Некоммерческое акционерное общество

«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Кафедра «IT - Инжиниринг»

**ЛАБОРАТОРНАЯ РАБОТА №1**

По дисциплине «Современные Криптографические Методы Защиты Информации»

На тему: Криптоанализ классических шифров

Специальность 7M06103-Вычислительная техника и программное обеспечение

Выполнил Сакан Ерлан Группа МВТн-21-2

\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_201\_\_\_г.

(оценка) (подпись)

Алматы 2022

При решении заданий на криптоанализ шифров перестановки необходимо восстановить начальный порядок следования букв текста. Для этого используется анализ совместимости символов, в чем может помочь таблица сочетаемости.

При анализе сочетаемости букв друг с другом следует иметь в виду зависимость появления букв в открытом тексте от значительного числа предшествующих букв. Для анализа этих закономерностей используют понятие условной вероятности. Систематически вопрос о зависимости букв алфавита в открытом тексте от предыдущих букв исследовался известным русским математиком А.А.Марковым (1856 — 1922). Он доказал, что появления букв в открытом тексте нельзя считать независимыми друг от друга. В связи с этим А. А. Марковым отмечена еще одна устойчивая закономерность открытых текстов, связанная с чередованием гласных и согласных букв. Им были подсчитаны частоты встречаемости биграмм вида гласная-гласная (г,г), гласная-согласная (г,с), согласная-гласная (с,г), согласная, согласная (с,с) в русском тексте длиной в 105 знаков. Р.

Для шифра столбцовой перестановки рассмотрим два примера:

1. ПКТИРАОЛНАОИЧ\_З\_ЕСЬНЕЛНЖО
2. ПКЕЕРРПО\_ЙУСТ\_ИТПСУТЛЯЕИН

Шифр «ПКТИРАОЛНАОИЧ\_З\_ЕСЬНЕЛНЖО» содержит 25. Мы сможем записать его в таблицу 5 на 5. Зная, что шифрование проводилось по столбцам, следовательно расшифрование следует проводить таким же путем

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п | к | т | и | р |
| а | о | л | н | а |
| о | и | ч | \_ | з |
| \_ | е | с | ь | н |
| е | л | н | ж | о |

Воспользовавшись таблицей сочетаемости, выявим следующее:

ри - 80, кр - 27, то - 63, ип – 65.

Отбросив прочее, менее сочетаемые варианты получаем следующее.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| к | р | и | п | т |
| о | а | н | а | л |
| и | з | \_ | о | ч |
| е | н | ь | \_ | с |
| л | о | ж | е | н |

Получаем текст: криптоанализ слишком сложен.

Шифр «ПКЕЕРРПО\_ЙУСТ\_ИТПСУТЛЯЕИН» содержит 25. Мы сможем записать его в таблицу 5 на 5. Зная, что шифрование проводилось по столбцам, следовательно расшифрование следует проводить таким же путем

Второй шифр расшифруем прежним способом.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п | к | е | е | р |
| р | п | о | \_ | й |
| у | с | т | \_ | и |
| т | п | с | у | т |
| л | я | е | и | н |

Воспользовавшись таблицей сочетаемости, выявим следующее:

пе - 68, ре - 80, ер – 88.

Отбросив прочее, менее сочетаемые варианты получаем следующее.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п | е | р | е | к |
| р | о | й | \_ | п |
| у | т | и | \_ | с |
| т | с | т | у | п |
| л | е | н | и | я |

Получаем текст: перекрой пути пре «ст» ступления.

Для шифра двойной столбцовой перестановки рассмотрим два примера:

1. АВАРНСЧАА\_НЕДВЕДЕРПЕОЙ\_ИС
2. П\_БИРДЛЬНЕВ\_ОП\_ОПЗДЕВЫГЕА

Шифр «АВАРНСЧАА\_НЕДВЕДЕРПЕОЙ\_ИС» содержит 25. Мы сможем записать его в таблицу 5 на 5. Зная, что шифрование проводилось по столбцам, следовательно расшифрование следует проводить таким же путем

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| А | В | А | Р | Н |
| С | Ч | А | А | \_ |
| Н | Е | Д | В | Е |
| Д | Е | Р | П | Е |
| О | Й | \_ | И | С |

Воспользовавшись таблицей сочетаемости, выявим следующее:

АВ – 88, ВА – 97, РН - 20, НА - 80, АВ – 12.

Отбросив прочее, менее сочетаемые варианты получаем следующее.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Р** | **Н** | **А** | **В** | **А** |
| А | \_ | А | Ч | С |
| В | Е | Д | Е | Н |
| П | Е | Р | Е | Д |
| И | С | \_ | Й | О |

На 4 строке мы получили «перед»

Теперь воспользуемся строковой перестановкой.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| П | Е | Р | Е | Д |
| А | Ч | А | \_ | С |
| В | Е | Д | Е | Н |
| И | Й | \_ | С | О |
| **Р** | **В** | **А** | **Н** | **А** |

Получаем текст: передача сведений сорвана.

Шифр **«**П\_БИРДЛЬНЕВ\_ОП\_ОПЗДЕВЫГЕА» содержит 25. Мы сможем записать его в таблицу 5 на 5. Зная, что шифрование проводилось по столбцам, следовательно расшифрование следует проводить таким же путем

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| П | \_ | Б | И | Р |
| Д | Л | Ь | Н | Е |
| В | \_ | О | П | \_ |
| О | П | З | Д | Е |
| **В** | **Ы** | **Г** | **Е** | **А** |

Первая строка содержит малую возможность сочетания и, следовательно, воспользуемся 4 строкой.

Воспользовавшись таблицей сочетаемости, выявим следующее:

ЗД – 49, ОЕ – 88, ПО - 40.

Отбросив прочее, менее сочетаемые варианты получаем следующее.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \_ | П | Р | Б | И |
| Л | Д | Е | Ь | Н |
| \_ | В | \_ | О | П |
| П | О | Е | З | Д |
| **Ы** | **В** | **А** | **Г** | **Е** |

На 4 строке мы получили «поезд»

Теперь воспользуемся строковой перестановкой.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| П | О | Е | З | Д |
| \_ | П | Р | Б | И |
| **Ы** | **В** | **А** | **Г** | **Е** |
| \_ | В | \_ | О | П |
| Л | Д | Е | Ь | Н |

Получаем текст: ПОЕЗД «ПРЕБЫВАЕТ» ПРБИЫВАГЕ В «ПОЛДЕНЬ» ОПЛДЕБН.