|  |
| --- |
|  |

Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение

высшего образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ

МОРДОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

им. Н.П. ОГАРЁВА»

(ФГБОУ ВО «МГУ им. Н.П. Огарёва»)

Институт электроники и светотехники

Кафедра информационной безопасности и сервиса

ЛАБОРАТОРНАЯ РАБОТА №6

по теме:

«Перестановочные шифры»

Автор отчёта о лабораторной работе  А. Е. Конышев

подпись, дата

Обозначение лабораторной работы ЛР–02069964–02.03.02–08–23

Направление подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Проверил работу

канд. техн. наук, доц.  И. П. Карьгин

подпись, дата

Саранск 2023

**Шифр «Лесенка».**

Открытый текст записывается вдоль наклонных строк определенной длины («ступенек»), а затем считывается построчно по горизонтали. Например, чтобы шифровать сообщение «шифр с использованием перестановки» по методу лесенки со ступеньками длиной 2, запишем это сообщение в виде:

Ш Ф С С О Ь О А И М Е Е Т Н В И

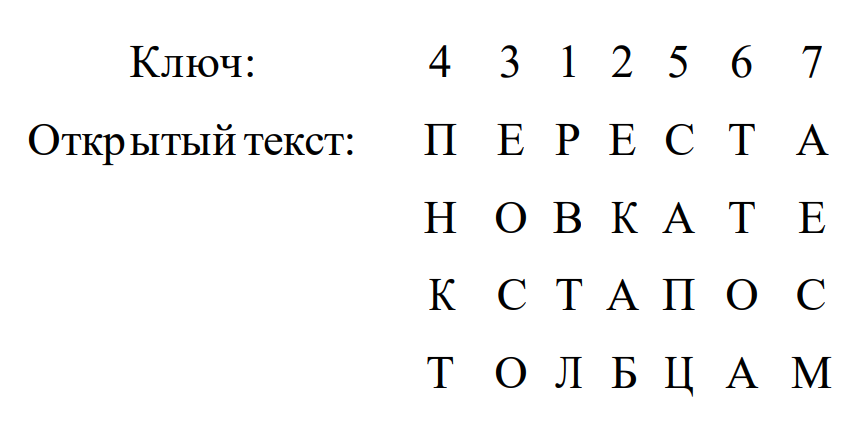
И Р И П Л З В Н Е П Р С А О К

Шифрованное сообщение будет иметь следующий вид:

ШФССОЬОАИМЕЕТНВИИРИПЛЗВНЕПРСАОК

**Шифр вертикальной перестановки.**

сложная схема предполагает запись текста сообщения в горизонтальные строки одинаковой длины и последующее считывание текста столбец за столбцом, но не по порядку, а в соответствии с некоторой перестановкой столбцов. Порядок считывания столбцов при этом становиться ключом алгоритма. Ниже приведен пример шифрования фразы «ПЕРЕСТАНОВКА ТЕКСТА ПО СТОЛБЦАМ» с ключом 4312567.



Шифрованный текст: РВТЛЕКАБЕОСОПНКТСАПЦТТОААЕСМ

**Расшифровка сообщений, зашифрованных шифром «Лесенка».**

Для расшифровки сообщения необходимо вместе с текстом передать высоту лесенки. Записав сообщение блоками по горизонтали и считав его со ступенек, получим исходное сообщение.

Если же высота лесенки нам не известна, то необходимо будет перебрать все возможные высоты до половины длины текста.

**Расшифровка сообщений, зашифрованных шифром вертикальной перестановки.**

Для расшифровки сообщения необходимо разбить сообщение на блоки, по длине равные длине всего сообщения, деленной на длину ключа. Полученные блоки написать вертикально в порядке, указанным ключом. Считав символы по горизонтали, получим исходное сообщение.

Расшифровка индивидуального задания:

1 задание:

Исходное сообщение: «МЕЕЕСНЬМТПЦСНРЧЯТЫЗДОЕЕТОЫЕТИСООВЧЛИГЧСЕСИВКИЕОИЕКЛВСАУОНСЕЛОЬЯПНМБИТСОЙНЗОИЕЕЕНФВДОАЛЕНСМО».

Так как высота ступенек неизвестна, будем перебирать всевозможные высоты, начиная с 2.

Полученные результаты.

2 МОЕИЕЕЕКСЛНВЬСМАТУПОЦНССНЕРЛЧОЯЬТЯЫПЗНДМОБЕИЕТТСООЫЙЕНТЗИОСИОЕОЕВЕЧНЛФИВГДЧОСАЕЛСЕИНВСКМИОЕ

3 МОЬЕВЯЕЧПЕЛНСИМНГБЬЧИМСТТЕСПСОЦИЙСВННКЗРИОЧЕИЯОЕТИЕЫЕЕЗКНДЛФОВВЕСДЕАОТУАООЛЫНЕЕСНТЕСИЛМСООО

4 МТОСЕОИОЕЫЕЙЕЕКНСТЛЗНИВОЬССИМОАЕТОУЕПВОЕЦЧННСЛСФНИЕВРГЛДЧЧООЯСЬАТЕЯЛЫСПЕЗИННДВМСОКБМЕИИОЕЕТ

5 МДЧОЗЕОСНОЕЕЕСИЕЕСЕЕСТИЛЕНОВОЕЬЫКЬНМЕИЯФТТЕПВПИОНДЦСИМОСОЕБАНОКИЛРВЛТЕЧЧВСНЯЛСОСТИАЙМЫГУНОЗ

6 МТООЬЕЕЫВИЯЕЕЗЧЕПЕЕДЛКННСОИЛМФНЕГВБВЬЕЧСИДМТСАТОТОЕУСАПЫСООЛЦЕИНЙЕСТВСНННИКЕЗСРСИЛОМЧОЕОИОЯ

7 МРЕЕСМЕЕЧТСАБНЕЯИИУИФЕТСВОТВСЫОКНСДНЗОИСООЬДВЕЕЙАМОЧОЛНЛТЕЛИОЗЕПЕИЕЬОНЦТГКЯИССОЧЛПЕМНЫСВНЕО

8 МНОГИЕСФЕРЫЧЕЛОВЕЧЕСКОЙДЕЯТЕЛЬНОСТИСВЯЗАНЫСИСПОЛЬЗОВАНИЕМДОКУМЕНТОВИОБЕСПЕЧЕНИЕМЦЕЛОСТНОСТИ

9 МСЕОИВЬЙВЕНЕВВСЯНДЕРТЧКАПЗОЕЧОЛИУНОАСЯЫИЕОМИЛНТЕГОНБЕЕЬЫТЧИСИЕНМЗИСЕЕТЕСТДСЕКЛСНМПООСЛООФОЦ

10 МЦДИЧООНЗДЕСОССИНМООЕНЕОЕЕСБИАЕРЕОСКЕИЕЛСЧТВИЛЛТЕЕНЯОЧВВОСЕНЬТЫЛКСЬОНСМЫЕИИАЯЙФМТЗТГЕУПНВОП

11 МПЗТИКВЛИИОЕЦДИГИСОТЕАЕСОСЧЕАЬСЕЛЕНЕОСОУЯОЕЕСРЕОЕИОПЙНННЧТВСЕНННФСЬЯОЧИКСМЗВММТЫЛВЛЕБОДОТЫЕ

12 МТТОВСЕНПОЕАЕПЫЫЧИКСНЙЕЛЕЦЗЕЛВЛЕМННЕЕСДТИКВЛБЗФНСНОИГИСОИОВСНРЕСЧЕАЬТИДМЬЧЕОСОУЯСЕООМЯТОЕИО

13 ММЧЕИИВКНПОЕАЕТЯЕСГКЛСНЙЕЛЕПТТОЧИВЕМННЕЕЦЫООСЕСЛБЗФНССЗЫВЕОАОИОВСННДЕЧСИУЬТИДМЬРОТЛИЕОЯСЕОО

14 ММЧЕИИВКОЬИЗНЛЕТЯЕСГКЛНЯТОФЕЕПТТОЧИВСПСИВНЕЦЫООСЕСЕНОЕДСССЗЫВЕОАЛМЙЕОМННДЕЧСИУОБНЕАОЬРОТЛИЕ

15 ММРДЫОЧККОЬИЗНЛЕТЧОЕВСИЛНЯТОФЕЕПЯЕТЧЕЕВСПСИВНЕЦТЕИЛСОСЕНОЕДСССЫТСИИИАЛМЙЕОМННЗООГВЕУОБНЕАОЬ

16 МЬНЗООГВЕУОБЙЕВЕЕМРДЫОЧККОЬИНЕДНЕТЧОЕВСИЛНЯТЗЕОСЕПЯЕТЧЕЕВСПСОНАМСЦТЕИЛСОСЕНОИФЛОНСЫТСИИИАЛМ

17 МЬНЗООГИОВНЬБЙЕВЕЕМРДЫОЧВИССЯИНЕДНЕТЧОЕВСКЕАЕПТЗЕОСЕПЯЕТЧЕИКУЛНСОНАМСЦТЕИЛСЕЛООМОИФЛОНСЫТСИ

18 МЬСТЕЕОГИОВНЬБЙЕВЕЕМНЫЕТВЧВИССЯИНЕДНЕТРЗТИЧСКЕАЕПТЗЕОСЕПЧДОСЛЕИКУЛНСОНАМСЦЯОЫОИСЕЛООМОИФЛОН

19 МНЦЯОЫОИСЕЛООМОИНОНЕЬСТЕЕОГИОВНЬБЙЕФАСЕМНЫЕТВЧВИССЯИНЕВЛМЕТРЗТИЧСКЕАЕПТЗЕДЕОСПЧДОСЛЕИКУЛНСО

20 МНЦЯОЫОИСЕЛОЛПИЙИНОНЕЬСТЕЕОГИОВНОНТНЕФАСЕМНЫЕТВЧВИССЬМСЗЕВЛМЕТРЗТИЧСКЕАЕЯБООЕДЕОСПЧДОСЛЕИКУ

21 МНЦЯОЫОИЕКИВОЛПИЙИНОНЕЬСТЕЕОГСИЕСНОНТНЕФАСЕМНЫЕТВЧИЕКАСЬМСЗЕВЛМЕТРЗТИЧСВОЛУЕЯБООЕДЕОСПЧДОСЛ

22 МНЦЯДТТОИЕКИВОЛПИЙИНОНЕЬСТООИВГСИЕСНОНТНЕФАСЕМНЫЕЫСЧЧИЕКАСЬМСЗЕВЛМЕТРЗЕЕОЛСВОЛУЕЯБООЕДЕОСПЧ

23 МСТНТООИВГСИЕСНОНТНЕФАСЕНПРЫЕЫСЧЧИЕКАСЬМСЗЕВЛМЕЬЦЧЗЕЕОЛСВОЛУЕЯБООЕДЕОЕМСЯДТТОИЕКИВОЛПИЙИНОН

24 МСТНТООИВГСИЕСНОНТНЕНДЛСЕНПРЫЕЫСЧЧИЕКАСЬМСЗЕФОЕМЕЬЦЧЗЕЕОЛСВОЛУЕЯБООЕВАНОЕМСЯДТТОИЕКИВОЛПИЙИ

25 МСТНТООИВГСИЕСНОНИОЗЕНДЛСЕНПРЫЕЫСЧЧИЕКАСЬМТЙОЕФОЕМЕЬЦЧЗЕЕОЛСВОЛУЕЯБСНИЕВАНОЕМСЯДТТОИЕКИВОЛП

26 МСТНТООИВГСИЕСОЕЬНИОЗЕНДЛСЕНПРЫЕЫСЧЧИЕКАНЛЯМТЙОЕФОЕМЕЬЦЧЗЕЕОЛСВОЛУСОПБСНИЕВАНОЕМСЯДТТОИЕКИВ

27 МСТНТООИВГСКОКСОЕЬНИОЗЕНДЛСЕНПРЫЕЫСЧЧИИИЛАНЛЯМТЙОЕФОЕМЕЬЦЧЗЕЕОЛСВЕЕВУСОПБСНИЕВАНОЕМСЯДТТОИЕ

28 МСТНТООИОЛЧСКОКСОЕЬНИОЗЕНДЛСЕНПРЫЕЫСВИСИИИЛАНЛЯМТЙОЕФОЕМЕЬЦЧЗЕЕОЧГЕВЕЕВУСОПБСНИЕВАНОЕМСЯДТТ

29 МСТНТДЕЫИОЛЧСКОКСОЕЬНИОЗЕНДЛСЕНПРЫОТЕСВИСИИИЛАНЛЯМТЙОЕФОЕМЕЬЦЧЗЕОТОЧГЕВЕЕВУСОПБСНИЕВАНОЕМСЯ

30 МСМЦРТДЕЫИОЛЧСКОКСОЕЬНИОЗЕНДЛСЕНТСЧЫОТЕСВИСИИИЛАНЛЯМТЙОЕФОЕМЕЬПНЯЗЕОТОЧГЕВЕЕВУСОПБСНИЕВАНОЕ

31 МЕЬПНЯЗЕОТОЧГЕВЕЕВУСОПБСНИЕВАНМЕСМЦРТДЕЫИОЛЧСКОКСОЕЬНИОЗЕНДЛСОЕНТСЧЫОТЕСВИСИИИЛАНЛЯМТЙОЕФОЕ

32 МЕЬПНЯЗЕОТОЧГЕВЕЕВУСОПБСНИЕВОЛНМЕСМЦРТДЕЫИОЛЧСКОКСОЕЬНИОЗЕНДАЕСОЕНТСЧЫОТЕСВИСИИИЛАНЛЯМТЙОЕФ

33 МЕЬПНЯЗЕОТОЧГЕВЕЕВУСОПБСНИЕНВОЛНМЕСМЦРТДЕЫИОЛЧСКОКСОЕЬНИОЗЕЕФДАЕСОЕНТСЧЫОТЕСВИСИИИЛАНЛЯМТЙО

34 МЕЬПНЯЗЕОТОЧГЕВЕЕВУСОПБСЙЗИЕНВОЛНМЕСМЦРТДЕЫИОЛЧСКОКСОЕЬНИОНОЕЕФДАЕСОЕНТСЧЫОТЕСВИСИИИЛАНЛЯМТ

35 МЕЬПНЯЗЕОТОЧГЕВЕЕВУСОПМИСЙЗИЕНВОЛНМЕСМЦРТДЕЫИОЛЧСКОКСОЕЬНБТОНОЕЕФДАЕСОЕНТСЧЫОТЕСВИСИИИЛАНЛЯ

36 МЕЬПНЯЗЕОТОЧГЕВЕЕВУСЛЬПМИСЙЗИЕНВОЛНМЕСМЦРТДЕЫИОЛЧСКОКСОЕОЯНБТОНОЕЕФДАЕСОЕНТСЧЫОТЕСВИСИИИЛАН

37 МЕЬПНЯЗЕОТОЧГЕВЕЕВАОСЛЬПМИСЙЗИЕНВОЛНМЕСМЦРТДЕЫИОЛЧСКОКСУНЕОЯНБТОНОЕЕФДАЕСОЕНТСЧЫОТЕСВИСИИИЛ

38 МЕЬПНЯЗЕОТОЧГЕВЕИКВАОСЛЬПМИСЙЗИЕНВОЛНМЕСМЦРТДЕЫИОЛЧСКОЕЛСУНЕОЯНБТОНОЕЕФДАЕСОЕНТСЧЫОТЕСВИСИИ

39 МЕЬПНЯЗЕОТОЧГЕИКЕИКВАОСЛЬПМИСЙЗИЕНВОЛНМЕСМЦРТДЕЫИОЛЧСВИОЕЛСУНЕОЯНБТОНОЕЕФДАЕСОЕНТСЧЫОТЕСВИС

40 МЕЬПНЯЗЕОТОЧИЧЕИКЕИКВАОСЛЬПМИСЙЗИЕНВОЛНМЕСМЦРТДЕЫИОЛГССВИОЕЛСУНЕОЯНБТОНОЕЕФДАЕСОЕНТСЧЫОТЕСВ

41 МЕЬПНЯЗЕОТСОЧИЧЕИКЕИКВАОСЛЬПМИСЙЗИЕНВОЛНМЕСМЦРТДЕЫИОВЛГССВИОЕЛСУНЕОЯНБТОНОЕЕФДАЕСОЕНТСЧЫОТЕ

42 МЕЬПНЯЗЕТЫТСОЧИЧЕИКЕИКВАОСЛЬПМИСЙЗИЕНВОЛНМЕСМЦРТДЕОЕИОВЛГССВИОЕЛСУНЕОЯНБТОНОЕЕФДАЕСОЕНТСЧЫО

43 МЕЬПНЯЫДЕТЫТСОЧИЧЕИКЕИКВАОСЛЬПМИСЙЗИЕНВОЛНМЕСМЦРТЗОЕОЕИОВЛГССВИОЕЛСУНЕОЯНБТОНОЕЕФДАЕСОЕНТСЧ

44 МЕЬПСРЯЫДЕТЫТСОЧИЧЕИКЕИКВАОСЛЬПМИСЙЗИЕНВОЛНМЕСМЦНЧТЗОЕОЕИОВЛГССВИОЕЛСУНЕОЯНБТОНОЕЕФДАЕСОЕНТ

Прочитав все варианты, единственное сообщение, имеющее смысл– 7 сообщение со ступенькой равной 8.

8 МНОГИЕСФЕРЫЧЕЛОВЕЧЕСКОЙДЕЯТЕЛЬНОСТИСВЯЗАНЫСИСПОЛЬЗОВАНИЕМДОКУМЕНТОВИОБЕСПЕЧЕНИЕМЦЕЛОСТНОСТИ

Сообщение имеет вид: МНОГИЕ СФЕРЫ ЧЕЛОВЕЧЕСКОЙ ДЕЯТЕЛЬНОСТИ СВЯЗАНЫ С ИСПОЛЬЗОВАНИЕМ ДОКУМЕНТОВ И ОБЕСПЕЧЕНИЕМ ЦЕЛОСТНОСТИ.

2 задание:

Зашифрованный текст: ОННАНЦОНДЛЬХФИСНИАТЫКЕЬД

Частично восстановленный ключ: XX24X3

Переберем все возможные ключи по восстановленному и получим соответствующие тексты:

key = 152463, decrypt = ОИНФКДНАЦИЕЛНТОСЬЬАЫННДХ

key = 162453, decrypt = ОКНФИДНЕЦИАЛНЬОСТЬАДННЫХ

key = 512463, decrypt = ИОНФКДАНЦИЕЛТНОСЬЬЫАННДХ

key = 562413, decrypt = ИКНФОДАЕЦИНЛТЬОСНЬЫДННАХ

key = 612453, decrypt = КОНФИДЕНЦИАЛЬНОСТЬДАННЫХ

key = 652413, decrypt = КИНФОДЕАЦИНЛЬТОСНЬДЫННАХ

Единственное сообщение, имеющее смыл – с ключом 61245, сообщение – КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ.