obţinut-o?

3. **Cifrul transpoziţie coloană (Pătratul Latin)**

   (a) Citiţi despre cifrul transpoziţie pe coloană. Criptaţi un mesaj oarecare şi vedeţi cum funcţionează.

   (b) Decriptaţi următorul mesaj (e în română):

   FUAEOUAAMRD
   FBIRPIOUTMF
   NRVIEDLAAAR
   EERANSEIBUA
   CUNIENPNIAR
   EGDIOANSRTR
   LSIEIAUCIVC
   OCSUNOPTANA
   RLBPPIEIARU
   PLSIARTCERO
   SITRUTRATTZ
   TEASTSPEIUG

   (c) Care este cheia? Cum aţi găsit-o?

4. **Sistemul de criptare Cezar**

   (a) Studiaţi sistemul Cezar. Criptaţi un mesaj oarecare şi vedeţi cum funcţionează.

   (b) Decriptaţi următorul mesaj (este în engleză).
   LZWJW SJW SDKG DWLLWJK GX ZAK LG UAUWJG SK OWDD SK LG ZAK AFLAESLWK GF HJANSLW SXXSAJK SFV AF LZW DSLLWJ AX ZW ZSV SFQLZAFY UGFXAVWFLASD LG KSQ ZW OJGLW AL AF UAHZWJ LZSL AK TQ KG UZSFYAFY LZW GJVWJ GX LZW DWLLWJK GX LZW SDHZSTWL LZSL FGL S OGJV UGMDV TW ESVW GML AX SFQGFW OAKZWK LG VWUAHZWJ LZWKW SFV YWL SL LZWAJ EWSFAFY ZW EMKL KMTKLALMLW LZW XGMJLZ DWLLWJ GX LZW SDHZSTWL FSEWDQ V XGJ S SFV KG OALZ LZW GLZWJK LZW DANWK GX LZW USWKSJK DAXW GX BMDAMK USWKSJ

   (c) Care este mesajul? Dar cheia?

   (d) Câte chei posibile sunt?

5. **Sistemul de criptare Vigenere**

   (a) Citiţi despre sistemul Vigenere şi despre criptanaliza acestuia.

   (b) Criptaţi şi decriptaţi un mesaj folosind o cheie cunoscută.

   (c) Decriptaţi mesajul următor.
   CCAWXAOJTPUBFZNAHAGKBAHGUVBTOWMVNGLPGTCXOS
   JKHTJPGUGIYCXZNKLLVZLVMVKTIEOCTUSTMC
   GKHRLLVLPNFWYRTIYGDLRXHBZYEIOAGERJKMGLT
   WVPKEPTTROEGSLTKXCCKSYSODRRTRGRMRKJCWPD
   HICHHIYVCGACUDYCBFKJDTZATZPTLHNFUVORVYY
   IASCRSSLQEIGQBBMRCXWFGIRWTHNVHXTQGCDXGJ
   KETTKGVJAAXOXKOBVBGILPNHNFRHHLFTPNIHUXR
   PWFGIQIAOZXIDCYPSYIMWYKAQLJNRQDPVUNAHIM
   TEYGHITUTWLQCDCIBAKRSQSYKJCSXJOXECYCKJY
   RMIGCLNAFGRSIACXFFIOCEZNWXF