ПРОГРАМОВІ ВИМОГИ

для складання іспиту з навчальної дисципліни
«Математичні та алгоритмічні основи криптографічного захисту інформації»
спеціальність 121 «Інженерія програмного забезпечення»
ОП «Якість та безпека програмного забезпечення»

1. Захист інформації, його складові і рівні формування режиму інформаційної безпеки
2. Основні поняття криптології. Принцип Керкхоффса. Етапи розвитку криптографічних систем
3. Види історичних шифрів
4. Класичні шифри перестановки
5. Класичні шифри заміни
6. Криптографічна стійкість шифрів. Класифікація атак. Метод «грубої сили»
7. Блокові алгоритми і режими шифрування
8. Арифметика. Прості числа. НСД. Розширений алгоритм Евкліда.
9. Алгебраїчні структури. Група. Кільце. Поле. Скінченні поля.
10. Кільце лишків. Модульна арифметика. Функція Ейлера. Теореми Ейлера та Ферма.
11. Методи знаходження мультиплікативного оберненого елемента по модулю простого числа.
12. Поля Галуа GF(p^n). Побудова полів Галуа GF(2^n)
13. Множення двох байтів над полем Галуа GF(2^8)
14. Еліптичні криві
15. SP-мережа
16. Мережа Фейстеля
17. Симетричні криптосистеми. Загальна схема роботи. Шифр Калина як національний стандарт симетричного шифру
18. Асиметричні криптосистеми. Загальна схема роботи
19. Комбіновані криптосистеми. Їх переваги та недоліки.
20. Класифікація сучасних криптосистем та основні вимоги до них
21. Алгоритм шифрування DES. Основні операції. Стійкість
22. Функція шифрування f у алгоритмі DES
23. Формування раундових ключів у алгоритмі DES
24. Симетричний алгоритм блочного шифрування AES (Rijndael). Опис алгоритму
25. Раундові перетворення у AES
26. озгортання ключів шифрування у AES
27. Розшифрування у AES
28. Алгоритм асиметричного шифрування даних RSA, його криптостійкість та швидкість роботи
29. Протокол обміну сеансовими ключами Діффі–Хелмана.
30. Алгоритм Ель-Гамаля, його безпека та криптостійкість

31. Еліптична криптографія. Реалізація протоколу Діффі—Хелмана на основі еліптичних кривих.
32. Еліптична криптографія. Криптосистема Ель–Гамаля на основі еліптичних кривих.
33. Хешування. Вимоги до хеш-функцій. Способи взлому. Хеш-функція ”Купина” як національний стандарт.
34. Схема Меркеля–Дамгарда. Алгоритми сімейства MD і SHA
35. Опис алгоритму SHA-1, SHA-3
36. Поняття електронного цифрового підпису (ЕЦП). Схеми використання.
37. ЕЦП на основі асиметричної системи Діффі—Хелмана
38. Система ЕЦП Ель-Гамаля (EGSA).
39. Алгоритм ЕЦП DSA
40. Алгоритм ЕЦП ECDSA

Рекомендована література

1. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2012. – 256 с.
2. Бабаш А.В., Шанкин Г.П. Криптография. – М.: Солон-ПРЕСС, 2007. – 512 с.
3. Венбо Мао. Современная криптография. Теория и практика. М: Вильямс, 2005. – 768 с.
4. Вербіцький О. В. Вступ до криптології. – Львів: Видавництво НТЛ., 2008. – 248 с.
5. Глинчук Л.Я. Криптологія: навч.-метод. посіб. – Луцьк: Вежа-Друк, 2014. – 163 с.
6. Ємець В., Мельник А., Попович Р. Сучасна криптографія: основні поняття – Л.: БаК. – 2003. –144 с.
7. Задірака В.К., Олексюк О.С. Комп’ютерна криптологія: Підручник. – Київ – Тернопіль: Збруч, 2002. – 504 с.
8. Лахно В. А. Опорний конспект лекцій з дисципліни "Основи криптографічного захисту інформації". – Київ: [Б. в.], 2016. – 172 с.
9. Остапов С.Е., Валь Л.О. Основи криптографії. Навчальний посібник. – Чернівці: Книги – ХХІ, 2008. – 188 с.
10. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації: навчальний посібник. – Харків: Вид. ХНЕУ, 2013. – 476 с.
11. Столлингс В. Криптография и защита сетей: принципы и практики, 2-е изд.: Пер. с англ. – М.: Изд. дом «Вильямс», 2007. – 672 с.
12. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]. –Режим доступу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
13. Шнайер Б. Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С. – М.: ”Триумф”, 2001. – 610 с.