

Всероссийская олимпиада студентов «Я – профессионал»

задания заключительного (очного) теоретического этапа
по направлению

**«Безопасность информационных систем и технологий
критически важных объектов»**

Категория участия: «Бакалавриат»
(для поступающих в магистратуру)

Вариант № 1

Номер задания	Задание	Макс. кол-во баллов						
Раздел 1. «Основы информационной безопасности»								
1.	<p>Задан алгоритм шифрования $C_i \equiv (3M_i + 8) \pmod{26}$ сообщений на английском языке, где M_i – численное представление i-ой буквы исходного английского текста (А - 0, В - 1, С - 2, D - 3, ..., Z - 25), C_i - численное представление i-ой буквы шифртекста. Вычислить алгоритм расшифрования $M_i \equiv (xC_i + y) \pmod{26}$, где $x, y \in \{0, 1, \dots, 25\}$. В ответе записать ключ расшифрования – пару (x, y). (Значения вводятся через запятую).</p> <p>Ответ: 9, 6.</p> <p>$C_i \equiv (3M_i + 8) \pmod{26} \leftrightarrow 3M_i \equiv (C_i - 8) \pmod{26} \leftrightarrow 3M_i \equiv (C_i + 18) \pmod{26} \leftrightarrow M_i \equiv (3^{-1}C_i + 6) \pmod{26} \leftrightarrow M_i \equiv (9C_i + 6) \pmod{26}$</p>	2						
2.	<p>Заданы три четырехразрядных регистра сдвига с линейными обратными связями (РСЛОС), уравнения работы которых имеют вид:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td align="center" style="width: 33%;">1</td> <td style="width: 33%;"> $q_1(t+1) = q_4(t)$ $q_2(t+1) = q_1(t) + q_4(t)$ $q_3(t+1) = q_2(t) + q_4(t)$ $q_4(t+1) = q_3(t) + q_4(t)$ </td> <td align="center" style="width: 33%;">2</td> <td style="width: 33%;"> $q_1(t+1) = q_4(t)$ $q_2(t+1) = q_1(t) + q_4(t)$ $q_3(t+1) = q_2(t)$ $q_4(t+1) = q_3(t)$ </td> <td align="center" style="width: 33%;">3</td> <td style="width: 33%;"> $q_1(t+1) = q_4(t)$ $q_2(t+1) = q_1(t)$ $q_3(t+1) = q_2(t)$ $q_4(t+1) = q_3(t) + q_4(t)$ </td> </tr> </table> <p>где $q_i(t+1)$ и $q_i(t)$ – содержимое i-го разряда РСЛОС, а сложение выполняется по модулю два.</p> <p>Какие РСЛОС могут использоваться в качестве генераторов ненулевых элементов конечного поля $GF(2^4)$:</p> <p>А. Только РСЛОС 2 и 3. В. Только РСЛОС 2. С. Только РСЛОС 3. Д. Только РСЛОС 1. Е. Все три.</p> <p>В ответе указать правильный вариант.</p>	1	$q_1(t+1) = q_4(t)$ $q_2(t+1) = q_1(t) + q_4(t)$ $q_3(t+1) = q_2(t) + q_4(t)$ $q_4(t+1) = q_3(t) + q_4(t)$	2	$q_1(t+1) = q_4(t)$ $q_2(t+1) = q_1(t) + q_4(t)$ $q_3(t+1) = q_2(t)$ $q_4(t+1) = q_3(t)$	3	$q_1(t+1) = q_4(t)$ $q_2(t+1) = q_1(t)$ $q_3(t+1) = q_2(t)$ $q_4(t+1) = q_3(t) + q_4(t)$	4
1	$q_1(t+1) = q_4(t)$ $q_2(t+1) = q_1(t) + q_4(t)$ $q_3(t+1) = q_2(t) + q_4(t)$ $q_4(t+1) = q_3(t) + q_4(t)$	2	$q_1(t+1) = q_4(t)$ $q_2(t+1) = q_1(t) + q_4(t)$ $q_3(t+1) = q_2(t)$ $q_4(t+1) = q_3(t)$	3	$q_1(t+1) = q_4(t)$ $q_2(t+1) = q_1(t)$ $q_3(t+1) = q_2(t)$ $q_4(t+1) = q_3(t) + q_4(t)$			

	<p>Ответ: А. Только РСЛОС 2 и 3 имеют диаграмму переключений, состоящую из двух кодов колец длиной 15 и 1.</p>	
3.	<p>Какой одной командой можно заменить фрагмент кода на Ассемблере (система команд x86, стандартная нотация Intel):</p> <pre> mov ax, OFFSET RetAddr push ax jmp MyProc RetAddr: </pre> <p>Ответ: call MyProc.</p>	5
4.	<p>Укажите ложные утверждения.</p> <p>А. В качественной криптографической хеш-функции не должно быть коллизий.</p> <p>Б. В случае использования качественной криптографической хеш-функции минимальное изменение на ее входе должно приводить в среднем к изменению 50% бит хеш-образа.</p> <p>В. В случае использования качественной криптографической хеш-функции любое изменение на ее входе должно приводить в среднем к изменению 50% бит хеш-образа.</p> <p>Г. При использовании качественной криптографической хеш-функции задача нахождения коллизий вычислительно неразрешима.</p> <p>В ответе указать все правильные варианты ответа.</p> <p>Ответ: А.</p>	4
Раздел 2. «Криптографические методы защиты информации»		
5.	<p>Определите количество слабых ключей в алгоритме шифрования «Магма» (ГОСТ Р 34.12-2015).</p>	5
6.	<p>Известно, что после шифрования сообщений "11" и "9" с помощью алгоритма RSA с одинаковым ключом и 8-битным модулем были получены соответственно шифртексты "7" и "16". Чему равен результат зашифрования на том же ключе сообщения "99"?</p>	5
7.	<p>Известен отрезок линейной рекуррентной последовательности, линейная сложность которой равна 6: 100000100001. Определите закон рекурсии.</p>	5
	Решение	

ЭКЗАМЕНАЦИОННЫЙ ЛИСТ

Дисциплина _____ Дата экзамена _____
 Фамилия студента _____ № группы _____
 № экзаменационного билета _____ Время выдачи билета _____ ч. _____ мин.
 Время начала ответа _____ ч. _____ мин. Оценка _____
 Подпись экзаменатора _____

*Баскальварт.
 Вариант N 1.*

15

$k = 256 \text{ бит}$

$K = (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$

$q_1 = k_1$	$q_9 = k_1$	$q_{17} = k_1$	$q_{25} = k_1$
$q_2 = k_2$	$q_{10} = k_2$	$q_{18} = k_2$	$q_{26} = k_2$
$q_3 = k_3$	$q_{11} = k_3$	$q_{19} = k_3$	$q_{27} = k_3$
$q_4 = k_4$	$q_{12} = k_4$	$q_{20} = k_4$	$q_{28} = k_4$
$q_5 = k_5$	$q_{13} = k_5$	$q_{21} = k_5$	$q_{29} = k_5$
$q_6 = k_6$	$q_{14} = k_6$	$q_{22} = k_6$	$q_{30} = k_6$
$q_7 = k_7$	$q_{15} = k_7$	$q_{23} = k_7$	$q_{31} = k_7$
$q_8 = k_8$	$q_{16} = k_8$	$q_{24} = k_8$	$q_{32} = k_8$

Ключ k - состоит $\Rightarrow k_1 = k_2 = k_3 = k_4 = k_5 = k_6 = k_7 = k_8$

Количество битов ключа: $\underline{2^{32}}$

16

$E(11) = 7$

$E(9) = 16$

$E(11, 9) = 7 \cdot 16 = \underline{112}$

\uparrow в силу теоремы RSA

17

По алгоритму Берлекэмпа - найти обратный
 элемент модулю: $\underline{F_{116} = x \cdot 2 \cdot x_{112}}$

Раздел 3. «Безопасность информационных технологий и техническая защита информации»

8.

Найдите уязвимость в программном коде и дайте ей объяснение.
 BOOL WINAPI _exportSEVENZ_OpenArchive(constchar *Name, int *Type)
 {
 Traverser *t = new Traverser(Name);
 if (!t->Valid())
 {
 return FALSE;
 delete t;
 }
 delete s_selected_traverser;
 s_selected_traverser = t;

6

	<pre>return TRUE; } Решение В приведенном примере происходит утечка данных из памяти. return FALSE; delete t;</pre> <p>Для устранения ошибки необходимо поменять местами вызов операторов «return» и «delete».</p> <p>Ответ: Возможна утечка из памяти. Для устранения ошибки необходимо поменять местами вызов операторов «return» и «delete».</p>	
<p>9.</p>	<p>В ходе проведения лабораторных измерений в низкочастотном акустоэлектрическом канале утечки информации (КУИ) без воздействия на техническое средство тональным акустическим сигналом напряжение шума на выходных контактах технического средства (приемника) в полосе пропускания анализатора спектра $\Delta F = 6$ Гц составляет $U_{ш} = 12$ мкВ.</p> <p>Необходимо: рассчитать напряжение шума в октавной полосе $U_{ш.окт}$ шириной $\Delta F_{окт} = 1,2$ кГц. Предполагается, что спектральная плотность мощности шума является равномерной.</p> <p>Решение. Напряжение шума в октавной полосе рассчитывается следующим образом:</p> $U_{ш.окт_i} = U_{ш_{np}} \cdot \sqrt{\frac{\Delta F_{окт_i}}{\Delta F_{np}}},$ <p>тогда $\Delta F_{окт}/\Delta F = \left(\frac{U_{ш.окт}}{U_{ш}}\right)^2$;</p> $U_{ш.окт} = U_{ш} \cdot \sqrt{\frac{\Delta F_{окт}}{\Delta F}} = 12 \cdot 10^{-6} \cdot \sqrt{\frac{1200}{6}} = 0,0001697 \text{ В} = 169,7 \text{ мкВ.}$ <p>Ответ: Напряжение шума в октавной полосе $U_{ш.окт} = 169,7$ мкВ.</p>	<p>6</p>
<p>10.</p>	<p>Проводник телефонного канала связи способен равномерно пропускать колебания в интервале от 0 до 30 кГц. Известно то, что: на более высоких частотах коэффициент передачи канала (по мощности) не изменяется и равен нулю; в качестве защиты телефонного канала применено средство (активной) защиты информации - генератор белого шума (гауссовский). В результате применения генератора шума в канале связи присутствует белый шум. Отношение $\left(\frac{P_c}{P_{ш}}\right)$ средней мощности полезного сигнала к средней мощности шума в канале связи составило 40 дБ.</p> <p>Необходимо: вычислить пропускную способность C канала связи.</p> <p>Подсказки:</p> <p>1) Пропускная способность канала связи определяется по формуле (16.72) из учебника Баскакова С.И. РТЦиС, 1983:</p> $C = \frac{\log_2 M}{T} = \Pi \cdot \log_2 \left(1 + \frac{P_c}{P_{ш}}\right).$ <p>2) Это тот случай (условие задачи), когда мощность сигнала в разы превышает мощность шума.</p> <p>Решение. "Белый" шум – это шум с постоянной спектральной плотностью в</p>	<p>8</p>

	<p>речевом диапазоне частот. Так как пропускная способность определяется по формуле (16.72, учебник Баскакова С.И. РТЦиС, 1983), то: для расчета</p> $C = \frac{\log_2 M}{T} = \Pi \cdot \log_2 \left(1 + \frac{P_c}{P_{ш}}\right)$ <p>необходимо найти все величины.</p> <p>1) из условия задачи в частотной области ширина полосы пропускания Π равна $3 \cdot 10^4$ Гц;</p> <p>2) для удобства вычисления выполним необходимое преобразование, выражение в скобках выразим через X, тогда $\log_2 x = \frac{\lg x}{\lg 2} = \frac{1}{\lg 2} \cdot \lg x = 3,32 \cdot \lg x$ (данный пункт упрощает решение, но он не обязателен);</p> <p>3) выполним перевод дБ в разы: так как 40 дБ это отношение средней мощности полезного сигнала к средней мощности шума канале связи $\Rightarrow 40 \text{ дБ} = \frac{P_1}{P_0}$, а $\frac{P_1}{P_0} = \sqrt[10]{10^{\text{дБ}}} = 10^{\frac{\text{дБ}}{10}} = 10^4$, где дБ по условию 40 дБ.</p> <p>Следовательно $C = \Pi \cdot \log_2 \left(1 + \frac{P_c}{P_{ш}}\right) = 3 \cdot 10^4 \cdot 3,32 \cdot \lg(1+10^4) \approx 398,4$ Кбит/с.</p> <p>Ответ: $C \approx 398,4$ Кбит/с.</p>	
--	---	--

Вариант № 2

Номер задания	Задание	Макс. кол-во баллов
Раздел 1. «Основы информационной безопасности»		
1.	<p>Задан алгоритм шифрования $C_i \equiv (2M_i + 5) \pmod{26}$ сообщений на английском языке, где M_i – численное представление i-ой буквы исходного английского текста (А - 0, В - 1, С - 2, D - 3, ..., Z - 25), C_i – численное представление i-ой буквы шифртекста. Вычислить алгоритм расшифрования $M_i \equiv (xC_i + y) \pmod{26}$, где $x, y \in \{0, 1, \dots, 25\}$. В ответе записать ключ расшифрования – пару (x, y). (Значения вводятся через запятую).</p> <p>Ответ: Ø.</p> <p>$C_i \equiv (2M_i + 5) \pmod{26} \leftrightarrow 2M_i \equiv (C_i - 5) \pmod{26} \leftrightarrow 2M_i \equiv (C_i + 21) \pmod{26} \leftrightarrow M_i \equiv (2^{-1}C_i + 2^{-1} \times 21) \pmod{26}$, $2^{-1} \pmod{26}$ не существует.</p>	2
2.	<p>Задан четырехразрядный регистра сдвига с линейными обратными связями (РСЛОС), уравнения работы которого имеет вид:</p> $\begin{aligned} q_1(t+1) &= q_4(t) \\ q_2(t+1) &= q_1(t) \\ q_3(t+1) &= q_2(t) \\ q_4(t+1) &= q_3(t) + q_4(t) \end{aligned}$ <p>где $q_i(t+1)$ и $q_i(t)$ – содержимое i-го разряда РСЛОС, а сложение выполняется по модулю два. Синтезировать на основе заданного РСЛОС устройство, диаграмма переключений которого состоит из одного кодового кольца длиной 16, включающего в себя все состояния устройства.</p> <p>В ответе привести уравнения работы синтезированного устройства.</p>	5

	<p>Ответ:</p> $q_1(t+1) = q_4(t)$ $q_2(t+1) = q_1(t)$ $q_3(t+1) = q_2(t)$ $q_4(t+1) = q_3(t) + q_4(t) + \bar{q}_1(t) \cdot \bar{q}_2(t) \cdot \bar{q}_4(t)$	
3.	<p>На чем основана стойкость криптосистем с открытым ключом?</p> <p>А. На секретности ключа зашифрования. Б. На секретности алгоритма расшифрования. В. На сложности решения некой математической задачи. Г. На секретности алгоритма зашифрования.</p> <p>В ответе указать все правильные варианты ответа. Ответ: В.</p>	3
4.	<p>Задача защиты программ от статического и динамического исследования решается путем использования технологии "изошренного" программирования, предполагающей экзотическую, имеющую необычный вид реализацию алгоритмов с использованием редких команд процессора или их нестандартных сочетаний; реализацию нескольких полностью эквивалентных вариантов одного и того же алгоритма, при каждом обращении к которому случайным образом выбирается один из вариантов его реализации и др. Используя эту технологию, разработать не менее трех эквивалентных реализаций команды <code>xchg ax,bx</code>. Размер эквивалентного кода не ограничивается.</p> <p>Ответ:</p> <pre> push ax xor ax, bx push cx push bx xor bx, ax mov cx, ax pop ax xor ax, bx mov ax, bx pop bx mov bx, cx pop cx </pre>	5
Раздел 2. «Криптографические методы защиты информации»		
5.	<p>Определите количество слабых ключей в алгоритме шифрования DES.</p>	5
6.	<p>Известно, что после шифрования сообщений "7" и "15" с помощью алгоритма RSA с одинаковым ключом и 8-битным модулем были получены соответственно шифртексты "11" и "19". Чему равен остаток от деления на 128 результата зашифрования на том же ключе сообщения "105"?</p>	5
7.	<p>Известен отрезок линейной рекуррентной последовательности, линейная сложность которой равна 5: 0111110001. Определите закон рекурсии.</p>	5
	Решение	

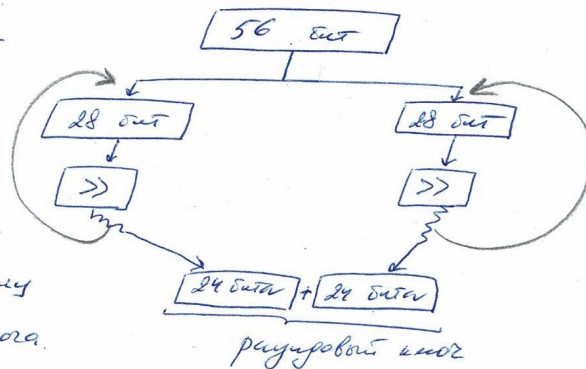
ЭКЗАМЕНАЦИОННЫЙ ЛИСТ

Дисциплина _____ Дата экзамена _____
 Фамилия студента _____ № группы _____
 № экзаменационного билета _____ Время выдачи билета _____ ч. _____ ми
 Время начала ответа _____ ч. _____ мин. Оценка _____
 Подпись экзаменатора _____

Бакалавриат
 Вариант № 2

№5 k - 56 бит

Ключ симметричный,
 если размер
 ко 28 бит
 количество состоит
 из чужих или своих
 ⇒ 4 своих ключа.



№6

$$E(7) = 11$$

$$E(15) = 19$$

$$E(7 \cdot 15) = 11 \cdot 19 = 209$$

↳ в силу особенностей RSA.

$$209 \bmod 128 = 101$$

№7

По алгоритму Беркеланда-Месса определяем
 закон рекурсии: $K_{i+5} = K_i \oplus K_{i+2}$.

Раздел 3. «Безопасность информационных технологий и техническая защита информации»

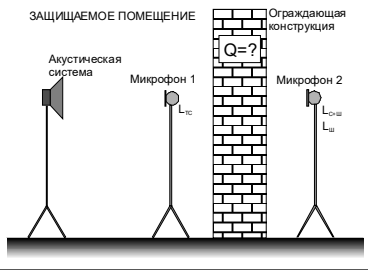
8.

Найдите уязвимость в программном коде и дайте ей объяснение.

```

void host_lookup(char *user_supplied_addr)
{
    struct hostent *hp;
    in_addr_t *addr;
    char hostname[64];
    in_addr_t inet_addr(const char *cp);
    /*routine that ensures user_supplied_addr is in the right format for
    conversion */ validate_addr_form(user_supplied_addr);
    addr = inet_addr(user_supplied_addr);
    hp = gethostbyaddr( addr, sizeof(struct in_addr), AF_INET);
    strcpy(hostname, hp->h_name);
    
```

6

	<p>} Решение В приведенном примере происходит выделение буфера под хранение переменной «hostname» размером 64 байт. В случае, если значение переменной «hostname» будет более 64 байт, произойдет переполнение буфера.</p> <p>Ответ: Возможно переполнение буфера. В случае, если значение переменной «hostname» будет более 64 байт произойдет переполнение буфера.</p>	
9.	 <p>При оценке защищенности речевой информации в помещении получены следующие результаты: Звуковое давление тестового акустического сигнала, измеренное микрофоном №1, составляет $L_{TC}=99$дБ. Звуковое давление сигнала и шума, измеренное микрофоном №2, составляет $L_{C+ш} = 59$дБ. При отключении тестового акустического сигнала звуковое давление шума, измеренное микрофоном №2, составляет $L_{ш} = 39$дБ. Необходимо: рассчитать звукоизоляцию Q ограждающей конструкции.</p> <p>Решение Вычисляем звуковое давление сигнала за ограждающей конструкцией Если $L_{C+ш} - L_{ш} > 10$дБ, то $L_C = L_{C+ш}$. Таким образом $L_C = 59$дБ. Звукоизоляция Q - это разница между тестовым сигналом и сигналом за пределами ограждающей конструкции Таким образом $Q = L_{TC} - L_C = 99 - 59 = 40$дБ.</p> <p>Ответ: $Q = 40$ дБ.</p>	6
10.	<p>Проводник телефонного канала связи способен равномерно пропускать колебания в интервале от 0 до 30 кГц. Известно то, что: на более высоких частотах коэффициент передачи канала (по мощности) не изменяется и равен нулю; в качестве защиты телефонного канала применено средство (активной) защиты информации – генератор белого шума (гауссовский). В результате применения генератора шума в канале связи присутствует белый шум. Отношение $\left(\frac{P_C}{P_{ш}}\right)$ средней мощности полезного сигнала к средней мощности шума канале составляет 1 дБ.</p> <p>Необходимо: вычислить пропускную способность C канала.</p> <p>Подсказки:</p> <p>1) Пропускная способность канала определяется по формуле (16.72) из учебника Баскакова С.И. РТЦиС, 1983: $C = \frac{\log_2 M}{T} = П \cdot \log_2 \left(1 + \frac{P_C}{P_{ш}}\right).$</p> <p>2) По условию задачи это тот случай, когда мощность сигнала и</p>	8

мощность шума равны.

Решение

"Белый" шум – это шум с постоянной спектральной плотностью в речевом диапазоне частот. Так как пропускная способность определяется по формуле (16.72, учебник Баскакова С.И. РТЦ и С, 1983), то: для расчета

$$C = \frac{\log_2 M}{T} = \Pi \cdot \log_2 \left(1 + \frac{P_c}{P_{ш}}\right)$$
 необходимо найти все величины.

1) из условия задачи в частотной области ширина полосы пропускания Π равна $3 \cdot 10^4$ Гц;

2) для удобства вычисления выполним необходимое преобразование выражение в скобках выразим через X , тогда $\log_2 x = \frac{\lg x}{\lg 2} = \frac{1}{\lg 2} \cdot$

$\lg x = 3,32 \cdot \lg x$ (данный пункт упрощает решение, но он **не обязателен**);

3) выполним перевод дБ в разы: так как 1 дБ это отношение средней мощности полезного сигнала к средней мощности шума канале =>

$$1 \text{ дБ} = \frac{P_1}{P_0}, \text{ а } \frac{P_1}{P_0} = \sqrt[10]{10^{\text{дБ}}} = 10^{\frac{\text{дБ}}{10}} = 10^{0,1} = 1, \text{ где дБ по условию } 1 \text{ дБ.}$$

$$\text{Следовательно } C = \Pi \cdot \log_2 \left(1 + \frac{P_c}{P_{ш}}\right) = 3 \cdot 10^4 \cdot 3,32 \cdot \lg(1 + 10^{0,1}) = 3 \cdot 10^4 \cdot 3,32 \cdot 1 \approx 35,2 \text{ Кбит/с.}$$

Ответ: $C \approx 35,2$ Кбит/с (значение для линии связи низкого качества).