Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Кафедра информатики и прикладной математики

Методы и средства защиты компьютерной информации

Метод вероятных слов

Лабораторная работа 4

Вариант 17

Старался: Шкаруба Н.Е.

Группа: P3418

Цель работы:

Научиться методу шифрования и расшифровки текста методом вижинера.

Расшифрованный текст с обычным ключем

```
Е ЪНСЩ ОРЗКЯРЧ УЪНЯХЧЕОЕКЮЗЦЛЧЬЕСЙЭОЩПДВЦ ТСФЧВЪФУМЗКХЦСАЪТУБРГМПОЧ З НЭОХТПУИСПКГЩР ЬПДУУ КЧОЦ ЦГВ
ЕСЛИ СООБЩЕНИЕ ДЛИННЕЕ ЧЕМ ДЛИНА БЛОКА СООТВЕТСТВУЮЩЕГО АЛГОРИТМА ТО ОНО РАЗБИВАЕТСЯ НА БЛОКИ СООТВ
АППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТА

ФАЦГКДЮЗФОСМЭИЬЙДАШЪЧФЫДАЦВЛФУТЪССБЪЭПСМ ПЭЪТРНГСНОЗСЩЭУЕПКСХЧОРГУЦРЮО АНСЬЪК ЧХ КТНЬЙСЪЗЩНПЕКЯРРМЧ
ЕТСТВУЮЩЕЙ ДЛИНЫ ПРИЧЕМ ПОСЛЕДНИЙ БЛОК ДОПОЛНЯЕТСЯ В СЛУЧАЕ НЕОБХОДИМОСТИ ФИКСИРОВАННЫМИ ЗНАЧЕНИЯМИ
ППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАП
```

Ключ

АППЕТИТ

Протокол расшифровки обычного ключа

1) Попробовав примерно все слова из предложенных, я ничего не разглядел. Были похожие слова БУКВА - МАНИЕ, ШИФРО - УЮЩЕМ, но подолгу копавшись в них, я их бросал.

2) На следующий день решил пройтись по всем словам заново, более аккуратно. СООБЩЕНИЕ подошло, показав ИТАППЕТИТ, в котором я разглядел АППЕТИТ, и смог расшифровать остальное.

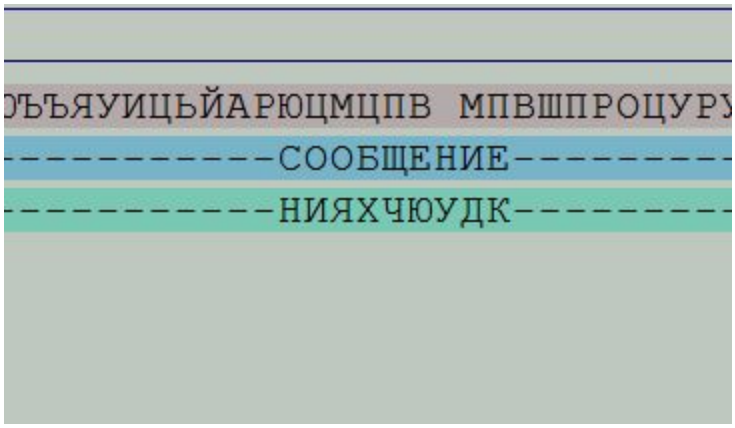
```
Е ЪНСЩ ОРЗКЯРЧ УЪНЯХЧЕОЕКЮЗЦЛЧЬЕСЙЭОЩПДВЦ ТСФЧВЪФУМЗКХЦСАЪТУБРГМПОЧ З НЭОХТПУИСПКГЩР ЬПДУУ КЧОЦ ЦГВ
ЕСЛИ СООБЩЕНИЕ ДЛИННЕЕ ЧЕМ ДЛИНА БЛОКА СООТВЕТСТВУЮЩЕГО АЛГОРИТМА ТО ОНО РАЗБИВАЕТСЯ НА БЛОКИ СООТВ
АППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТА

ФАЦГКДЮЗФОСМЭИЬЙДАШЪЧФЫДАЦВЛФУТЪССБЪЭПСМ ПЭЪТРНГСНОЗСЩЭУЕПКСХЧОРГУЦРЮО АНСЬЪК ЧХ КТНЬЙСЪЗЩНПЕКЯРРМЧ
ЕТСТВУЮЩЕЙ ДЛИНЫ ПРИЧЕМ ПОСЛЕДНИЙ БЛОК ДОПОЛНЯЕТСЯ В СЛУЧАЕ НЕОБХОДИМОСТИ ФИКСИРОВАННЫМИ ЗНАЧЕНИЯМИ
ППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАППЕТИТАП
```

Бегущий ключ

ЕСТЬ ТОЛЬКО МИГ МЕЖДУ ПРОШЛЫМ И БУДУЩЕМ ИМЕННО ОН НАЗЫВАЕТСЯ

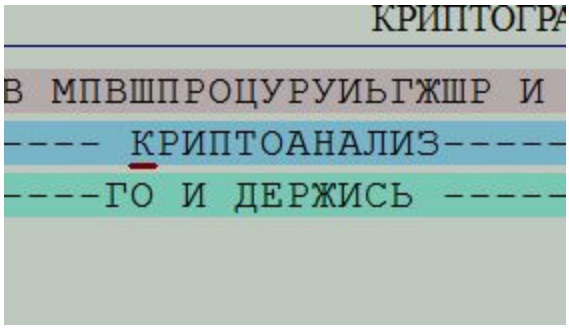
Протокол расшифровки бегущего ключа

1) Ищу хоть что-то

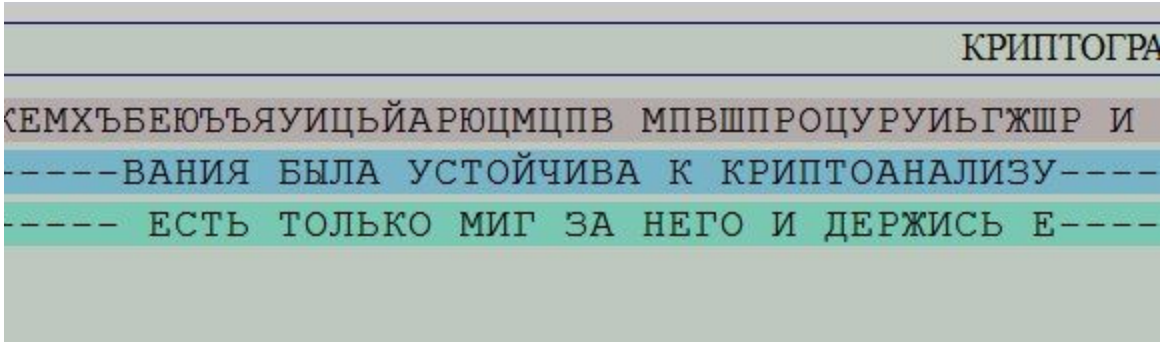


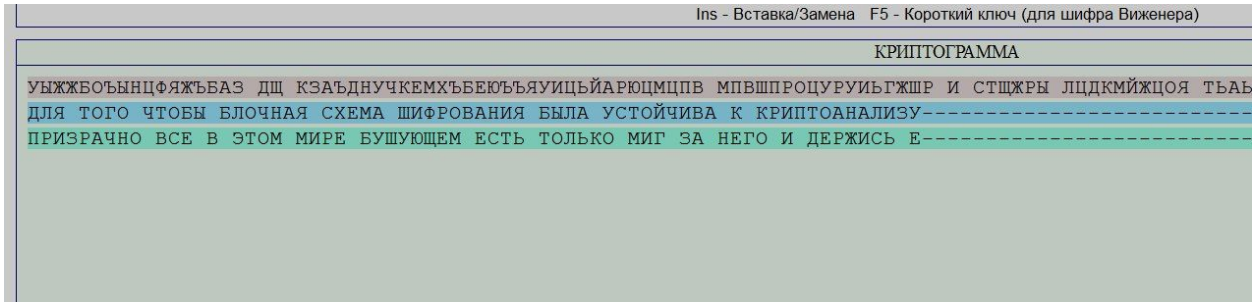
2) СООБЩЕНИЕ, ЗАДАЧА, КРИПТОГРАФИЯ, МЕТОДне подошли.

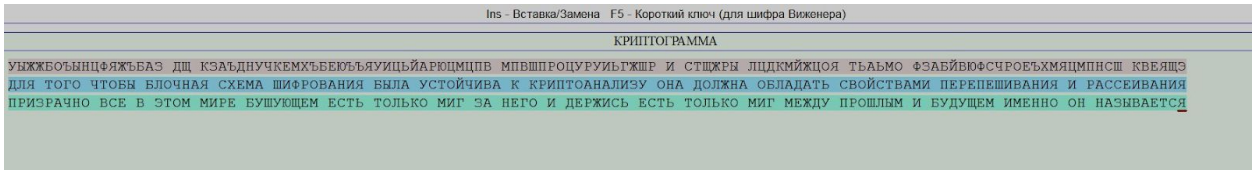
3) КРИПТОАНАЛИЗ выстрелил,осталось найти остальное



4) Далее играясь с словами я нашел решение, это песня Олега Даля :)







Спасибо за внимание! Лабораторная была очень сложная, потому что в описании работы были перепутаны названия файлов, в которых нужно было искать ключи. Написано:
Для вижинера файл имеет вид word_rkNN.kr
Для бегущего ключа файл имеет вид word_vNN.kr
Так вот, наоборот надо, ибо rk значит running key, а v - vigenere.