Криптология

1. Криптосистема Рабина – частный случай криптографической системы RSA при $e=2$, $d=2^{-1}$, позволяет реализовать шифрование и электронную цифровую подпись. Стойкость системы основывается на сложности решения квадратичных сравнений. Схема электронной цифровой подписи заключается в следующем: если m – сообщение, то подписью s является решение сравнения $m \equiv s^2 \bmod n$, где $n = pq$ – произведение больших простых чисел (p,q – секретный ключ, n – открытый ключ). Пусть абонент А отправляет подписанные сообщения абоненту Б. Предложите способ, с помощью которого абонент А может скрывать информацию в открытом ключе n при использовании указанной схемы. Сколько сообщений потребуется отправить, чтобы скрыто передать 4096 бит информации, если n – 2048-битное число, и пара открытый/секретный ключ для каждого сообщения выбирается заново?

2. При каких условиях на числа a, b, m функцию
$$f(\gamma,x)=(a\gamma+bx) \bmod m,$$
где a, b – элементы кольца вычетов по модулю m, m – натуральное, можно использовать для шифрования? При каких условиях алгоритмы шифрования и расшифрования будут одинаковы?

3. DESX – симметричный блочный шифр, созданный Роном Ривестом в 1984 году на основе алгоритма DES с целью устранения его главного недостатка – малой длины ключа. Алгоритм зашифрования DESX – $K_2 \oplus E_K\left(M \oplus K_1\right)$, где K_1 и K_2 – фрагменты ключа, E_K – подстановка алгоритма DES на ключе K.

   Оцените трудоемкость нахождения ключа методом согласования при использовании алгоритма шифрования DESX при независимом выборе K_1, K_2, K.

4. Для функционирования симметричных блочных шифров в режимах шифрования CBC (сцепление блоков шифртекста) и CFB (гаммирование с обратной связью по шифртексту) необходимо использование вектора инициализации IV, также называемого синхропосылкой. Вектор инициализации должен быть известен отправителю и получателю.

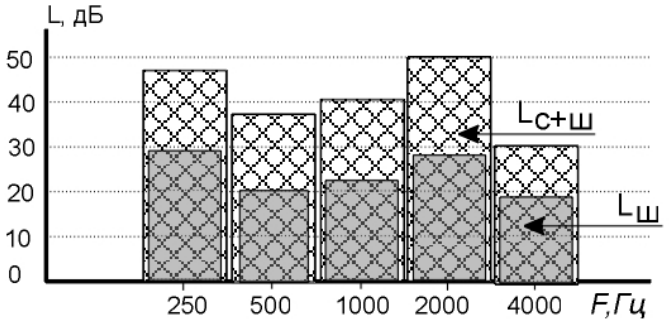
   Является ли безопасным использование в качестве вектора инициализации последнего блока шифртекста, полученного при шифровании предыдущего сообщения (при шифровании сообщений на одном ключе)? Почему?

5. Вам известны открытые параметры криптосистемы RSA: $n=75726223$, $e=42791935$, а также пара открытый текст $M=2$ и шифртекст $C=13104610$.

   Определите секретную экспоненту d.

Техническая защита информации

1. Результаты измерений за ограждающей конструкцией представлены на рисунке. Как изменится расчетное значение словесной разборчивости речи, если уровень тестового акустического сигнала в каждой октаве увеличить в два раза.



2. В ходе проведения измерений в канале акустоэлектрического преобразования получены следующие результаты:

I	Частота, fi, Гц	Измеренное напряжение сигнала+шума,Uс+ш,1дБ	Измеренное напряжение шума,Uш, i дБ
1	275	0	0
2	525	3	4
3	1025	2	2
4	2025	-1	-1
5	4025	-3	-2

После уменьшения полосы пропускания(□f) в 4 раза ,были получены новые результаты:

I	Частота, fi, Гц	Измеренное напряжение сигнала+шума,Uс+ш,1дБ	Измеренное напряжение шума,Uш, i дБ
1	275	-6	-5
2	525	-3	-3
3	1025	-4	-3
4	2025	-7	-6
5	4025	-9	-9

Как изменится расчетное значение словесной разборчивости речи на выходных контактах технического средства после уменьшения полосы пропускания анализатора спектра в четыре раза (уменьшится, увеличится, или останется без изменений)?

3. В ходе проведения измерений в акустоэлектромагнитном канале утечки информации в пятой октаве были получены следующие результаты:
-измеренное звуковое давление L=93дБ;
-напряжение «сигнал+шум» на выходе электрической антенны Uс+ш=6дБ;
-напряжение шума на выходе электрической антенны Uш=7дБ;
Рассчитать напряженность электрического поля информативного сигнала, приведенного к нормированному звуковому давлению Lн=53дБ на границе контролируемой зоны, если:
-коэффициент затухания Кз=5;
-калибровочный коэффициент антенны Кант=26 дБ относительно 1/м.

4. Во сколько раз ослабнет электромагнитный сигнал по стандартному закону затухания от точки проведения измерения до 6 м, если граница ближней зоны 2 м?

Практический тур (прикладная информатика)

Задача A. DLOG [20 баллов]

Найдите значение переменной $flag (32 символа хекса) в следующем php-скрипте, если известно, что результат работы скрипта равен
108999149936443723253212603538225611 93.

Практический тур (безопасность веб-приложений)

Задача B. Shader Crackme [15 баллов]

Найдите значения двух аргументов командной строки, которые необходимо передать программе, (копия) для показа сообщения об успешном прохождении задания. Найденные значения запишите через пробел и отправьте на проверку через форму ниже.

Задача C. Взломай меня [10 баллов]

Crackme.exe (x32), Crackme.exe (x64). Сгенерируйте серийный номер для своего логина и отправьте ответ на проверку в формате логин:серийный номер без пробелов.

Задача D. Забытый сервер 1 [10 баллов]

Ответ на задачу хранится в одной из баз данных забытого сервера. Найдите уязвимость на сайте и прочитайте с ее помощью ответ. Ответ состоит из 32 цифр и букв латинского алфавита.

Задача E. Забытый сервер 2 [10 баллов]

Ответ на задачу хранится в одном из файлов на сервере. Найдите уязвимость на сайте и прочитайте с ее помощью файл. Ответ состоит из 32 цифр и букв латинского алфавита.

Задача F. Зараженный компьютер [10 баллов]

Найдите на зараженном компьютере 5 вредоносных программ. В каждой из программ или около нее находится флаг. Образ зараженной виртуальной машины находится на вашем компьютере. Каждый флаг состоит из 32 цифр и букв латинского алфавита. За каждый найденный флаг начисляется 2 балла. Ответ в виде текстового файла, содержащего найденные кодовые слова (1 слово на строке), отправьте на проверку через форму ниже.

Задача G. Зашифрованные файлы [15 баллов]

В архиве содержится несколько файлов. Расшифруйте каждый файл и ответ в виде текстового файла, содержащего расшифрованные слова (1 слово на строке), отправьте на проверку через форму ниже. За каждое найденное слово начисляется 3 балла.

Задача H. Зашифрованная программа [10 баллов]

Найдите пароль для программы