Kriptografija ir informacijos sauga 2020
Egzamino klausimų temos

Egzamino užduotį sudarys 5 klausimai. Vieno klausimo vertė - 1 balas. Atsakant į klausimą reiks naudojantis duotais (arba pasirenkamais) duomenimis pateikti šifravimo, dešifravimo, skaitmeninio parašo ar kitų algoritmų pavyzdį. Vertinimui svarbus ne tik atsakymas, bet ir dėstymas: naudojami dydžiai apibrėžti (paaiškinti), taikomos formulės korektiškai užrašytos.

1. Šifravimas ir dešifravimas naudojant Hilo šifrą.
2. Šifravimas ir dešifravimas naudojant Vigenere šifrą.
3. Šifravimas ir dešifravimas naudojant paprastą ENIGMA tipo šifrą.
4. Šifravimas ir dešifravimas naudojant Feistelio schemą.
5. Šifravimas ir dešifravimas blokiniais šifrais CBC, OFB, CFB, CRT režimais.
6. Veiksmai su baitais AES šifre.
7. Rakto srauto generavimas naudojant tiesinių registrų sistemą.
8. Šifravimas ir dešifravimas su A5/1.
9. Maišos funkcijų konstravimas pagal Merkle-Damgaard schemą.
10. Vienkartinių slaptažodžių Lamporto schema.
11. Diffie-Hellmanno susitarimo dėl rakto protokolas.
12. Atvirkštinio elemento skaičiavimas Euklido algoritmu.
13. Greitasis kėlimo laipsniu algoritmas.
14. Lyginių sistemos sprendimas su kinų liekanų teorema.
15. Generuojančio elemento duotu moduliu radimas.
16. Diskretaus logaritmo skaičiavimas „baby step - giant step“ algoritmu.
17. Sudaryti kuprinės kriptosistemą, kai duotas svorių skaičius. Šifravimas ir dešifravimas su kuprinės kriptosistema.
18. Sudaryti RSA kriptosistemą kai duoti pirminiai. Šifravimas ir dešifravimas su RSA.

19. Sudaryti ElGamalio kriptosistemą su duotu moduliu. Šifravimas ir dešifravimas.

20. Pateikti skaitinį RSA aklo parašo pavyzdį.

21. Paaiškinti ElGamalio skaitmeninio parašo sudarymo ir tikrinimo algoritmus skaitiniu pavyzdžiu.

22. Paaiškinti Shnorro skaitmeninio parašo sudarymo ir tikrinimo algoritmus skaitiniu pavyzdžiu.

23. Paaiškinti DSA skaitmeninio parašo sudarymo ir tikrinimo algoritmus skaitiniu pavyzdžiu.

24. Padalyti paslaptį pagal Shamiro schemą su slenksčiu. Atkurti padalytą paslaptį

25. Padalyti paslaptį pagal Shamiro schemą su slenksčiu ir užmaskuotomis dalimis. Atkurti padalytą paslaptį.

26. Paaiškinti netiesioginį įrodymą apie kvadratinio lyginio sprendinį skaitiniu pavyzdžiu.

27. Paaiškinti netiesioginį interaktyvų įrodymą apie diskretųjį logaritmą skaitiniu pavyzdžiu.

28. Sukurti netiesioginį neinteraktyvų įrodymą apie diskretųjį logarimą.