1. kontrolltöö aines “Kodeerimine ja krüptimine”

3. variant

1. (10p) Kirjelda, kuidas saab ründaja CBC-režiimis kodeeritud krüptoteksti muutes kutsuda lähtetekstis esile ennustatavaid bitimuutusi.

2. (15p) Olgu elemendid a ja b valitud ühtlase jaotusega hulgast Z_n. Kas võib väita, et element $a \cdot b$ on ühtlase jaotusega?

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