ВОПРОСЫ ПО КУРСУ «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ»

|  |  |
| --- | --- |
| КРИПТОГРАФИЯ С СЕКРЕТНЫМ КЛЮЧОМ | |
| **Введение** | |
| 1) | история криптологии |
| 2) | коммуникации и угрозы |
| 3) | криптосистема |
| **Классические криптосистемы** | |
| 4) | алфавит |
| 5) | шифр сдвига |
| 6) | аффинный шифр (обращение по модулю, функция Эйлера) |
| 7) | шифр простой замены |
| 8) | шифр Хилла |
| 9) | шифр перестановки |
| 10) | шифр Виженера |
| **Задачи криптоанализа** | |
| 11) | атаки |
| 12) | частотные атаки |
| 13) | криптоанализ шифра Виженера |
| **Элементы теории Шеннона** | |
| 14) | модель противника |
| 15) | совершенная криптосистема |
| 16) | энтропия |
| 17) | расстояние единственности |
| **Конечные поля** | |
| 18) | конечные поля |
| 19) | многочлены |
| 20) | поля из *pn* элементов |
| 21) | подгруппы |
| 22) | подполя и расширения полей |
| 23) | характеристика поля |
| 24) | лемма о степени суммы и разности |
| 25) | мультипликативная группа |
| 26) | функция "след" |
| **Блочные криптосистемы** | |
| 27) | блочно-итерационные криптосистемы |
| 28) | представления двоичных слов |
| 29) | SP-криптосистемы |
| 30) | τ-инволютивные подстановки |
| 31) | криптосистемы Фейстеля |
| **AES** | |
| 32) | AES |
| 33) | инверсные *S*-блоки |

|  |  |
| --- | --- |
| **Атака "грубой силой"** | |
| 34) | базовая атака |
| 35) | простые соотношения |
| 36) | баланс "время – память" |
| **Разностная атака** | |
| 37) | разностная атака |
| **Режимы шифрования** | |
| 38) | режим простой замены |
| 39) | режимы шифрования |
| 40) | имитозащита |
| **Поточные криптосистемы** | |
| 41) | поточные криптосистемы |
| 42) | конечные автоматы |
| 43) | РСЛОС |
| 44) | РСЛОС и функция "след" |
| 45) | период л.р.п. |
| 46) | порядок многочлена |
| 47) | постулаты Голомба |
| 48) | генераторы на базе РСЛОС |
| КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ | |
| **Протокол Диффи – Хеллмана** | |
| 49) | протокол |
| 50) | "противник посередине" |
| 51) | реализация протокола |
| **Элементы теории сложности** | |
| 52) | вычислительные задачи |
| 53) | машина Тьюринга |
| 54) | разрешимые и неразрешимые задачи |
| 55) | ресурсы |
| 56) | вероятностные машины |
| 57) | алгоритмы Лас-Вегас и Монте-Карло |
| 58) | сложностные классы |
| 59) | язык *PRIMES* |
| **Односторониие функции** | |
| 60) | односторонние функции |
| 61) | функции с лазейкой |
| 62) | шифрование с открытым ключом |
| 63) | системы ЭЦП |
| **Инфраструктура открытых ключей** | |
| 64) | сертификаты открытых ключей |
| 65) | инфраструктура открытых ключей |
| 66) | инфраструктура РБ |

|  |  |
| --- | --- |
| **RSA** | |
| 67) | криптосистема RSA |
| 68) | RSA и факторизация |
| **Реализация RSA** | |
| 69) | арифметика больших чисел |
| 70) | алгоритм Евклида |
| 71) | расширенный алгоритм Евклида |
| 72) | возведение в степень |
| 73) | китайская система сравнений |
| 74) | оптимизация RSA |
| **Генерация простых** | |
| 75) | генерация простых |
| 76) | распределение простых |
| 77) | тест Ферма |
| 78) | тест Рабина – Миллера |
| 79) | построение простых |
| **Функции хэширования** | |
| 80) | определение и использование |
| 81) | задачи криптоанализа |
| 82) | блочно-итерационные функции |
| 83) | конструкция Дамгарда |
| **Атака "дней рождения"** | |
| 84) | базовая атака |
| 85) | модифицированная атака |
| 86) | алгоритм Брента |
| **ЭЦП** | |
| 87) | ЭЦП ЭльГамаля |
| 88) | стойкость ЭЦП ЭльГамаля |
| 89) | модификации ЭЦП ЭльГамаля |
| 90) | метод Монтгомери |
| 91) | ЭЦП Шнорра |
| 92) | СТБ 1176.2-99 |
| **Факторизация** | |
| 93) | задача факторизации |
| 94) | алгоритм *p* – 1 |
| 95) | ρ-метод |
| 96) | выбор модуля RSA |
| **Дискретное логарифмирование** | |
| 97) | метод больших-малых шагов |
| 98) | ρ-метод |
| 99) | метод Поллига – Хеллмана |
| 100) | λ-метод |