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, ~~функция Кармайкла~~)
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 p^n 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)	т-инволютивные подстановки
31)	криптосистемы Фейстеля
AES	
32)	AES
33)	инверсные *S*-блоки
34)	~~стратегия «широкого следа»~~

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

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