Криптографија - испитна питања 2019/2020.

1. Плејферова шифра
2. Шифра ADFGVX
3. Еуклидов алгоритам, мултипликативни инверз
4. Мала Фермаова теорема, алгоритам степеновања квадрирањем, кинеска теорема о остацима
5. Афина шифра
6. Проточне шифре: RC4, самосинхронишућа шифра, случајна шифра
7. Коначна поља $\mathbf{F}_2[x]/(f(x))$.
8. Упрошћена варијанта AES
9. AES , карактеристике
10. Начини коришћења блоковских шифри
11. Напади на блоковске шифре, сусрет на пола пута
12. Сложености алгоритама за рачунање са великим бројевима
13. RSA
14. Протокол Дифи-Хелман
15. ЕлГамалов алгоритам за шифровање
16. Размена кључева Меси-Омура
17. Елиптичке криве
18. Протокол Дифи-Хелман са елиптичким кривама
19. ЕлГамалов алгоритам за шифровање са елиптичким кривама
20. Хеш функције, MD5, кодови за аутентикацију
21. Потписи помоћу RSA
22. Ел Гамалов потпис
23. Потпис помоћу елиптичке криве
24. Шноров поступак аутентикације и потписа
25. PKI, сертификати
26. Сигурност на интернету, TLS

27. Временски печат
28. КЕРБЕРОС
29. Управљање кључевима
30. Дељење тајне
31. Криптоанализа — основни појмови, Вижнерова шифра
32. Криптоанализа низа добијеног помоћу ЛПР
33. Криптонализа генератора b/p
34. Линеарна криптоанализа
35. Диференцијална криптоанализа
36. Рођендански парадокс, факторизација
37. Фермаова факторизација
38. Факторизација помоћу верижних разломака
39. Факторизација помоћу елиптичких кривих
40. Поље бројева
41. Сито у пољу бројева
42. Полиг-Хелманов алгоритам за решавање проблема дискретног логаритма у $\mathbf{F}_q^*$
43. Алгоритам за израчунавање индекса