# KRIPTOGRAFIJA

**Zadaća 1.145** $X$

Rok za podizanje zadaće je od 11.03.2005. do (uključivo) 18.03.2005. Rok za predaju ove zadaće je 01.04.2005.

1. Afinom šifrom s ključem $K$ je iz otvorenog teksta na hrvatskom jeziku dobiven sljedeći šifrat:

   ```
   BTSRQ TGXRX TNZZX NIRWP CTZJP XQZCE PIRNR NPUJI
   JFPXC ZIZNB TZUZS TQTCR UPBZN XTBZN ZDEZN GZDZC
   FTETA CTGZD XZQZG TGIPW ZCTIR SZITC TSEPX PUPUT
   XRUIT BRYTX RXJAY EARZY KPAPF BPWZM ETFJG TXTSZ
   ERAGP NPGXS RBQZE ZNXCT BPXRJ SPQTZ ATXQZ MTXIT
   ```

   Navedite pet najfrekventnijih slova, te pet najfrekventnijih bigrama u ovom šifratu.

   Odredite ključ $K = (a, b)$ i otvoreni tekst (dekriptirajte šifrat)!

2. Dekriptirajte šifrat

   ```
   LOXQK NLXSL MZSYS LHXFK OWLOF KQHWK NLXKE NQOOF
   JWODF ILJQN KWLMJ WOXQO WJQMF XQSLN LXICQ KSMOL
   XRFDW CFDNL XFLOX QMWOW PLKEW DPQMX SILZW EWJYW
   VRCFY JWXFS KQZSO XQULN LMZFD FYDOF JWLHW CSKQO
   XQKNW VHCFO FXQCX QFEPL KRQCF DFECL NFOF
   ```

   dobiven supstitucijskom šifrom, i to Cezarovom šifrom s ključnom riječi. Poznato je da je otvoreni tekst pisan na hrvatskom jeziku, te da je ključna riječ izraz (fraza ili riječ) na hrvatskom jeziku.