Пермский край
2024-2025 учебный год

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ПО ТРУДУ (ТЕХНОЛОГИИ)
МУНИЦИПАЛЬНЫЙ ЭТАП
10-11 КЛАСС

ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ТЕОРЕТИЧЕСКИЙ ТУР

КЛЮЧИ

1. A, B, C, D, E

2. A, B, C, D

3. A

4.

1	2	3	4
B	A	C	D

5. D, C, B, E, A

6. D

7. C, E, F

8. тайна

Решение:

По программе очевидно (даже без знания языка C++), что здесь идет работа с массивом строк и в каждой строке выбирается буква на определенной позиции. В строке кода result=result+s[i][3]; видно, что из строки выбирается буква с номером 3. Так как буквы в строке нумеруются с нуля (о чем, возможно, нужно было догадаться), то выбираются буквы с 4 позиции.

*"кро**т**овые" "пен**а**ты" "злe**й**шие" "коз**н**и" "сад**а**"*

9. 1) A; 2) A, C

10. A, B, C, D, F

11. квалифицированная подпись

Решение:

Строку «конилиявивднриспацапаофь» необходимо последовательно вставить в решетку 8*3

	1	2	3
1	к	и	а
2	о	в	ц
3	н	д	а
4	и	н	п
5	л	р	а
6	и	и	о
7	я	с	ф
8	в	п	ь

и получить строку «киаовцндаинплраииоясфвпь». Затем нужно использовать решетку 4*6.

	1	2	3	4	5	6
1	к	в	а	л	и	ф
2	и	ц	и	р	о	в
3	а	н	н	а	я	п
4	о	д	п	и	с	ь

12. 96

Решение:

Если к 254 прибавить 2, то будет 256. В двоичном коде это **1**00000000. Единица не влезет в байт и пропадет. Таким образом слагаемое 98 можно разбить на 2 и 96. В итоге получаем два слагаемых, одно из которых пропадает ~~256~~+ 96.

13. Ответ: у первого сотрудника самый не надежный пароль: A4$Fz Решение.

- определить L: подсчитать количество символов в каждом пароле
- определить A: подсчитать количество символов, с помощью которых записан пароль
- перевести в минуты максимальный срок действия пароля (T);
- рассчитать P для каждого пароля, по указанной формуле, подставив значения V, T, A, L;
- определить из полученных P наибольшее значение (наибольшая вероятность подбора пароля с указанной скоростью перебора паролей (V), с учетом срок а действия пароля (T)). Пароль с этим значением обладает меньшей стойкостью к атакам перебора (не надежный пароль A4$Fz – у первого сотрудника).

14. звезда

Решение:

Вычтем из кода шифрованного текста код ключа, и сопоставим полученным кодам буквы алфавита

Шифр	Код	Буква	ключ	код	буква
е	5	к	9	-4	з
в	2	а	0	2	в
ж	6	б	1	5	е
з	7	а	0	7	з
г	3	л	10	-7	д
а	0	а	0	0	а

Коды -4 и -7 можно понимать как сдвиг (отсчет) от буквы «а» по алфавиту в обратную сторону, так буква «з» получается сдвигом а->л->к->и->з

15. Кто-то может перехватить сообщение и вырезать подпись Алисы. Он может вставить ее в любое другое сообщение, переслав его от имени Алисы, при этом злоумышленнику не требуется расшифровывать саму подпись.

16. C

17.

a) Удалено 2 файла (photo.jpg и secret_data.xlsx).
b) Наибольший размер имеет файл backup.zip (500 КБ).
c) Файл photo.jpg могли удалить только пользователи с правами администратора, так как у него установлены права на запись только для администратора.

18. 50 секунд

Решение:

Время восстановления удалённых файлов:

- photo.jpg: 200 КБ × 0,1 с/КБ = 20 с
- secret_data.xlsx: 300 КБ × 0,1 с/КБ = 30 с

Общая сумма = 20 + 30 = 50 секунд.

19. A

Объяснение:

```
r'\(\d{3}\) \d{3}-\d{4}'
```

- **Вариант A** правильно описывает формат `(XXX) XXX-XXXX`, где три цифры в скобках и три цифры, за которыми следует дефис, затем четыре цифры.
- **Вариант B** неверен, поскольку он не соответствует формату с открывающими и закрывающими скобками. В этом варианте нет скобок вокруг первых трех цифр.
- **Вариант C** также неверен, так как он позволяет от 2 до 3 цифр в скобках и от 4 до 5 цифр после дефиса, что не соответствует требуемому формату телефонного номера.

20. B

Объяснение:

- **Вариант A** слишком общий и не содержит важной информации о предпочтениях, активности, продолжительности и бюджете, что делает его неэффективным для комплексного запроса.
- **Вариант B** чётко описывает все критерии, которые необходимо учитывать при планировании путешествия: климат, интересы, продолжительность и бюджет. Это позволяет ИИ сформировать детализированный и целенаправленный ответ, соответствующий запросу пользователя.
- **Вариант C** достаточно подробен, но учитывает не все параметры, а значит результаты запроса дадут менее эффективные результаты поиска.
- **Вариант D** достаточно расплывчат и не уточняет, что именно пользователь ищет в своём путешествии, поэтому не обеспечивает необходимого контекста для максимально информативного ответа.

21. ***Решение:***

Часть 1: Понимание основ

1. **Выбор простых чисел (1 балл).**

Правильный вариант - (p = 7), (q = 13), потому как оба числа являются простыми

Вариант (p = 9), (q = 11) – неверный, потому как 9 не является простым числом.

2. **Вопрос (1 балл):** Почему важно, чтобы (p) и (q) были простыми числами? Объясните, какие последствия будут, если одно из выбранных чисел не является простым.

Пример правильного ответа: Простые числа обеспечивают сложность факторизации (n), что делает систему более безопасной.

Если одно из чисел не является простым, это приводит к тому, что невозможно правильно рассчитать (φ(n)), что делает алгоритм ненадежным.

Часть 2: Вопросы на понимание

3. **Генерация ключей (1 + 1 балл за каждое вычисление):**
   Используя значения (p = 7) и (q = 13):
   - Вычислите (n)

     n = 7 * 13 = 91

   - Вычислите (φ(n))

     φ(n) = (7-1)(13-1) = 6 * 12 = 72.

4. **Выбор открытого ключа (1 за вычисление + 1 за комментарий):**
   Какое значение вы могли бы выбрать для (e), если (φ(n) = 72)?

   Можно выбрать (e = 5) (потому что 5 и 72 взаимно просты)

   Как вы можете это обосновать?

   Надо взять такое *e*, чтобы НОД(*e, φ(n)*) = 1

5. **Закрытый ключ (1 за достоверное пояснение):**
   Почему важно, чтобы закрытый ключ (d) не был известен всем? Опишите, как вы могли бы использовать (d) для дешифрования.

   Закрытый ключ (d) должен быть в секрете, чтобы никто не мог легко расшифровать сообщения, так как это может раскрыть конфиденциальные данные. Именно знание закрытого ключа (d) позволяет достоверно расшифровать сообщение.

2 балла за пояснение о конфиденциальности, 2 балла за упоминание закрытого ключа, 3 балла за разделение понятий зашифрованного и оригинального сообщения.

Дополнительные вопросы

6. **Преимущества RSA (1 балл):**
   Объясните, почему алгоритм RSA считается безопасным для передачи данных.

   Пример ответа:

   Основное преимущество заключается в том, что, даже если другая сторона знает открытый ключ, ему крайне сложно вычислить закрытый ключ на основе (n).

7. **Применение RSA (1 балл):**
   В каких ситуациях вы можете использовать RSA в реальной жизни? Приведите пример.

   Пример ответа:

   RSA используется в онлайн-банкинге, в защищённых протоколах, потому как обеспечивает безопасность транзакций или аутентификацию при входе на защищенные сайты.

   Примеры про передачу военной информации сложно притянуть к реальной жизни, но тоже можно засчитать как наполовину верный.

8. **Дополнительные примеры (1 балл):**
   Приведите одну пару скромных простых чисел ((p, q)) и объясните, что произойдет, если бы вы использовали их вместо тех, которые выбрали.

   Пример ответа:

   Выбор других чисел даст нам другие значения (n) и, следовательно, изменит значения открытого ключа (e) и закрытого ключа (d).

*** Замечание,** для вопросов теста 6, 7, 9, 10 обоснованием является следующий источник:

КРИТЕРИИ ОЦЕНИВАНИЯ

<table>
<tr><th>№</th><th>Ответы</th><th>Баллы</th></tr>
<tr><td>1.</td><td>A, B, C, D, E</td><td>2</td></tr>
<tr><td>2.</td><td>A, B, C, D</td><td>2</td></tr>
<tr><td>3.</td><td>A</td><td>2</td></tr>
<tr><td>4.</td><td><table><tr><td>1</td><td>2</td><td>3</td><td>4</td></tr><tr><td>B</td><td>A</td><td>C</td><td>D</td></tr></table></td><td>2</td></tr>
<tr><td>5.</td><td>D, C, B, E, A</td><td>2</td></tr>
<tr><td>6.</td><td>Может быть написан пункт ответа D или представлен развернутый ответ, соответствующий этому пункту.</td><td>2</td></tr>
<tr><td>7.</td><td>Могут быть написаны пункты ответа
C, E, F или представлены развернутые ответы, соответствующие этим пунктам.</td><td>2</td></tr>
<tr><td>8.</td><td>Должно быть написано слово «тайна».</td><td>2</td></tr>
<tr><td>9.</td><td>Могут быть написаны пункты ответа 1) A; 2) A, C или представлены развернутые ответы, соответствующие этим пунктам.</td><td>2</td></tr>
<tr><td>10.</td><td>Могут быть написаны пункты ответа A, B, C, D, F или представлены развернутые ответы, соответствующие этим пунктам.</td><td>2</td></tr>
<tr><td>11.</td><td>Должна быть написана строка «квалифицированная подпись», она может быть написана без пробела, так как этот символ не учитывался при шифровании</td><td>3</td></tr>
<tr><td>12.</td><td>96
Ответ должен быть только 96.</td><td>3</td></tr>
<tr><td>13.</td><td>Может быть написан ответ «у первого сотрудника самый не надежный пароль: A4$Fz»</td><td>3</td></tr>
<tr><td>14.</td><td>Должно быть написано слово «звезда».</td><td>3</td></tr>
<tr><td>15.</td><td>Кто-то может перехватить сообщение и вырезать подпись Алисы. Он может вставить ее в любое другое сообщение, переслав его от имени Алисы.
В ответе должна присутствовать идея, что подпись не защищена от копирования и вставки в другой документ.</td><td>3</td></tr>
<tr><td>16.</td><td>Может быть написан пункт ответа C или представлен развернутый ответ, соответствующий этому пункту.</td><td>3</td></tr>
<tr><td>17.</td><td>Ответы должны отражать смысл приведенных ниже примеров. За каждый правильный пункт по начисляется 1 баллу!
a) Удалено 2 файла (photo.jpg и secret_data.xlsx).
b) Наибольший размер имеет файл backup.zip (500 КБ).</td><td>3</td></tr>
</table>

	c) Файл photo.jpg могли удалить только пользователи с правами администратора, так как у него установлены права на запись только для администратора.	
18.	Должно быть написано **50 секунд.**	**3**
19.	Может быть написан пункт ответа А или представлен развернутый ответ, соответствующий этому пункту.	**3**
20.	Может быть написан пункт ответа В или представлен развернутый ответ, соответствующий этому пункту.	**3**
21.	*Оценивается в соответствии с выше данными комментариями*	**10**
	ВСЕГО БАЛЛОВ	**60**

.