



**FERIT**

**Zavod za komunikacije**



**KIBERNETIČKA SIGURNOST**  
(laboratorijske vježbe)

## Vježba 5. **KRIPTOANALIZA**

### **Zadatak 1. Cezarova šifra**

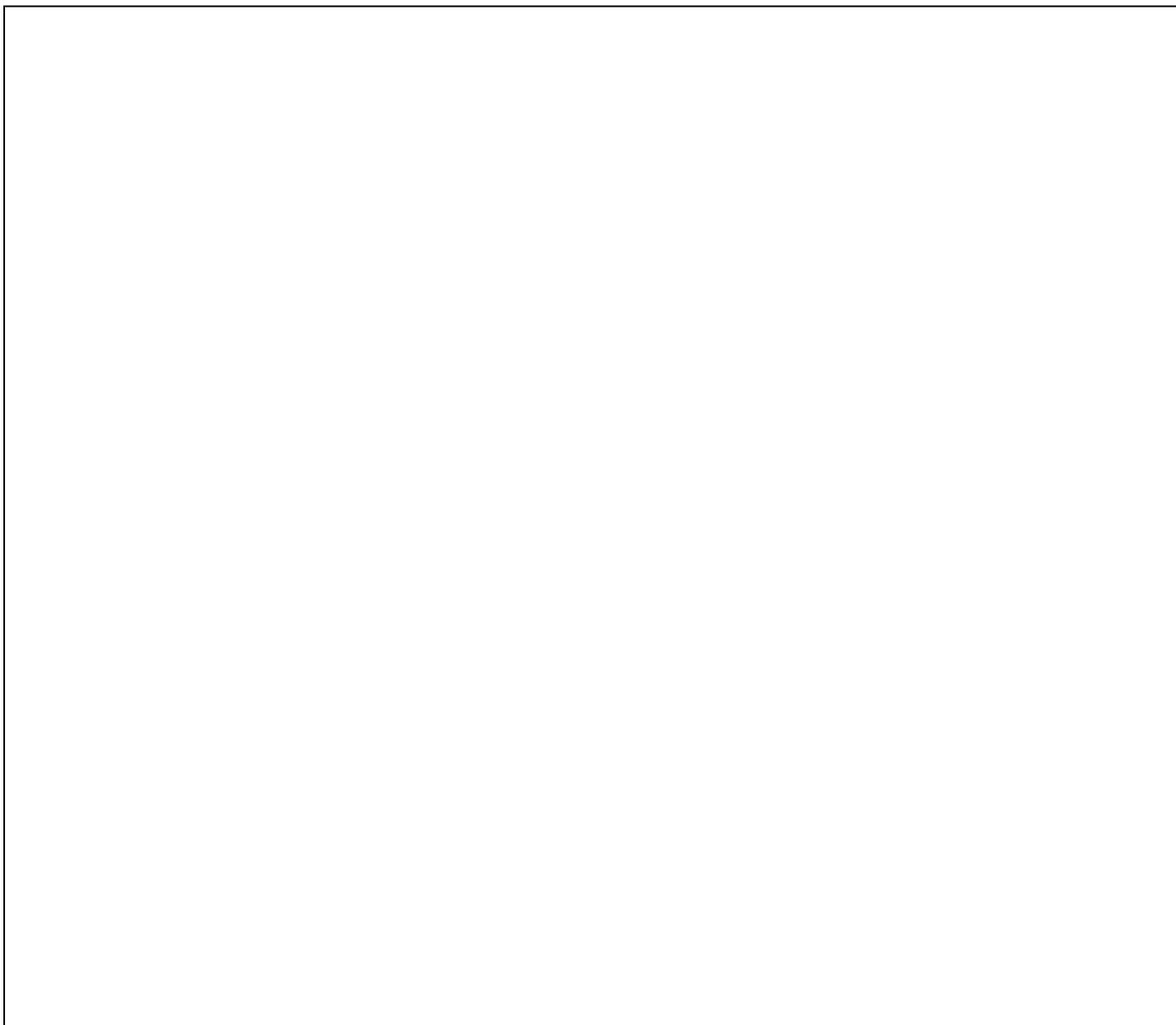
- U aplikaciji *CrypTool* pomoću sustava za kriptanalizu Cezarove šifre „grubom silom“ dekriptirati sljedeće šifrate:
  - UWRSJGNSKAXJS: \_\_\_\_\_
  - EGFGSTWUWVFSKMHKLALMUABS: \_\_\_\_\_
  - KVCVBFDLZBRTZAV: \_\_\_\_\_
  - VASBEZNGVXN: \_\_\_\_\_
- Ucertati i objasniti sustav za kriptanalizu Cezarove šifre „grubom silom“:

- Pomoću sustava za kriptanalizu Cezarove šifre „grubom silom“ dekriptirati sljedeći šifrat:

Aopz zhtwsl wlymvytz h iybal-mvyjl jpwolyalea-vusf haahjr vu aol Jhlzhy jpwoly. Aol ihzpj wypujpwsł pz aoha aol jpwolyalea pz kljyfwalk dpao hss wvzzpisl zopma chsblz huk mvy lhjo ylzbsapun wshpualea pa pz joljrlk pm pa jvuahpuz dvykz myvt h kpjapvuhyf. Pm zlclyhs dvykz hyl mvbuk pa jhu il hzzbtlk dpao opno wyvihipsaf aoha aopz pz aol jvyylja kljyfwapvu.



- Ucertati i objasniti sustav za kriptanalizu Cezarove šifre analizom frekvencija:



- Pomoću sustava za kriptanalizu Cezarove šifre analizom frekvencija dekriptirati sljedeći šifrat:

Zxbpxo txp x mlifqfzfxk xka dbkboxi lc qeb ixqb Oljxk obmryifz, tel dobxqiv buqbkaba qeb Oljxk bjmfob ybclob  
pbfwfkd mltbo xka jxhfkf efjpbic afzqxqlo lc Oljb, mxsfkd qeb txv clo qeb fjmbofxi pvpqbj.

- U predviđeni prostor upišite vlastite zaključke, zapažanja i komentare:

## Zadatak 2. Vigenereova šifra

- Dekriptirati sljedeći tekst, ako se zna da je šifriran Vigenereovom šifrom:

Vpt mmiub llpc fwrpqvpbtk hvukgptkkwc vj r rwafecrppliikkk rptygz lhw wqzbbprvms ic Cgwc Iekvqhae Rnjtyxz czdbu 1467 cvs bwvf i blxrn kxwlt lxzg kq alptj jtaavgv rptygz pstycjtaw. Rnjtyxz'u anzxvo wesc jyqijlvf iawlrnmiz ewvmg zimgzps aftlh, hru uexagyga llv kvspgrvms ic ntqiprx vpt sikvmg vj kjm rrvigaevrukvv hpgjiqlx zp bwl gxrptyxvzb. Ahxvt, qc 1508, Qsyevclw Ktqioidkch, pr yka lvvb Rwapkicxwpe, zpdtxvf bwl xrdcah vvebp, h gikbxjec ewbwsegvi vj kjm Kpkvpèzt jmgjmg. Alv Vzخالvoqjz gxrpty, lfymklv, fptn wvfxqslh r rzdnavuaxci, ikoxk eef xglhzebpipv ughaid hwg zazvkwprx dmdivp kxwlt iawlrnmiz.

- U predviđeni prostor upišite vlastite zaključke, zapažanja i komentare (analizirajte princip rada sustava za kriptanalizu Vigenereove šifre):

### Zadatak 3. DES i AES

- Šifrirajte vlastito ime i prezime (npr. PETARPETROVIC) pomoću DES algoritma, uz zadani ključ: 0x1234567890ABCDEF:

Šifrat (hex): \_\_\_\_\_

- Pomoću sustava za kriptanalizu DES-a pokušajte dekriptirati prethodno dobiveni šifrat, uz unos dijela ključa (\* označava nepoznati dio ključa). U tablicu unesite potrebno vrijeme dekriptiranja:

Ključ	Vrijeme
1234567890ABCDEF	
12345678*****	
123456*****	
1234*****	
*****	

- Šifrirajte vlastito ime i prezime (npr. PETARPETROVIC) pomoću AES algoritma, uz zadani ključ: 0x11223344556677889900AABBCCDDEEFF:

Šifrat (hex): \_\_\_\_\_

- Pomoću sustava za kriptanalizu AES-a pokušajte dekriptirati prethodno dobiveni šifrat, uz unos dijela ključa (\* označava nepoznati dio ključa). U tablicu unesite potrebno vrijeme dekriptiranja:

Ključ	Vrijeme
11223344556677889900AABBCCDDEEFF	
11223344556677889900AABB*****	
11223344556677889900*****	
112233445566778899*****	
1122334455667788*****	
*****	

- U predviđeni prostor upišite vlastite zaključke, zapažanja i komentare:

ZAKLJUČAK

Popunjava student		Popunjava nastavnik	
Ime i prezime:		Datum pregleda:	Potpis: