**Олимпиада по криптографии « Энигма»**

**Задания I уровня состоит из следующих теоретических вопросов:**

***Количество вопросов – 24.***

***Количество баллов за 1 правильный ответ – 0,5.***

***Максимальный результат – 12 баллов.***

***Время выполнения – 35 минут.***

**1.1.** Блок информации, применяемый для защиты от навязывания ложной информации, зависящий от ключа и данных- это..

а) имитовставка

б) имитозащита

в) ЭЦП

г) МАС

**1.2.** В алгоритмах электронной подписи подписывание производится …

а) закрытым ключом отправителя

б) закрытым ключом получателя

в) открытым ключом получателя

г) открытым ключом отправителя

**1.3.** Как называется преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины с применением односторонних функций?

а) кодирование

б) сжатие

в) хеширование

г) шифрование

**1.4.** Алгоритм DES использует операцию:

а) сложения по модулю 216;

б) циклического сдвига битов;

в) подстановки с помощью S-блоков.

**1.5.** Алгоритмы DES и ГОСТ 28147—89 имеют структуру:

а) «квадрат»;

б) подстановочно-перестановочная сеть;

в) сеть Фейстеля.

**1.6.** Число раундов алгоритма AES определяется:

а) размером входного блока;

б) длиной ключа;

в) содержимым входного блока.

**1.7.** Длина ключа современного симметричного шифра должна составлять не менее ... бит для обеспечения практической стойкости:

а) 64;

б) 128;

в) 256.

**1.8.** Примером помехоустойчивого кодирования является:

а) XOR-гаммирование;

б) добавление битов четности в ключ алгоритма DES;

в) ASCII-кодировапие.

**1.9.** Модификация и подмена сообщений, передаваемых по каналу шифрованной связи, а также навязывание ложных сообщений называется:

а) помехами;

б) атакой на основе сбоев;

в) имитацией.

**1.10.** В случае применения асимметричной криптосистемы отправитель сообщения использует для шифрования:

а) свой открытый ключ;

б) свой личный ключ;

в) открытый ключ получателя;

г) личный ключ получателя.

**1.11.** Проверка подписи в асимметричных криптосистемах предполагает использование:

а) открытого ключа получателя;

б) личного ключа получателя;

в) открытого ключа отправителя;

г) личного ключа отправителя.

**1.12.** Основной проблемой практического использования асимметричных криптосистем является:

а) проблема распределения ключей;

б) невозможность аутентификации отправителя;

в) низкая производительность.

**1.13.** Криптосистема Диффи — Хеллмана является протоколом:

а) шифрования;

б) распределения ключей;

в) электронной подписи;

г) взаимной аутентификации.

**1.14.** Значение функции Эйлера от N определяется как ... натуральных чисел в ряду от 1 до N - 1, взаимно простых с N:

а) количество;

б) сумма;

в) среднее;

г) произведение.

**1.15.** Расширенный алгоритм Евклида используется в асимметричных криптосистемах для решения задачи:

а) факторизации числа;

б) нахождения числа, обратного заданному по модулю;

в) быстрого возведения в степень по модулю.

**1.16.** Безопасность криптосистемы RSA основана на вычислительной сложности задачи ... больших чисел:

а) дискретного логарифмирования;

б) факторизации;

в) вычисления степени по модулю.

**1.17.** Безопасность криптосистемы ... базируется на вычислительной сложности задачи дискретного логарифмирования:

а) Блюма — Гольдвассер;

б) RSA;

в) Эль-Гамаля.

**1.18.** Для обеспечения практической стойкости длина ключа криптосистемы RSA должна быть не менее:

а) 1024 бит;

б) 128 бит;

в) 512 бит.

**1.19.** Хэш-функциями называются ... функции, сопоставляющие тексту произвольной длины число фиксированной длины:

а) взаимно-однозначные;

б) односторонние;

в) односторонние с лазейкой.

**1.20.** Хэш-функция ... в настоящее время не рекомендована для использования, поскольку для нее найдены коллизии, которые могут быть эксплуатированы на практике для создания поддельных цифровых сертификатов:

а) SHA-1;

б) SHA-2;

в) MD5;

г) Кессак;

д) ГОСТ 34.11-2012.

**1.21.** Алгоритм RSA генерирует … в качестве цифровой подписи сообщения:

а) пару чисел;

б) новое сообщение двойной длины;

в) одно число.

**1.22.** Цифровая подпись по алгоритму ... является детерминированной:

а) DSA;

б) RSA;

в) Эль-Гамаля.

**1.23.** Протокол электронных денег базируется на использовании ... цифровой подписи:

а) групповой;

б) слепой;

в) неотвергаемой.

**1.24.**  Протоколом защищенного обмена информацией, действующем на сетевом уровне архитектуры взаимодействия открытых систем, является протокол:

а) IPSec;

б) SSL/TLS;

в) S/MIME.

**Задания II уровня состоит из следующих практических задач:**

***Количество задач – 7.***

***Количество баллов за правильный ответ – 2.***

***Максимальный результат – 14 баллов.***

***Время выполнения –45 минут.***

**Практическая задача 2.1:**

Определить секретный ключ шифрования с применением алгоритма Диффи-Хелмана. Вводные данные У=5; Р=23; Х(Алисы)=5; Х(Боба)=7. Ответ в числовой форме.

**Практическая задача 2.2:**

С помощью алгоритма RSA дешифрировать шифрограмму «5, 10, 22, 6, 12, 21, 15, 27, 30, 31, 10, 12» закрытым ключом (3, 33). Алфавит состоит из 33 букв.

**Практическая задача 2.3:**

Вычислить с применением алгоритма RSA для формирования пары открытого\закрытого ключей значения n, m, d.

Алгоритм RSA p=5, q=11, e=7

Ввод ответов в числовой форме через пробел, например, при n=15, m=10, d=12, в ответ ввести 15 10 12

**Практическая задача 2.4:**

Определите количество возможных вариантов замены знаков в сообщении из символов равных ответу из Практической задачи1 .Алфавит сообщения - английский прописной(26 символов)

**Практическая задача 2.5:**

Для шифра Эль-Гамаля с заданными параметрами p=19, g=2, х=5, k=7 найти недостающие параметры и описать процесс передачи сообщения m=5 пользователю В.

**Практическая задача 2.6:**

Сообщество пользователей ГОСТа 34.10-2012 имеют общие параметры q=11, p=67. Вычислить открытый ключ (y) и построить подпись для сообщения m при следующих секретных параметрах 𝑑=5, h=m=5, k=9

**Практическая задача 2.7:**

Для указанных открытых ключей (y) пользователей системы Эль-Гамаля с общими параметрами p=23, g=5 проверить подлинность подписанных сообщений: y=11: [10,15,3]

**Задания III уровня состоит из следующих практических задач:**

***Количество задач –4 .***

***Количество баллов за правильный ответ – 1.***

***Максимальный результат – 4 балла.***

***Время выполнения – 10 минут.***

**Практическое задание 3.1**

Извлечь изображение с помощью программы Filigrana используя пароль полученный в практическом задании 2.2(пароль вводить Caps Lock с пробелом) и, записать полученный текст с картинки в бланк ответов.

**Практическое задание 3.2**

С помощью программы LAB\_RAB расшифровать сообщение «Ц!d!gя!pъю!f5!kъ!n!f!g!d!gшээ» с помощью метода замены, используя ключ из практического задания 2.1, записать полученное сообщение в бланк с ответами.

**Практическое задание 3**

С помощью программы LAB\_RAB расшифровать сообщение «\_5,@E:53Ks=<;B>A6<3G4R» с помощью метода гаммирования, используя ключ (названия протокола используемого для обеспечения безопасной передачи данных по протоколу HTTP), записать полученное сообщение в бланк с ответами.

**Практическое задание 4**

Извлечь изображение с помощью программы Filigrana используя пароль полученный в практическом задании 3.1(пароль вводить Caps Lock с пробелом) и, записать полученный текст с картинки в бланк ответов.