Теоретический тур

РАЗДЕЛ №1: 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.

РАЗДЕЛ №2: Безопасность информационных технологий

№	Вопрос	Вариант ответа	
1.	Какой из перечисленных ниже способов управления рисками является наиболее нежелательным?	a)	принятие риска
		b)	уменьшение риска
		c)	передача риска
		d)	отказ от риска
2.	Какая сетевая топология представлена в архитектуре Token Ring?	a)	физически представляет звезду, а логически – кольцо
		b)	физически представляет кольцо, а логически – звезду
		c)	физически представляет кольцо, и логически – кольцо
		d)	физически представляет кольцо, а логически – ячеистую топологию
3.	Какой вид проверок наиболее эффективен для выявления программных закладок?	a)	антивирусные проверки
		b)	фаззинг-тестирование
		c)	специальные проверки и специальные исследования
		d)	ревизия исходного кода
4.	Чему равна длина блока DES?	a)	8 байт
		b)	32 байт
		c)	64 байт
		d)	16 байт
5.	Какой сетевой пакет представляет собой сегмент данных?	a)	ARP - пакет
		b)	IP - пакет
		c)	TCP - пакет
		d)	UDP – пакет
6.	О каком виде атаки идет речь, когда субъект на высоком уровне безопасности записывает данные в определенную область хранения информации, которую читает субъект на низком уровне безопасности?	a)	атака посредством скрытых каналов по уровню представления данных
		b)	атака «человек посередине»
		c)	атака посредством скрытых каналов по памяти
		d)	атака посредством скрытых каналов по времени
7.	Для защиты секретной черной жемчужины капитан Джек Воробей использует одно волшебное место. Какому принципу разграничения доступа должно соответствовать это место?	a)	«песочнице»
		b)	ролевому принципу
		c)	мандатному принципу
		d)	дискреционному принципу
8.	Какой протокол целесообразно использовать для передачи потокового аудио, если допустимы потери сетевого трафика?	a)	ICMP
		b)	IP
		c)	TCP
		d)	UDP
9.	Что используется для создания цифровой подписи?	a)	закрытый ключ отправителя
		b)	закрытый и открытый ключи отправителя
		c)	общий секретный ключ отправителя и получателя
		d)	открытый ключ отправителя

10.	В случае, если биометрическое средство настроено в очень чувствительном режиме, какая из характеристик преобладает (основная гипотеза – предоставляющий биометрию не является легальным пользователем системы)?	a)	ошибка 1-го рода
		b)	ошибка 2-го рода
		c)	ошибка 3-го рода
		d)	крайне чувствительному режиму свойственны ошибки всех родов
11.	Отметьте слово, которое в тайном письме Цезаря соответствовало имени близкой его сердцу египетской царицы?	a)	opatracle
		b)	tracleopa
		c)	fohrsdwud
		d)	ziblmxqox
12.	Сетевая инфраструктура университета реализована много лет назад и из-за периодических сбоев ожидает кардинальной модернизации в следующем году. Какой AAA-протокол предпочтительнее использовать в настоящее время для реализации централизованного управления безопасным доступом?	a)	NTLN v/2
		b)	Kerberos V5
		c)	RADIUS
		d)	TACACS+
13.	Оборудование инновационного технопарка оценивается в 1 000 000 $. Согласно заявлению материально-технической службы, два раза в неделю фиксируется факт пропажи. По оценке экспертов, недобропорядочный сотрудник в случае удачи способен вынести до 0,1% оборудования. Выберите максимальное значение ALE (Annualized Loss Expectancy – ожидаемые среднегодовые потери):	a)	10
		b)	285
		c)	28500
		d)	104 000
14.	Трех ученых в Сколково попросили назвать какие-либо существенные классы методов шифрования. Первый ответил: книжный шкаф и одноразовый блокнот. Второй: перестановочные, подстановочные, блочные, поточные. Третий: асимметричные и симметричные. Сколько ученых ошиблось с ответом?	a)	1
		b)	2
		c)	3
		d)	все ответили правильно
15.	В какое время считается, что восстановление после сбоев закончено?	a)	система полностью возобновила работу на альтернативной площадке
		b)	система полностью возобновила работу на главной площадке
		c)	критически важные подсистемы функционируют на главной площадке
		d)	издан приказ, где учтены ошибки и перечислены виновные «торжества»

16.	Буратино отправляет Мальвине романтическое письмо, в котором указано, где он спрятал золотой ключик. Лиса Алиса с Котом Базилио перехватывают его, но вместо текста видят картинку с субтропическими листопадным фикусом. Что применил Буратино?	a)	визуальное шифрование
		b)	кодирование
		c)	стеганографию
		d)	социальную атаку
17.	Полковник Сандерс приказал менеджерам московского и якутского филиалов иметь специально разработанный им ключ шифрования для взаимодействия между ресторанами полезного и здорового питания через Интернет. Как называется технология, которую он применяет?	a)	закрытые облачные вычисления
		b)	симметричное шифрование
		c)	шифрование с открытым ключом
		d)	кодирование интернет-вещей
18.	Что значит «черная дыра» в сетевой безопасности?	a)	разновидность backdoor
		b)	разновидность honeypot
		c)	сервер darknet
		d)	уязвимость zero day
19.	Для удобства капитан Врунгель установил программно-аппаратный комплекс «iЭхолот» на камбуз и хочет подключиться к серверу Мосводоканала через ssh, но у него не получается. Оказывается, на сервере Мосводоканала все порты по умолчанию закрыты. Какой порт нужно открыть капитану для подключения?	a)	22
		b)	23
		c)	8080
		d)	443
20.	Али-Баба и 40 разбойников решили организовать безопасное взаимодействие каждого с каждым при помощи симметричного шифрования. Сколько ключей им потребуется?	a)	41
		b)	82
		c)	820
		d)	2199023255552

Практический тур

Задача A. DLOG

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

Задача B. Shader Crackme

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

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

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

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

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

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

Найдите пароль для программы