Криптографија

специјални курс 4И
испитна питања 2024./2025.
доц. др Драган Ђокић

На испиту ће бити 3 питања са овог списка + 2 кратка задатка

1. Навести разлике између симетричних и асиметричних криптосистема
2. Цезарова и афина шифра и њихова криптоанализа
3. Једнократна шифра (One Time Pad)
4. Матрично криптовање диграфа
5. Једносмерне функције. Навести пример једносмерне функције
6. Дифи-Хелманов алгоритам за усаглашавање кључа
7. Алгоритам за степеновање поновљеним квадрирањем
8. Дефинисати дискретни логаритам. Навести 3 криптосистема који се заснивају на проблему дискретног логаритма
9. Алгоритам Гељфонд-Шенкса (Baby-step-giant-step алгоритам)
10. Полиг-Хелманов алгоритам
11. Меси-Омура криптосистем
12. Алиса шаље Бобану поруку помоћу Меси-Омура криптосистема, и претпоставимо да је Цица видела целокупну комуникацију. Објаснити зашто Цица ипак не може да декриптује поруку
13. ЕлГамалов криптосистем
14. Како се генерише случајан велики прост број
15. Тестови прималности. Шта су улазни и излазни подаци код теста прималности
16. Дефинисати псеудопросте и Кармајклове бројеве. Шта је главни недостатак Кармајкловог теста прималности
17. Милер-Рабинов тест прималности
18. Веза између псеудопростих и јако псеудопростих бројева. Ефикасност Кармајкловог и Милер-Рабиновог теста
19. Ривест-Шамир-Ејделман криптосистем

20. Привидно једносмерне функције. Навести пример привидно једносмерне функције
21. Фермаов метод факторизације
22. Криптоанализа РСА Фермаовим методом
23. Полардов $(p-1)$-метод
24. Зашто се јавни кључ $n = pq$ у РСА не може изабрати тако да не буде осетљив на напад Полардовим методом
25. Интегритет поруке и хеш алгоритам
26. Аутентикација, дигитални потпис и сертификат
27. Дигитални потпис помоћу РСА криптосистема
28. Чему служи хеширање приликом дигиталног потписа
29. Какво побољшање доносе елиптичке криве у а) сигурности криптосистема б) криптоанализи
30. Дефинисати и нацртати елиптичку криву над пољем реалних бројева
31. Дефинисати елиптичку криву над коначним пољем
32. Дефинисати операције на елиптичкој кривој. Групни закон на елиптичкој кривој
33. Хасеова теорема за број тачака на елиптичкој кривој. Зашто рад са групом $(E(\mathbb{F}_q), \oplus)$ нуди више могућности од групе $(\mathbb{F}_q \setminus \{0\}, \cdot)$
34. Проблем дискретног логаритма над елиптичким кривама
35. Кодирање и декодирање података помоћу елиптичке криве
36. Дифи-Хелманово усаглашавање кључа над елиптичким кривама
37. ЕлГамалов критпосистем над елиптичким кривама
38. Ленстрин метод факторизације