**Методические указания к контрольной работе**

**«Шифрование»**

Автор: Кийко Валерий Васильевич,

преподаватель Уральского государственного колледжа имени И.И. Ползунова

### Екатеринбург 2023

**Цель контрольной работы:** проверить и закрепить знания студентов алгоритмов формирования классических шифров [1].

1. **Простые подстановочные шифры.**

Дано:

- незашифрованный текст (Приложение 1);

- используемый алфавит для шифрования (Приложение 2).

Задачи:

- составить ключ шифрования перестановкой символов алфавита произвольным образом;

- используя простой алгоритм перестановки и ключ шифрования выполнить шифрование заданного текста;

- составить ключ для дешифрования.

1. **Полиалфавитные шифры.**

Дано:

- незашифрованный текст (Приложение 1);

- используемый алфавит для шифрования (Приложение 2).

- кортеж (Приложение 3).

Задачи:

- используя шифр Виженера выполнить шифрование заданного текста;

- составить ключ для дешифрования.

1. **Перестановочные шифры.**

Дано:

- незашифрованный текст (Приложение 1);

- используемый алфавит (Приложение 2);

- размер блоков равен 6;

- ключ шифрования (приложение 5).

Задачи:

- используя перестановочный шифр выполнить шифрование заданного текста;

- составить ключ для дешифрования.

 ***Примечание:*** пример выполнения контрольной работы приведен в приложении 6.

1. https://uch-lit.ru/matematika-2/dlya-studentov/mao-venbo-sovremennaya-kriptografiya-teoriya-i-praktika-onlayn?ysclid=lmw8n5j8ij301917204 – Мао Венбо. Современная криптография: теория и практика (дата обращения 23.09.2023).

Приложение 1

Исходный текст

|  |  |
| --- | --- |
| №варианта | Незашифрованный текст |
| 1 | Большое количество данных в |
| 2 | Блоки будут преобразованы в |
| 3 | Режим считается безопасным |
| 4 | Последовательность блоков |
| 5 | Более уязвим к атакам потока |
| 6 | Длина ключа целесообразно к |
| 7 | Все слабые ключи должны быть |
| 8 | Использовать заранее ключи |
| 9 | Безопасным считается режим |
| 10 | Целесообразно к длине ключа |
| 11 | Самым распространенным был |
| 12 | Алгоритм разработан в годах |
| 13 | Должна быть возможность при |
| 14 | Шифрование данных без каких |
| 15 | Случайного выбора одного из |
| 16 | Он состоит из четырех этапов |
| 17 | Следующие этапы состоят при |
| 18 | Входной блок проходит через |
| 19 | При возможности должна быть |
| 20 | Был самым распространенным |
| 21 | Должно быть все ключи слабые |
| 22 | Проходит через входной блок |
| 23 | На рисунке показан способ из |
| 24 | После последнего раунда три |
| 25 | Теперь мы должны показывать |
| 26 | Режим считается безопасным |
| 27 | Безопасным считается режим |
| 28 | Алгоритм разработан в годах |
| 29 | Шифрование данных без каких |
| 30 | Теперь мы должны показывать |

Приложение 2

Русский алфавит

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А а | Б б | В в | Г г | Д д | Е е | Ё ё | Ж ж | З з | И и |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|  |
| Й й | К к | Л л | М м | Н н | О о | П п | Р р | С с | Т т |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|  |
| У у | Ф ф | Х х | Ц ц | Ч ч | Ш ш | Щ щ | Ъ ъ | Ы ы | Ь ь |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|  |
| 31 | 32 | 33 |  |  |  |  |  |  |  |
| Э э | Ю ю | Я я |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В  | Г  | Д  | Е  | Ё  | Ж  | З  | И  | Й  | К  | Л  | М  | Н  | О  | П  | Р  | С  | Т  | У  | Ф  | Х  | Ц  | Ч  | Ш  | Щ  | Ъ  | Ы  | Ь  | Э | Ю | Я |

Приложение 3

Кортежи

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № вар-та | Кортеж (ключ) | № вар-та | Кортеж (ключ) | № вар-та | Кортеж (ключ) | № вар-та | Кортеж (ключ) |
| 1 | 7,11,2,13 | 16 | 11,2,13,7 | 31 | 2,13,7,11 | 46 | 13,7,11,2 |
| 2 | 6,12,21,2 | 17 | 12,21,2,6 | 32 | 21,2,6,12 | 47 | 2,6,12,21 |
| 3 | 5,22,7,11 | 18 | 22,7,11,5 | 33 | 7,11,5,22 | 48 | 11,5,22,7 |
| 4 | 9,23,7,13 | 19 | 23,7,13,9 | 34 | 7,13,9,23 | 49 | 13,9,23,7 |
| 5 | 8,13,9,22 | 20 | 13,9,22,8 | 35 | 9,22,8,13 | 50 | 22,8,13,9 |
| 6 | 4,17,1,28 | 21 | 17,1,28,4 | 36 | 1,28,4,17 | 51 | 28,4,17,1 |
| 7 | 3,26,19,11 | 22 | 26,19,11,3 | 37 | 19,11,3,26 | 52 | 11,3,26,19 |
| 8 | 13,2,28,21 | 23 | 2,28,21,13 | 38 | 28,21,13,2 | 53 | 21,13,2,28 |
| 9 | 27,6,19,5 | 24 | 6,19,5,27 | 39 | 19,5,27,6 | 54 | 5,27,6,19 |
| 10 | 29,5,13,7 | 25 | 5,13,7,29 | 40 | 13,7,29,5 | 55 | 7,29,5,13 |
| 11 | 14,25,8,24 | 26 | 25,8,24,14 | 41 | 8,24,14,25 | 56 | 24,14,25,8 |
| 12 | 15,26,7,21 | 27 | 26,7,21,15 | 42 | 7,21,15,26 | 57 | 21,15,26,7 |
| 13 | 17,14,4,28 | 28 | 14,4,28,17 | 43 | 4,28,17,14 | 58 | 28,17,14,4 |
| 14 | 16,7,24,9 | 29 | 7,24,9,16 | 44 | 24,9,16,7 | 59 | 9,16,7,24 |
| 15 | 19,10,7,25 | 30 | 10,7,25,19 | 45 | 7,25,19,10 | 60 | 25,19,10,7 |

Приложение 5

 Ключи шифрования (задание № 3 контрольной работы)

Четные варианты: 316425

Нечетные варианты: 536142

Приложение 6

Пример выполнения контрольной работы

|  |  |
| --- | --- |
| №варианта | Незашифрованный текст |
| 30 | Теперь мы должны показывать |

1. **Подстановочные шифры**

Исходный текст: **Теперь мы должны показывать**

Ключ шифрования

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В  | Г  | Д  | Е  | Ё  | Ж  | З  | И  | Й  | К  | Л  | М  | Н  | О  | П  | Р  | С  | Т  | У  | Ф  | Х  | Ц  | Ч  | Ш  | Щ  | Ъ  | Ы  | Ь  | Э | Ю | Я |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |
| **4** | **9** | **11** | **7** | **13** | **17** | **20** | **23** | **15** | **24** | **2** | **21** | **26** | **29** | **32** | **27** | **1** | **6** | **30** | **28** | **14** | **25** | **16** | **33** | **3** | **22** | **18** | **31** | **8** | **12** | **19** | **10** | **5** |

Зашифрованный текст: **Ъпапек ыж лщшхюж кёугнжйгък**

Ключ дешифрирования

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В  | Г  | Д  | Е  | Ё  | Ж  | З  | И  | Й  | К  | Л  | М  | Н  | О  | П  | Р  | С  | Т  | У  | Ф  | Х  | Ц  | Ч  | Ш  | Щ  | Ъ  | Ы  | Ь  | Э | Ю | Я |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |
| **17** | **11** | **25** | **1** | **33** | **18** | **4** | **29** | **2** | **32** | **3** | **30** | **5** | **21** | **9** | **23** | **6** | **27** | **31** | **7** | **12** | **26** | **8** | **10** | **22** | **13** | **16** | **20** | **14** | **19** | **28** | **15** | **24** |

1. **Полиалфавитные шифры**

Исходный текст: **Теперь мы должны показывать**

|  |  |
| --- | --- |
| № варианта | Кортеж (ключ) |
| 30 | 5,13, 7, 29 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В  | Г  | Д  | Е  | Ё  | Ж  | З  | И  | Й  | К  | Л  | М  | Н  | О  | П  | Р  | С  | Т  | У  | Ф  | Х  | Ц  | Ч  | Ш  | Щ  | Ъ  | Ы  | Ь  | Э | Ю | Я |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |
| 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 |
| **6** | **15** | **10** | **33** | **10** | **19** | **14** | **4** | **14** | **23** | **18** | **8** | **18** | **27** | **22** | **12** | **22** | **31** | **26** | **16** | **26** | **2** | **30** | **20** | **30** | **6** | **1** | **24** | **1** | **10** | **5** | **28** | **5** |

Зашифрованный текст: **Осфсэи ща икргфа фкжемаиеои**

Ключ для дешифрирования

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В  | Г  | Д  | Е  | Ё  | Ж  | З  | И  | Й  | К  | Л  | М  | Н  | О  | П  | Р  | С  | Т  | У  | Ф  | Х  | Ц  | Ч  | Ш  | Щ  | Ъ  | Ы  | Ь  | Э | Ю | Я |
| 6 | 15 | 10 | 33 | 10 | 19 | 14 | 4 | 14 | 23 | 18 | 8 | 18 | 27 | 22 | 12 | 22 | 31 | 26 | 16 | 26 | 2 | 30 | 20 | 30 | 6 | 1 | 24 | 1 | 10 | 5 | 28 | 5 |
| 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 | 13 | 7 | 29 | 5 |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** | **26** | **27** | **28** | **29** | **30** | **31** | **32** | **33** |

1. **Перестановочные шифры**

Ключ шифрования

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 | 1 | 6 | 4 | 2 | 5 |

Исходный текст: Теперь мыдолж ныпока зывать

Зашифрованный тескт: **Птьеер дмжоыл пнаоык взьаыт**

Ключ дешифрирования:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2 | 5 | 1 | 4 | 6 | 3 |