1. kontrolltöö aines "Kodeerimine ja krüptimine"

4. variant

1. (10p) Kirjelda statistilist rünnet asendusšifrile.

2. (15p) Olgu p algarv ja α tsüklilise rühma $(Z_p^*, \cdot)$ moodustaja. Olgu a valitud ühtlase jaotusega hulgast Z_{p-1}. Kas võib väita, et element α^a on rühmas $(Z_p^*, \cdot)$ ühtlase jaotusega?

3. (15p) Leia jada 1,0,0, 1,0,0, ... lineaarne keerukus ja vähima astmega karakteristlik polünoom.