Многопрофильная инженерная олимпиада «Звезда»
«Информационная безопасность»

10-11 классы **Заключительный этап** **2020-2021**

Задания, ответы и критерии оценивания

Задача 1.

А) С помощью любого ключа из кольца Z_{33} самостоятельно зашифровать слово «калькулятор» используя шифр Цезаря. *(3 балла)*

Б) Используя русский алфавит необходимо методом подбора ключа в шифре Цезаря расшифровать сообщение Y = ФТРЧФЛТУЯФЬХГЯЮХСЛТРЩГ. *(7 баллов)*

Решение.

Y = ФТРЧФЛТУЯФЬХГЯЮХСЛТРЩГ (21,19,17,24,21,12,19,20,32,21,29,22,3,32,31,22,18,12,19,17,26,3)

$\overline{k=1}$ > (20,18,16,23,20,11,18,19,31,20,28,21,2,31,30,21,17,11,18,16,25,2)=УСПЦУКСТЮУЫФВЮЭФРКСПШВ

$\overline{k=2}$ > (19,17,15,22,19,10,17,18,30,19,27,20,1,30,29,20,16,10,17,15,24,1)=ТРОХТЙРСЭТЪУБЭЬУПЙРОЧБ

$\overline{k=3}$ > (18,16,14,21,18,9,16,17,29,18,26,19,0,29,28,19,15,9,16,14,23,0)=СПНФСИПРЬСЩТАЬЫТОИПНЦА

$\overline{k=4}$ > (17,15,13,20,17,8,15,16,28,17,25,18,32,28,27,18,14,8,15,13,22,32)=РОМУРЗОПЫРШСЯЫЪСНЗОМХЯ

$\overline{k=5}$ > (16,14,12,19,16,7,14,15,27,16,24,17,31,27,26,17,13,7,14,12,21,31)=ПНЛТПЖНОЪПЧРЮЪЩРМЖНЛФЮ

$\overline{k=6}$ > (15,13,11,18,15,6,13,14,26,15,23,16,30,26,25,16,12,6,13,11,20,30)=ОМКСОЁМНЩОЦПЭЩШПЛЁМКУЭ

$\overline{k=7}$ > (14,12,10,17,14,5,12,13,25,14,22,15,29,25,24,15,11,5,12,10,19,29)=НЛЙРНЕЛМШНХОЬШЧОКЕЛЙТЬ

$\overline{k=8}$ > (13,11,9,16,13,4,11,12,24,13,21,14,28,24,23,14,10,4,11,9,18,28)=МКИПМДКЛЧМФНЫЧЦНЙДКИСЫ

$\overline{k=9}$ > (12,10,8,15,12,3,10,11,23,12,20,13,27,23,22,13,9,3,10,8,17,27)=ЛЙЗОЛГЙКЦЛУМЪЦХМИГЙЗРЪ

$\overline{k=10}$ > (11,9,7,14,11,2,9,10,22,11,19,12,26,22,21,12,8,2,9,7,16,26)=КИЖНКВИЙХКТЛЩХФЛЗВИЖПЩ

$\overline{k=11}$ > (10,8,6,13,10,1,8,9,21,10,18,11,25,21,20,11,7,1,8,6,15,25)=ЙЗЁМЙБЗИФЙСКШФУКЖБЗЁОШ

$\overline{k=12}$ > (9,7,5,12,9,0,7,8,20,9,17,10,24,20,19,10,6,0,7,5,14,24)=ИЖЕЛИАЖЗУИРЙЧУТЙЁАЖЕНЧ

$\overline{k=13}$ > (8,6,4,11,8,32,6,7,19,8,16,9,23,19,18,9,5,32,6,4,13,23)=ЗЁДКЗЯЁЖТЗПИЦТСИЕЯЁДМЦ

$\overline{k=14}$ > (7,5,3,10,7,31,5,6,18,7,15,8,22,18,17,8,4,31,5,3,12,22)=ЖЕГЙЖЮЕЁСЖОЗХСРЗДЮЕГЛХ

$\overline{k=15}$ > (6,4,2,9,6,30,4,5,17,6,14,7,21,17,16,7,3,30,4,2,11,21)=ЁДВИЁЭДЕРЁНЖФРПЖГЭДВКФ

$\overline{k=16}$ > (5,3,1,8,5,29,3,4,16,5,13,6,20,16,15,6,2,29,3,1,10,20)=ЕГБЗЕЬГДПЕМЁУПОЁВЬГБЙУ

$\overline{k=17}$ > (4,2,0,7,4,28,2,3,15,4,12,5,19,15,14,5,1,28,2,0,9,19)=ДВАЖДЫВГОДЛЕТОНЕБЫВАИТ

X= ДВАЖДЫВГОДЛЕТОНЕБЫВАИТ

Решение приведено только для пункта Б. Решение для пункта А приводится учеником. Проверяющим оценивается логичность решения. Возможна проверка с помощью онлайн калькулятора. Например, https://planetcalc.ru/1434/.

№ критерия	Количество баллов	Описание критерия
1	3	Правильно выполнено самостоятельное шифрование слова «калькулятор»
2	1	При расшифровке получена правильная фраза (читается общий смысл)
3	3	Фраза шифровалась с ошибкой. Если при расшифровке ученик получил слово «бываит», то он получает данные баллы

4 критерий – оценка написанного учеником решения (выбирается только 1 пункт)		
4 (а)	3	Приведено правильное достаточное решение
4 (б)	1	Приведено частично правильное (либо неполное) решение
4 (в)	0	Решение не приведено

Итоговая оценка складывается из суммы баллов за соответствующие решению ученика критерии.

Задача 2. Используя латинский алфавит с индексацией букв элементами кольца Z_{26}

А) Зашифровать с помощью шифра Виженера сообщение X = PANEM ET CIRCENSES. Ключ необходимо придумать самостоятельно. *(4 балла)*

Б) Расшифровать с помощью шифра Виженера сообщение Y = DCKJPZNRRNTVLNWMPVIHZCGPPBMJCQJROAMMA, ключ K = LIFE. *(8 баллов)*

Решение.

Y = DCKJPZNRRNTVLNWMPVIHZCGPPBMJCQJROAMMA

(3,2,10,9,15,25,13,17,17,13,19,21,11,13,22,12,15,21,8,7,25,2,6,15,15,1,12,9,2,16,9,17,14,0,12,12,0)

K = LIFE (11,8,5,4)

X=(18,20,5,5,4,17,8,13,6,5,14,17,0,5,17,8,4,13,3,3,14,20,1,11,4,19,7,5,17,8,4,13,3,18,7,8,15) =

SUFFERINGFORAFRIENDDOUBLETHFRIENDSHIP

Решение приведено только для пункта Б. Решение для пункта А приводится учеником. Проверяющим оценивается логичность решения. Возможна проверка с помощью онлайн калькулятора. Например, https://planetcalc.ru/2468/.

№ критерия	Количество баллов	Описание критерия
1	4	Правильно выполнено самостоятельное шифрование фразы «PANEM ET CIRCENSES»
2	1	При расшифровке получена правильная фраза
3	3	При расшифровке получена правильная числовая комбинация
4	4	Приведено правильное достаточное решение

Итоговая оценка складывается из суммы баллов за соответствующие решению ученика критерии.

Задача 3. Используя русский алфавит с индексацией букв элементами кольца Z_{33} расшифровать с помощью шифра Хилла сообщение Y = ЫКБЧТЖ.

Ключом в шифре Хилла является пара матриц: $A = \begin{pmatrix} 3 & 7 \\ 1 & 9 \end{pmatrix}$ $B = \begin{pmatrix} 10 \\ 4 \end{pmatrix}$. *(15 баллов)*

Решение.

$A^{-1} = \frac{1}{det\ A}\tilde{A}^t$

$\tilde{A} = \begin{pmatrix} 9 & -1 \\ -7 & 3 \end{pmatrix}$

det A = 27-7=20

$\tilde{A}^t = \begin{pmatrix} 9 & -7 \\ -1 & 3 \end{pmatrix}$

$\frac{1}{det\ A} = (20)^{-1} = 5$

$A^{-1} = \begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix}$

Y= ЫКБЧТЖ (28,11,1,24,19,7)

(28,11) -> (4,15)

$$\begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix}\left(\begin{pmatrix} 28 \\ 11 \end{pmatrix} - \begin{pmatrix} 10 \\ 4 \end{pmatrix}\right) = \begin{pmatrix} 12 & -2 \\ -5 & 15 \end{pmatrix}\begin{pmatrix} 18 \\ 7 \end{pmatrix} = \begin{pmatrix} 12*18 - 2*7 \\ -18*5 + 15*7 \end{pmatrix} = \begin{pmatrix} 4 \\ 15 \end{pmatrix}$$

(1,24) -> (17,15)

$$\begin{pmatrix} 12 & 31 \\ 28 & 15 \end{pmatrix}\left(\begin{pmatrix} 1 \\ 24 \end{pmatrix} - \begin{pmatrix} 10 \\ 4 \end{pmatrix}\right) = \begin{pmatrix} 12 & -2 \\ -5 & 15 \end{pmatrix}\begin{pmatrix} -9 \\ 20 \end{pmatrix} = \begin{pmatrix} -12*9 - 2*20 \\ 5*9 + 15*20 \end{pmatrix} = \begin{pmatrix} 17 \\ 15 \end{pmatrix}$$

(19,7) -> (3,0)

$$\begin{pmatrix}12 & 31\\ 28 & 15\end{pmatrix}\left(\begin{pmatrix}19\\7\end{pmatrix}-\begin{pmatrix}10\\4\end{pmatrix}\right)=\begin{pmatrix}12 & -2\\ -5 & 15\end{pmatrix}\begin{pmatrix}9\\3\end{pmatrix}=\begin{pmatrix}12*9-2*3\\ -9*5+15*3\end{pmatrix}=\begin{pmatrix}3\\0\end{pmatrix}$$

X (4,15,17,15,3,0) = ДОРОГА

№ критерия	Количество баллов	Описание критерия
1	4	Правильно найдена обратная матрица
2	1	При расшифровке получено правильное слово
3	4	При расшифровке получена правильная числовая комбинация
4 критерий – оценка написанного учеником решения (выбирается только 1 пункт)		
4 (а)	6	Приведено правильное достаточное решение
4 (б)	2	Приведено частично правильное (либо неполное) решение
4 (в)	0	Решение не приведено

Итоговая оценка складывается из суммы баллов за соответствующие решению ученика критерии.

Задача 4. Сообщение было последовательно зашифровано с помощью шифра Цезаря и шифра Виженера. Ключом в шифре Виженера является K=ЛУНА. Расшифровать сообщение

Y = ЫПЯНДБЗТЖЭНЬРЙН. Кольцо Z_{33} . *(12 баллов)*

Решение.

Y = ЫПЯНДБЗТЖЭНЬРЙН (28,16,32,14,4,1,8,19,7,30,14,29,17,10,14)

K = ЛУНА (12,20,14,0)

Y’ = (16,29,18,14,25,14,27,19,28,10,0,29,5,23,0)

$\xrightarrow{k=1}$ (15,28,17,13,24,13,26,18,27,9,32,28,4,22,32)=ОЫРМЧМЩСЪИЯЫДХЯ

$\xrightarrow{k=2}$ (14,27,16,12,23,12,25,17,26,8,31,27,3,21,31)=НЪПЛЦЛШРЩЗЮЪГФЮ

$\xrightarrow{k=3}$ (13,26,15,11,22,11,24,16,25,7,30,26,2,20,30)=МЩОКХКЧПШЖЭЩВУЭ

$\xrightarrow{k=4}$ (12,25,14,10,21,10,23,15,24,6,29,25,1,19,29)=ЛШНЙФЙЦОЧЁЬШБТЬ

$\xrightarrow{k=5}$ (11,24,13,9,20,9,22,14,23,5,28,24,0,18,28)=КЧМИУИХНЦЕЫЧАСЫ

$\xrightarrow{k=6}$ (10,23,12,8,19,8,21,13,22,4,27,23,32,17,27)=ЙЦЛЗТЗФМХДЪЦЯРЪ

$\xrightarrow{k=7}$ (9,22,11,7,18,7,20,12,21,3,26,22,31,16,26)=ИХКЖСЖУЛФГЩХЮПЩ

$\xrightarrow{k=8}$ (8,21,10,6,17,6,19,11,20,2,25,21,30,15,25)=ЗФЙЁРЁТКУВШФЭОШ

$\xrightarrow{k=9}$ (7,20,9,5,16,5,18,10,19,1,24,20,29,14,24)=ЖУИЕПЕСЙТБЧУЬНЧ

$\xrightarrow{k=10}$ (6,19,8,4,15,4,17,9,18,0,23,19,28,13,23)=ЁТЗДОДРИСАЦТЫМЦ

$\xrightarrow{k=11}$ (5,18,7,3,14,3,16,8,17,32,22,18,27,12,22)=ЕСЖГНГПЗРЯХСЪЛХ

$\xrightarrow{k=12}$ (4,17,6,2,13,2,15,7,16,31,21,17,26,11,21)=ДРЁВМВОЖПЮФРЩКФ

$\xrightarrow{k=13}$ (3,16,5,1,12,1,14,6,15,30,20,16,25,10,20)=ГПЕБЛБНЁОЭУПШЙУ

$\xrightarrow{k=14}$ (2,15,4,0,11,0,13,5,14,29,19,15,24,9,19)=ВОДАКАМЕНЬТОЧИТ

X = ВОДАКАМЕНЬТОЧИТ

№ критерия	Количество баллов	Описание критерия
1	4	При расшифровке получена правильная фраза
2	4	При дешифрации шифра Виженера получена правильная числовая комбинация (Y’)

3 критерий – оценка написанного учеником решения (выбирается только 1 пункт)		
3 (а)	4	Приведено правильное достаточное решение
3 (б)	1	Приведено частично правильное (либо неполное) решение
3 (в)	0	Решение не приведено

Итоговая оценка складывается из суммы баллов за соответствующие решению ученика критерии.

Задача 5. Сообщение было последовательно зашифровано с помощью шифра Виженера и шифра Хилла. Ключом в шифре Виженера является K = CLOUD. Ключом в шифре Хилла является пара матриц: $A = \begin{pmatrix} 10 & 7 \\ 9 & 13 \end{pmatrix}$ $B = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$. Расшифровать сообщение Y = JUGHIYUEDAFQYD. Кольцо Z_{26}. *(18 баллов)*

Решение.

$A^{-1} = \frac{1}{det\ A}\tilde{A}^t$

$\tilde{A} = \begin{pmatrix} 13 & -9 \\ -7 & 10 \end{pmatrix}$

det A = 130-63=15

$\tilde{A}^t = \begin{pmatrix} 13 & -7 \\ -9 & 10 \end{pmatrix}$

$\frac{1}{det\ A} = (15)^{-1} = 7$

$A^{-1} = \begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}$

Y= JUGHIYUEDAFQYD (9,20,6,7,8,24,20,4,3,0,5,16,24,3)

(9,20) -> (6,11)

$$\begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\left(\begin{pmatrix} 9 \\ 20 \end{pmatrix} - \begin{pmatrix} 2 \\ 5 \end{pmatrix}\right) = \begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\begin{pmatrix} 7 \\ 15 \end{pmatrix} = \begin{pmatrix} 13*7+3*15 \\ 15*7+18*15 \end{pmatrix} = \begin{pmatrix} 6 \\ 11 \end{pmatrix}$$

(6,7) -> (6,18)

$$\begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\left(\begin{pmatrix} 6 \\ 7 \end{pmatrix} - \begin{pmatrix} 2 \\ 5 \end{pmatrix}\right) = \begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\begin{pmatrix} 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 13*4+3*2 \\ 15*4+18*2 \end{pmatrix} = \begin{pmatrix} 6 \\ 18 \end{pmatrix}$$

(8,24) -> (5,16)

$$\begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\left(\begin{pmatrix} 8 \\ 24 \end{pmatrix} - \begin{pmatrix} 2 \\ 5 \end{pmatrix}\right) = \begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\begin{pmatrix} 6 \\ 19 \end{pmatrix} = \begin{pmatrix} 13*6+3*19 \\ 15*6+18*19 \end{pmatrix} = \begin{pmatrix} 5 \\ 16 \end{pmatrix}$$

(20,4) -> (23,18)

$$\begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\left(\begin{pmatrix} 20 \\ 4 \end{pmatrix} - \begin{pmatrix} 2 \\ 5 \end{pmatrix}\right) = \begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\begin{pmatrix} 18 \\ -1 \end{pmatrix} = \begin{pmatrix} 13*18-3*1 \\ 15*18-18*1 \end{pmatrix} = \begin{pmatrix} 23 \\ 18 \end{pmatrix}$$

(3,0) -> (24,3)

$$\begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\left(\begin{pmatrix} 3 \\ 0 \end{pmatrix} - \begin{pmatrix} 2 \\ 5 \end{pmatrix}\right) = \begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\begin{pmatrix} 1 \\ -5 \end{pmatrix} = \begin{pmatrix} 13*1-3*5 \\ 15*1-18*5 \end{pmatrix} = \begin{pmatrix} 24 \\ 3 \end{pmatrix}$$

(5,16) -> (20,9)

$$\begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\left(\begin{pmatrix} 5 \\ 16 \end{pmatrix} - \begin{pmatrix} 2 \\ 5 \end{pmatrix}\right) = \begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\begin{pmatrix} 3 \\ 11 \end{pmatrix} = \begin{pmatrix} 13*3+3*11 \\ 15*3+18*11 \end{pmatrix} = \begin{pmatrix} 20 \\ 9 \end{pmatrix}$$

(24,3) -> (20,8)

$$\begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\left(\begin{pmatrix} 24 \\ 3 \end{pmatrix} - \begin{pmatrix} 2 \\ 5 \end{pmatrix}\right) = \begin{pmatrix} 13 & 3 \\ 15 & 18 \end{pmatrix}\begin{pmatrix} 22 \\ -2 \end{pmatrix} = \begin{pmatrix} 13*22-3*2 \\ 15*22-18*2 \end{pmatrix} = \begin{pmatrix} 20 \\ 8 \end{pmatrix}$$

Y’ = (6,11,6,18,5,16,23,18,24,3,20,9,20,8)

K = CLOUD (2,11,14,20,3)

X = (4,0,18,24,2,14,12,4,4,0,18,24,6,14) = EASYCOMEEASYGO

№ критерия	Количество баллов	Описание критерия
1	4	Правильно найдена обратная матрица
2	1	При расшифровке получена правильная фраза
3	4	При дешифрации шифра Хилла получена правильная числовая комбинация (Y')
4	3	При дешифрации шифра Виженера получена правильная числовая комбинация (X)
5 критерий – оценка написанного учеником решения (выбирается только 1 пункт)		
5 (а)	6	Приведено правильное достаточное решение
5 (б)	2	Приведено частично правильное (либо неполное) решение
5 (в)	0	Решение не приведено

Итоговая оценка складывается из суммы баллов за соответствующие решению ученика критерии.

Проектная задача. На одном из языков программирования (Алгоритмический, C#, C++, Pascal, Java, Python) разработать программу для автоматического шифрования сообщений с помощью шифра Виженера. *(33 балла)*

№ критерия	Количество баллов	Описание критерия
1	33	Приведена программа, правильно реализующая шифр Виженера. При написании программы допущено не более 3-х синтаксических ошибок. Если одна и та же ошибка встречается несколько раз, она считается за одну ошибку.
2	25	При написании программы допущены незначительные логические ошибки, но ход решения правильный. При написании программы допущено не более 5-и синтаксических ошибок.
3	12	Программа выполняет шифрование входных данных, но логика шифрования сильно отличается от шифра Виженера. При написании программы допущено не более 7-и синтаксических ошибок.
4	5	Программа не дописана, но имеются идеи, совпадающие с алгоритмом шифрования.
5	0	Задание не выполнено.

Итоговая оценка – количество баллов за выбранный критерий