

Kontrolltöö näidisvariant

1. Millised ühised jooned on Caesari ja Vigeneri šifritel? Mis rolli šifreerimise juures mängib K_i ?
2. Milles seisneb tervikluse vastu suunatud küberrünne?
3. Kuidas omavahel on seotud turvameetmed ja riskid?
4. Milles seisneb segamine sümmeetriliste algoritmide juures?
5. Mida kujutavad endast S-boxid ja kus neid kasutatakse?
6. Kuidas arvutatakse funktsiooni f Blowfish algoritmis? Mis on sisendiks, mis operatsioone kasutatakse?
7. Mille põhjal valiti AES algoritmi?
8. Mis pikkusega võtit kasutab algoritm Serpent ning kas saab seejuures kasutada lühikest võtit? Miks?
9. Mille poolest polünoomide korrutamine erineb tavalisest korrutamisest?
10. Kuidas teostatakse SubBytes protseduuri algoritmis Rijndael? Too näiteid.
11. Mille poolest avatud võtmega krüpteerimine erineb sümmeetrilisest?
12. Millele toetub matemaatilises plaanis avaliku võtmega krüpteerimine?
13. Kuidas kasutatakse Hash-funktsioone digiallkirjastamisel? Miks saab Hash-funktsioone selleks kasutada?
14. Mis on autentimise pilet ja miks seda vaja on?