**I kolokvijum iz kriptologije 1**

1. Dešifrovati šifrat “tajnaporuka.cezar” sa ključem [11] i posebno definisanim alfabetom „ASTBNOUVWCDEPQRIJKLMXYZFGH“. Dalje slediti instrukcije iz dobijene poruke.

2. Trudi je uspela da prisluškuje kanal između Alise i Boba. Alisa i Bob šifruju poruke sa One-time pad šifrom. Međutim, napravili su grešku, koriste svaki put isti ključ. Fajlovi u folderu zadatka sadrže podatke koje je Trudi uspela da prisluškuje u komunikacionom kanalu, kao i tekst prve pretpostavljene poruke. U sledećem koraku Trudi treba da sazna kako glasi sledeća poruka na osnovu pribavljenih podataka.

Uneti rezultat za drugi deo zadataka:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ime i prezime:

Broj indeksa:

Napomena:

Kompletan folder sa projektima iz Cryptool-a sa početnim fajlovima je potrebno predati „nezipovano/neraraovano“ u folder kolokvijum, po završetku rada.