ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ТРУД (ТЕХНОЛОГИЯ). ПРОФИЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ». 2024–2025 уч. г. МУНИЦИПАЛЬНЫЙ ЭТАП
10–11 КЛАССЫ

Максимальный балл за работу – 100.

Общая часть

1. У московского транспорта появились три новых маскота (персонажа-талисмана). Установите соответствие между персонажем и видом транспорта, который является прототипом этого персонажа.

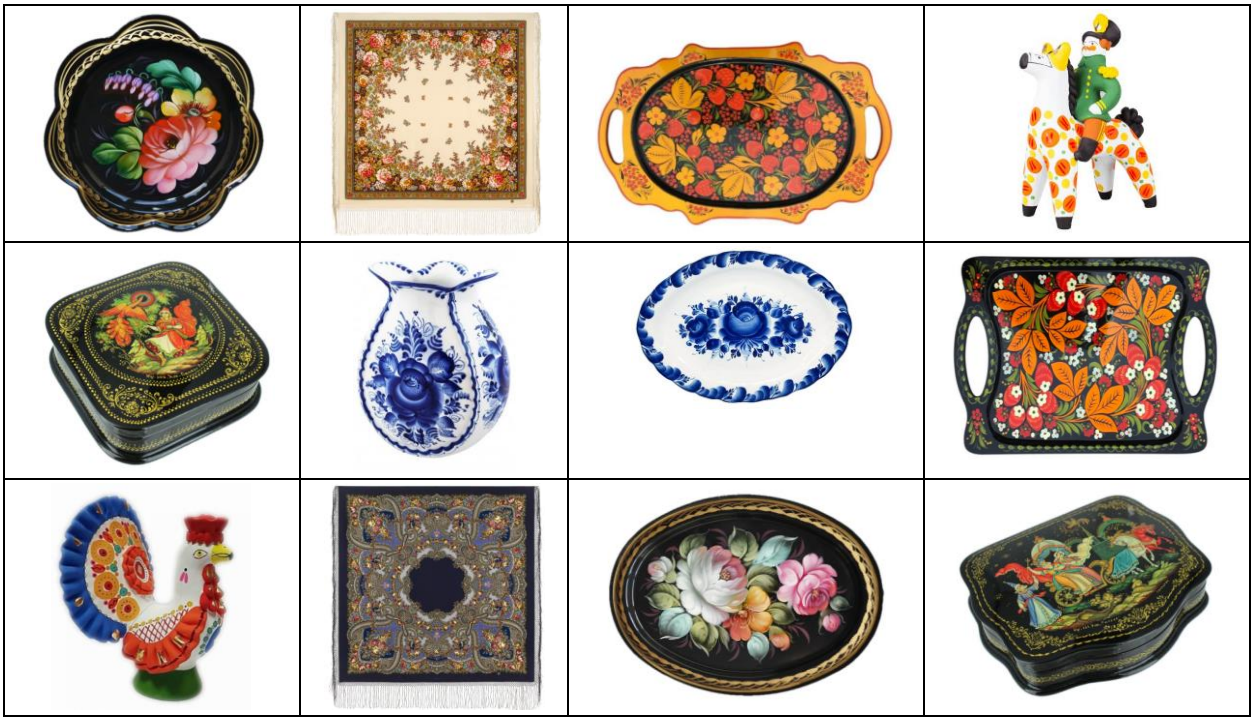
Вид транспорта: электробус, такси, речной трамвай, канатная дорога, метро.

	электробус
	такси
	речной трамвай
	канатная дорога
	метро

2. Рассмотрите изображение ручного инструмента. Как он называется?

- топор
- долото
- киянка
- рубанок
- угольник
- гвоздодёр
- напильник

3. Рассмотрите фотографии изделий народных промыслов России. Среди предложенных изображений выберите **два**, на которых представлены изделия, выполненные в технике хохломской росписи.



4. В магазине упаковка с 300 граммами голубики стоит 250 рублей. Во время проведения акции цена на упаковку голубики снизилась на 20%. Сколько рублей нужно заплатить, чтобы купить 1,5 кг голубики по акции?

5. В парке разбили прямоугольную клумбу. Длина клумбы равна 15 м, ширина равна 5 метрам. Вокруг клумбы решили сделать прямоугольную рамку **в две плитки**. Плитки все одинаковые и имеют форму квадратов. Сторона каждой плитки равна 25 см. Сколько плиток понадобится для такой рамки? Считайте, что первоначально вокруг клумбы нет ни одной плитки.

Специальная часть

6. Дан шифртекст, зашифрованный гаммированием. В этом способе шифрование выполняется следующим образом: складываются **номер символа исходного текста** в алфавите и **ключ** по модулю, равному **числу букв в алфавите**, и тогда рассматриваемый символ переходит в символ с получившимся в результате сложения по модулю номером в алфавите. Если в алфавите открытого текста, например, 10 символов, то сложение производится по модулю 10. Такой процесс сложения исходного текста и ключа называется в криптографии наложением гаммы (то есть ключа), символы которой последовательно повторяются. Для усложнения дешифрования из открытого текста убираются все знаки препинания и пробелы.

Расшифруйте послание на русском языке, зная, что гамма – 5 последовательных чисел Фибоначчи начиная с числа 2.

Шифртекст: **Р Х Ш У И Г Н Н Ш Н У Т Ш Щ Ч В И Ч Щ М Ш Е К Ъ Ы М**

Замечание: в данной задаче используется русский алфавит из 32 символов (Е и Ё отождествлены), а его буквы нумеруются начиная с 0.

В ответ запишите расшифрованное послание без пробелов.

7. Известно, что в числовом сообщении вида:

00011010 00001010 00010110 00010010

скрыто слово, относящееся к криптографии.

Запишите в ответ слово, которое скрыто в сообщении.

8. Злоумышленник собирается скрыть текстовое сообщение в видеофайле без звука длительностью 2 минуты. Видео имеет разрешение 100x100 пикселей и частоту 30 кадров в секунду. В каждом кадре максимальное значение интенсивности каждого из цветов составляет 0xFF. Злоумышленник будет использовать метод LSB для скрытия информации в каждом пикселе каждого RGB-кадра. Сколько символов он сможет скрыть в этом видеофайле, заменяя по одному значащему биту, если один символ занимает 8 бит? Ответ укажите в тысячах.

9. Алгоритм Base64 – стандарт кодирования двоичных данных при помощи только 64 символов ASCII. Он работает следующим образом.

1. Каждая буква или символ в тексте сначала преобразуется в двоичный код на основе ASCII-кодировки.
2. Полученные двоичные коды объединяются в одну длинную строку.

3. Полученная строка разбивается на группы по 6 бит.
4. Каждая 6-битная группа преобразуется в десятичное число.
5. Каждое число заменяется соответствующим символом из таблицы Base64.

Таблица Base64 содержит 64 символа: латинские буквы (A-Z, a-z), цифры (0–9) и два дополнительных символа (+ и /).

Закодируйте слово **Cipher** с помощью Base64.

Letter	ASCII Code	Binary
a	97	01100001
b	98	01100010
c	99	01100011
d	100	01100100
e	101	01100101
f	102	01100110
g	103	01100111
h	104	01101000
i	105	01101001
j	106	01101010
k	107	01101011
l	108	01101100
m	109	01101101
n	110	01101110
o	111	01101111
p	112	01110000
q	113	01110001
r	114	01110010
s	115	01110011
t	116	01110100
u	117	01110101
v	118	01110110
w	119	01110111
x	120	01111000
y	121	01111001
z	122	01111010

Letter	ASCII Code	Binary
A	65	01000001
B	66	01000010
C	67	01000011
D	68	01000100
E	69	01000101
F	70	01000110
G	71	01000111
H	72	01001000
I	73	01001001
J	74	01001010
K	75	01001011
L	76	01001100
M	77	01001101
N	78	01001110
O	79	01001111
P	80	01010000
Q	81	01010001
R	82	01010010
S	83	01010011
T	84	01010100
U	85	01010101
V	86	01010110
W	87	01010111
X	88	01011000
Y	89	01011001
Z	90	01011010

Соответствие символов и их значений в кодировке Base64

	Значение	
	10	**2**
A	0	000000
B	1	000001
C	2	000010
D	3	000011
E	4	000100
F	5	000101
G	6	000110
H	7	000111
I	8	001000
J	9	001001
K	10	001010
L	11	001011
M	12	001100
N	13	001101
O	14	001110
P	15	001111

	Значение	
	10	**2**
Q	16	010000
R	17	010001
S	18	010010
T	19	010011
U	20	010100
V	21	010101
W	22	010110
X	23	010111
Y	24	011000
Z	25	011001
a	26	011010
b	27	011011
c	28	011100
d	29	011101
e	30	011110
f	31	011111

	Значение	
	10	**2**
g	32	100000
h	33	100001
i	34	100010
j	35	100011
k	36	100100
l	37	100101
m	38	100110
n	39	100111
o	40	101000
p	41	101001
q	42	101010
r	43	101011
s	44	101100
t	45	101101
u	46	101110
v	47	101111

	Значение	
	10	**2**
w	48	110000
x	49	110001
y	50	110010
z	51	110011
0	52	110100
1	53	110101
2	54	110110
3	55	110111
4	56	111000
5	57	111001
6	58	111010
7	59	111011
8	60	111100
9	61	111101
+	62	111110
/	63	111111

10. Вам дано закодированное сообщение в формате Base64: **Rm9ybWF0**.

Ваша задача – расшифровать это сообщение и узнать, какое слово было закодировано.

11. Для шифрования используется таблица, в которой самая верхняя строка содержит буквы русского алфавита, расположенные в случайном порядке, самый левый столбец содержит номера строк. Остальные ячейки таблицы содержат двузначные числа, причём в столбце могут повторяться числа, а в строке нет. При шифровании строки таблицы просматриваются последовательно, начиная со строки под номером 1.

	А	В	У	Д	Л	Р	Й	Г	Е	О	Т	И	М	С	…
1	13	78	65	31	23	98	45	37	56	15	55	81	11	10	…
2	57	56	37	45	74	82	90	81	76	49	52	92	15	16	…
3	31	82	57	24	68	98	49	42	97	12	63	64	17	18	…
4	44	12	36	11	49	18	10	99	53	57	61	98	21	22	…
5	63	71	12	33	31	27	49	81	16	77	51	83	19	20	…
6	17	15	57	41	82	97	31	16	49	44	21	92	23	24	…
7	11	37	49	16	31	61	18	97	36	15	82	19	25	26	…
…	…	…	…	…	…	…	…	…	…	…	…	…	…		…

Известно, что таблица позволяет зашифровать одно слово несколькими способами, но для каждого получившегося шифра выполняются следующие условия:

- В начале шифртекста идёт начальная группа цифр, длина которой не превышает длину шифруемого слова, причём среди цифр этой начальной группы не может встретиться 0.
- Затем идут двузначные числа (число двузначных чисел совпадает с длиной шифруемого слова, то есть каждая буква слова шифруется одним двузначным числом).

Также известно, что зашифровано слово из 7 букв, имеющее отношение к программному обеспечению, и полученный шифр выглядит так:

121111 31 82 57 49 12 16 97

Какое слово было зашифровано?

12. Запишите, как выглядит начальная группа цифр при шифровании слова, полученного из предыдущего задания, если записанные после неё двузначные числа имеют вид: 31 82 57 49 82 97 18.

13. Запишите последние две цифры шифра, если шифруется слово ВИРУС, а начальная группа цифр выглядит так: 1121.

14. Сколько различных начальных групп цифр может быть в полученных шифрах, если в качестве исходного сообщения используется слово из 4 букв?

15. Выберите **все** верные утверждения о методе шифрования, который применялся в задании 11.

- При зашифровании слова АЛГОРИТМ начальная группа цифр может принимать вид: 11122.
- Максимальная цифра, которая может встретиться в начальной группе цифр при зашифровании слова КУРСОР, – это цифра 6.
- При зашифровании слова из 31 буквы начальная группа цифр может содержать цифру 3 не больше 3 раз.
- Если начальная группа цифр выглядит как 112, а последовательность двузначных чисел так: 11 15 12 12, это значит, что последние 2 буквы исходного текста совпадают.
- Существуют 3 начальные группы цифр длины 4 для зашифрования слова ХАКЕР.

16. Сопоставьте расширения файлов с описанием типов файлов, соответствующих этим расширениям.

Расширения файлов: .pcap, .pem, .apk, .sh, .md5.

файлы с хешами, используемые для проверки целостности данных	.pcap
скрипты оболочки, которые могут содержать команды для тестирования безопасности	.md5
файлы с сертификатами и ключами для шифрования	.pem
файлы захвата сетевого трафика	.apk
файлы приложений для Android, которые могут содержать уязвимости	.sh

17. Сопоставьте названия протоколов с их назначениями.

Названия протоколов: RADIUS, LDAP, Kerberos, ICMP, FTP.

протокол для аутентификации, авторизации и учёта доступа к сетям	FTP
протокол межсетевых управляющих сообщений	RADIUS
протокол для доступа к каталогам и управления ими, часто используемый для аутентификации	Kerberos
прикладной протокол передачи файлов, используемый для обмена данными между клиентом и сервером	LDAP
протокол сетевой аутентификации, который использует криптографию с симметричным ключом для аутентификации запросов	ICMP

18. Установите соответствия между криптографическими средствами защиты информации и их назначениями.

Криптографические средства защиты: алгоритм симметричного шифрования AES; алгоритм асимметричного шифрования RSA; криптографический алгоритм SHA-256; криптографические протоколы SSL/TLS.

проверка целостности информации	алгоритм симметричного шифрования AES
быстрое шифрование данных и расшифрование	алгоритм асимметричного шифрования RSA
защита передачи данных между узлами в сети интернет	криптографический алгоритм SHA-256
обмен ключами и создание цифровой подписи	криптографические протоколы SSL/TLS

19. Установите соответствия между терминами, относящимися к персональным данным, и их определениями.

Термины, относящиеся к персональным данным: блокирование персональных данных; обезличивание персональных данных; распространение персональных данных; уничтожение персональных данных; предоставление персональных данных.

1. Действия, направленные на раскрытие персональных данных неопределённому кругу лиц.
2. Действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.
3. Временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения персональных данных).
4. Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.
5. Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

20. Установите соответствия между приложениями для защиты информации на смартфоне с их назначениями.

позволяет устанавливать пароль или блокировать отпечатком пальца различные приложения	Adblock Browser
позволяет временно запрещать доступ к камере, другим программам и приложениям	Micro Guard FREE
блокирует навязчивую и вредоносную рекламу	Camera Blocker
позволяет спрятать IP-адрес от заинтересованных в этой информации ресурсов, а также обеспечивает защиту данных, если пользователь подключился к публичной точке доступа Wi-Fi	Boxcryptor
выявляет программы и приложения, которые пытаются получить доступ к микрофону, и предупреждает пользователя специальным сигналом	TunnelBear
зашифровывает файлы перед сохранением их в облачных базах данных, например Dropbox или Google Drive	AppLock

21. Вам представлен скриншот части вывода работы консольной утилиты curl, которая используется для выполнения HTTP-запросов. Рассмотрите скриншот и ответьте на вопросы.

```
$ curl -v https://example.com
*   Trying 93.184.216.34:443...
* Connected to example.com (93.184.216.34) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
*   CApath: /etc/ssl/certs
* SSL connection using TLS1.2 / ECDHE_RSA_AES_256_GCM_SHA384
* ALPN, server accepted to use h2
> GET / HTTP/2
> Host: example.com
> User-Agent: curl/7.68.0
> Accept: */*
>
< HTTP/2 200
< content-type: text/html; charset=UTF-8
< content-length: 1256
< date: Wed, 04 Oct 2023 12:00:00 GMT
< server: ExampleServer/1.0
< last-modified: Mon, 02 Oct 2023 10:00:00 GMT
< etag: "123456789abcdef"
< accept-ranges: bytes
<
<!doctype html>
<html>
<head>
    <title>Example Domain</title>
...
...
* Connection #0 to host example.com left intact
```

- Какой IP-адрес был использован для подключения к серверу?
- Какой метод HTTP-запроса был отправлен на сервер?
- Какова длина содержимого, возвращённого сервером, в байтах?

- Сервер вернул статус-код 200. Что он обозначает?

1. Статус-код 200 означает, что запрос клиента был успешно обработан и сервер вернул запрашиваемые данные.
2. Статус-код 200 указывает на то, что сервер временно недоступен из-за перегрузки или технического обслуживания.
3. Статус-код 200 означает, что произошла ошибка на стороне клиента и запрос не может быть выполнен.
4. Статус-код 200 сигнализирует о необходимости аутентификации для доступа к запрашиваемым данным.

Запишите номер верного варианта ответа.