Информационная безопасность
Решение открытого билета

1. Пароль состоит из 5 букв русского алфавита. При этом в системе хранится не сам пароль, а его ключ, который формируется по следующему принципу. Каждой букве алфавита ставится в соответствие определенное число (А —1, Б —2, В —3 и т. д.). Когда пользователь выбирает себе пароль, КЕПКА, то буквам пароля ставятся в соответствие следующие числа — К — 12, Е — 6, П — 17, К — 12, А — 1, а затем вычисляется следующая сумма — 12 + 6 + 17 + 12 + 1 = 48. Это число и есть ключ.

Будет ли такая система формирования ключа надежной? (*10 баллов*)

Решение:

Система не будет надежной. Например, если для указанного в задаче случая взять слово КККЕЕ, то для него сумма будет равна также 48 (12 + 12 + 12 + 6 + 6). То есть можно подобрать такое сочетание букв, что рассчитанная в результате сумма будет совпадать с искомой. Можно подобрать различные пары паролей, образующие коллизии, например, АБВГД и ББББГД, АЕЗНТ и БДИЛУ.

Ответ: Нет.

2. Перед группой хакеров стоит задача по выводу из строя компьютеров конкурирующей фирмы. Они создали вредоносное программное обеспечение, распространяющееся в сети. В силу особенностей разработки вирус при распространении с зараженного компьютера всегда поражает либо 4, либо 6 ещё не зараженных. В случае если такого количества незараженных компьютеров нет, то он не имеет возможности распространяться. В сети фирмы зарегистрировано 257 компьютеров. Возможно ли заражение всех компьютеров фирмы при условии, что изначально заражается один компьютер.

Если возможно, то приведите пример цепочки заражения. (*10 баллов*)

Решение:

Заражение возможно, если хотя бы одна из цепочек заражения может привести к полному заражению сети.

Рассмотрим возможные цепочки заражения. Изначально заражен 1 компьютер и не заражено 256.

1 этап заражения. Зараженный компьютер распространяет вирус либо на 4 компьютера, либо на 6 компьютеров. В результате возможно две ситуации: 5 зараженных и 252 не зараженных компьютера и 7 зараженных и 250 не зараженных компьютеров.

2 этап. Возьмем первую ситуацию. Так как незараженных компьютеров еще достаточно, каждый из зараженных будет распространять вирус. Возможны следующие ситуации:

- каждый из 5 компьютеров распространил вирус на 6 незараженных. Итого 35 компьютеров заражено, 222 остаются незараженными.

- один компьютер отправил вирус на 4 незараженных, каждый из остальных 4 компьютеров распространил вирус на 6 незараженных. Итого 33 компьютера заражено, 224 остаются незараженными.

…

- каждый из 5 компьютеров распространил вирус на 4 незараженных. Итого 25 компьютеров заражено, 232 остаются незараженными.

3 этап. Опять же для примера возьмем 1 ситуацию исхода предыдущего этапа.

Возможные исходы: все 35 компьютеров заражают по 6 (итого 245 зараженных, 12 незараженных), 34 по 6 и 1 по 4 (итого 243 зараженных и 14 незараженных) и так далее.

И снова обратимся к 1 ситуации, осталось 12 незараженных. Проверим, возможно ли их заражение на последнем этапе. Заразить 12 компьютеров могут вместе 3 зараженных, распространив вирус на 4 компьютера каждый, либо 2 заражённых, распространив вирус на 6. Это и будет пример цепочки заражения.

Ответ: заражение возможно.

3. Первокурсник Олег был крайне взволнован, когда его одногруппница Ирина выложила в соцсети подборку песен и картинок с загадочной подписью:

29

лкдкюеюжейк

Зная, что Ирина увлекается криптографией, помогите Олегу выяснить, что же написала девушка. (*15 баллов*)

Решение:

Из условий задачи понятно, что подпись зашифрована шифром Цезаря с ключом 29. Для расшифровки используем нумерованный алфавит из приложения. При расшифровке номер буквы в шифр-тексте сдвигается влево на размер ключа.

Составим таблицу дешифровки.

Шифр-текст	л	к	д	к	ю	е	ю	ж	е	й	к
Номер буквы в шифр-тексте	13	12	5	12	32	6	32	8	6	11	12
Ключ	29	29	29	29	29	29	29	29	29	29	29
Номер буквы исходного текста	17	16	9	16	3	10	3	12	10	15	16
Исходный текст	п	о	з	о	в	и	в	к	и	н	о

Ответ: позови в кино.

4. Дети играли в прятки, и мальчик Женя оказался закрытым в подвале. Он не мог открыть дверь изнутри, и стал внимательно осматривать помещение. Внезапно Женя увидел клочок бумаги, который завалился под старый запыленный шкаф. Мальчик прочитал написанное:

впоыиюяехтыбчвпжнпфж

На обратной стороне бумаги все буквы размыло, но можно было разобрать слова: «квадрат… шесть на пять … и/й …. е/ё… ь/ъ».

Возможно ли, что спасение сокрыто в этом послании?

Помогите Жене разгадать загадку. (*20 баллов*)

Решение:

По словам на обратной стороне бумаги можно понять, что речь идет о шифре «квадрат Полибия» с пояснением, что таблица шифрования состоит из 6 столбцов и 5 строк (также есть другие вариации шифра, с квадратом 6 на 6 и 5 на 5). Так как русский алфавит 33 символа (он не влезет в таблицу 6 на 5), в тексте дано пояснение, какие буквы необходимо объединить в одну ячейку матрицы шифрования. Составим матрицу шифрования.

	1	2	3	4	5	6
1	а	б	в	г	д	е/ё
2	ж	з	и/й	к	л	м
3	н	о	п	р	с	т
4	у	ф	х	ц	ч	ш
5	щ	ы	ь/ъ	э	ю	я

Составим таблицу координат зашифрованного текста. Первая строка – зашифрованный текст по буквам. Вторая и третья строки – номер столбца и номер строки буквы в матрице шифрования соответственно. Запишем в таблицу координаты букв зашифрованного текста.

	в	п	о	ы	и	ю	я	е	х	т	ы	б	ч	в	п	ж	н	п	ф	ж
столбец	3	3	2	2	3	5	6	6	3	6	2	2	5	3	3	1	1	3	2	1
строка	1	3	3	5	2	5	5	1	4	3	5	1	4	1	3	2	3	3	4	2

Выпишем координаты букв в виде столбец-строка по порядку в две строки. Например, для первых двух букв координаты будут выглядеть следующим образом: 31 33. Количество цифр(!) в каждой строке должно быть равно количеству букв в зашифрованной фразе.

31 33 23 25 32 55 65 61 34 63

25 21 54 31 33 12 13 33 24 12

Первая строка – первая координата буквы в исходной фразе – номер столбца. Вторая строка – вторая координата буквы в исходной фразе – номер строки.

Составим матрицу координат исходного текста и найдём новые значения в «квадрате Полибия»:

столбец	3	1	3	3	2	3	2	5	3	2	5	5	6	5	6	1	3	4	6	3
строка	2	5	2	1	5	4	3	1	3	3	1	2	1	3	3	3	2	4	1	2
	и	щ	и	в	ы	х	о	д	п	о	д	л	е	с	т	н	и	ц	е	й

Ответ: ищивыходподлестницей.

5. Юный супергерой Максим Пушкарев перехватил загадочное послание злодея, отправленное его сообщникам:

LSB

БОРИК ДЕРАР

«Теперь-то я знаю, когда они собираются ограбить банк!» – воскликнул Максим через некоторое время.

Извлеките информацию из перехваченного послания и узнайте, какие подробности о плане врага выяснил Максим. (*20 баллов*)

Решение:

Как догадался супергерой, тайное сообщение содержится внутри текста БОРИК ДЕРАР. При этом пометка LSB указывает, что сообщение скрыто в наименее значимых, т.е. младших, битах (least significant bits), а не в наиболее значимых, т.е. старших, битах (most significant bits, MSB) символов перехваченного текста.

Воспользовавшись в приложении таблицей 3, сопоставим перехваченные символы и соответствующие им двоичные коды: Б – 00001, О – 01110, Р – 10000, И – 01000, К – 01010, Д – 00100, Е – 00101, Р – 10000, А – 00000, Р – 10000.

Предположим, сообщение скрыто в одном младшем бите: Б – 0000<u>1</u>, О – 0111<u>0</u>, Р – 1000<u>0</u>, И – 0100<u>0</u>, К – 0101<u>0</u>, Д – 0010<u>0</u>, Е – 0010<u>1</u>, Р – 1000<u>0</u>, А – 0000<u>0</u>, Р – 1000<u>0</u>. Выпишем полученную последовательность: 1000001000. Поскольку двоичные коды представлены пятью битами, разделим полученную последовательность на отдельные последовательности длиной 5 битов: 10000, 01000. Сопоставим этим последовательностям соответствующие символы, согласно приложению: 10000 – Р, 01000 – И. Как видим, осмысленного текста не получилось.

Предположим, сообщение скрыто в двух младших битах: Б – 000<u>01</u>, О – 011<u>10</u>, Р – 100<u>00</u>, И – 010<u>00</u>, К – 010<u>10</u>, Д – 001<u>00</u>, Е – 001<u>01</u>, Р – 100<u>00</u>, А – 000<u>00</u>, Р – 100<u>00</u>. Выпишем полученную

последовательность: 01100000100001000000. Разделим полученную последовательность на отдельные последовательности длиной 5 битов и поставим им в соответствие буквы алфавита: 01100 – М, 00010 – В, 00010 – В, 00000 – А. Как видим, осмысленного текста снова не получилось.

Предположим, сообщение скрыто в трёх младших битах: Б – 00001, О – 01110, Р – 10000, И – 01000, К – 01010, Д – 00100, Е – 00101, Р – 10000, А – 00000, Р – 10000. Выпишем полученную последовательность: 00111000000001010010100000000. Разделим полученную последовательность на отдельные последовательности длиной 5 битов и поставим им в соответствие буквы алфавита: 00111 – З, 00000 – А, 00010 – В, 10010 – Т, 10000 – Р, 00000 – А. Получилось слово «завтра», которое является осмысленным и согласуется с исходной ситуацией, описанной в задании.

Ответ: завтра.

6. Сумма чисел равна 35. Три на пять будет пятнадцать. Зная это, и то, что длина Великой Китайской стены 21 196 километров, ответьте на следующий вопрос:

фпсрыпрвфмкхиеезиэеги? (*25 баллов*)

Решение:

По набору исходных данных (зашифрованный текст и набор цифр) понимаем, что это шифр Цезаря с непостоянным сдвигом или шифр Виженера.

Из цифр в тексте задания составим ключ шифрования: 35351521196.

Так как длина ключа меньше зашифрованного текста, то повторим ключ до достижения необходимой длины. Ключ для каждой буквы – цифра из ключа, стоящая под этой буквой. При расшифровке из номера буквы зашифрованного текста отнимаем ключ. Номер буквы соответствует нумерованному алфавиту из приложения.

Составим таблицу дешифровки.

Шифр-текст	ф	п	с	р	ы	п	р	в	ф	м	к	х	и	е	е	з	и	э	е	г	и
Номер буквы	22	17	19	18	29	17	18	3	22	14	12	23	10	6	6	9	10	31	6	4	10
Ключ	3	5	3	5	1	5	2	1	1	9	6	3	5	3	5	1	5	2	1	1	9
	19	12	16	13	28	12	16	2	21	5	6	20	5	3	1	8	5	29	5	3	1
	с	к	о	л	ь	к	о	б	у	д	е	т	д	в	а	ж	д	ы	д	в	а

Исходный вопрос: сколько будет дважды два?

Ответ: четыре.