**Отчёт по 1 лабораторной работе**

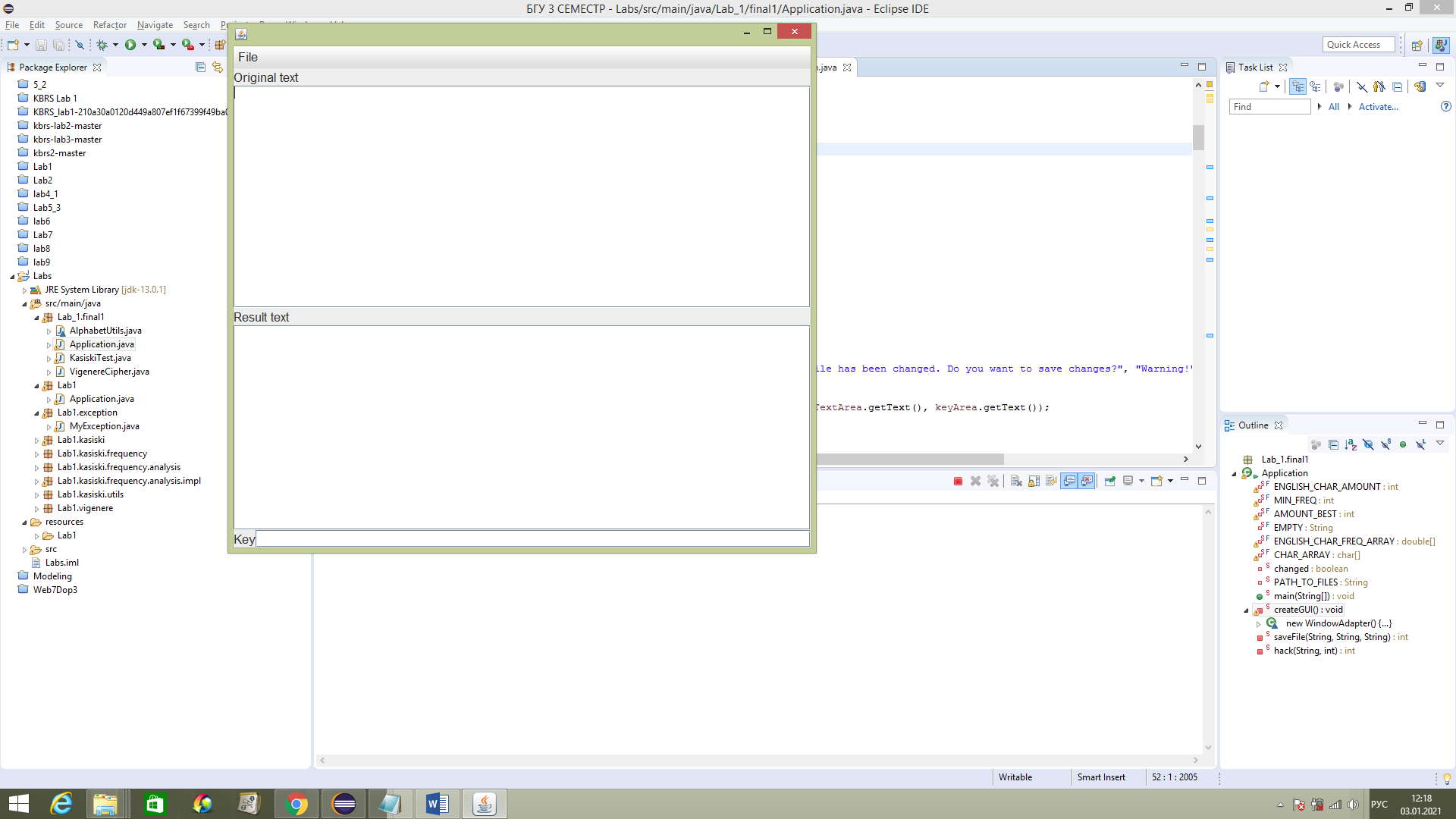
**Лозовский Максим**

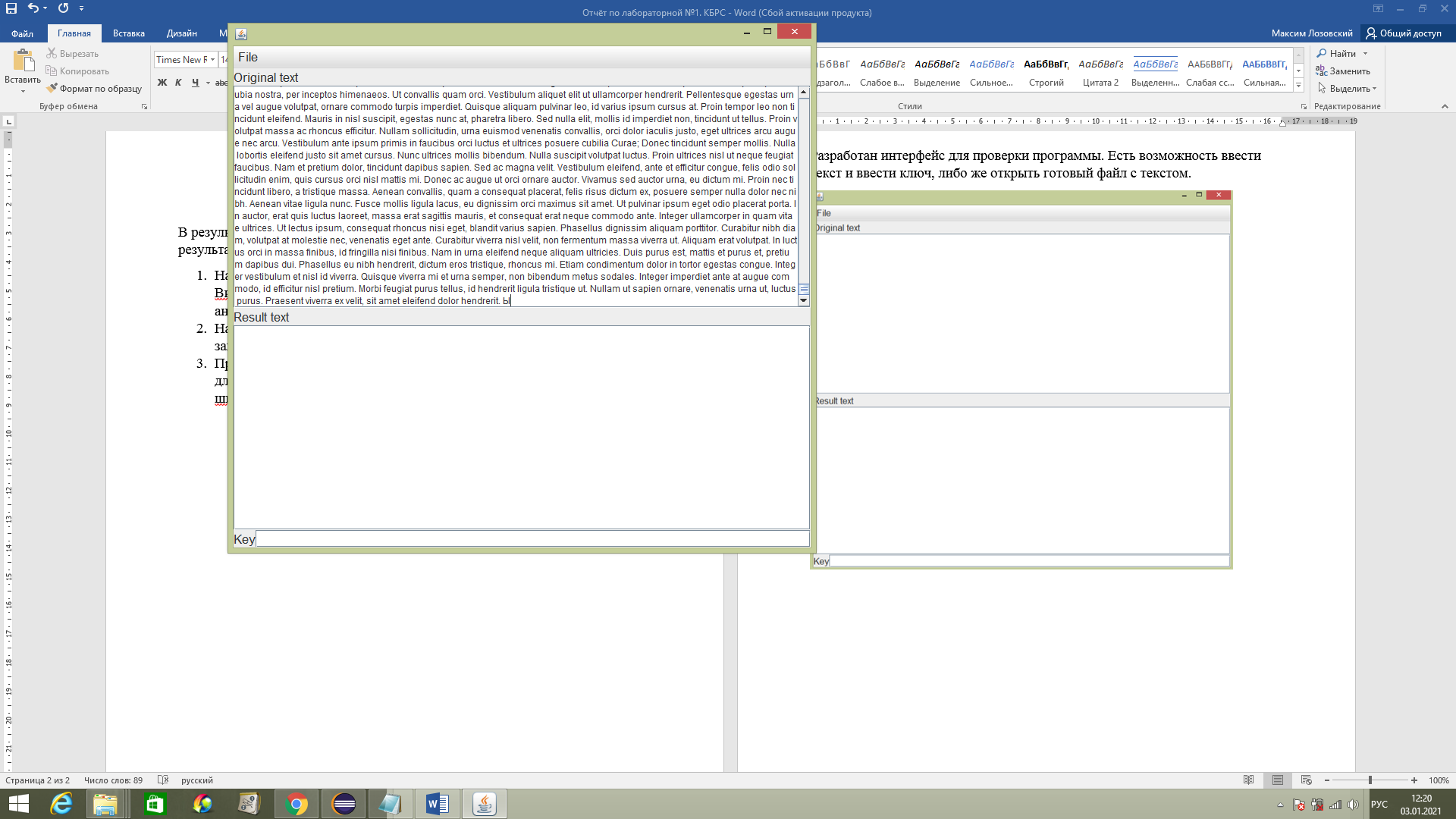
**4 курс 12 группа кафедра КТС**

В результате проведения лабораторной работы бли достигнуты следующие результаты:

1. Написана программное средство, которое осуществляет по методу Виженера шифрование и дешифрование текстового файла на английском языке
2. Написано программное средство, которое проводит анализ зашифрованного текста с помощью теста Касиски.
3. Проведены исследования зависимости вероятности успешной атаки от длины использованного при шифровании ключевого слова и от длины шифротекста.

Разработан интерфейс для проверки программы. Есть возможность ввести текст и ввести ключ, либо же открыть готовый файл с текстом.





Написаны тесты для проверки программы. Вот результаты:

--------------------

Key : LO

Possible key lengths for Kasiski are :

- Key length: 12 Occurences: 42

- Key length: 18 Occurences: 42

- Key length: 8 Occurences: 41

Text length to hack : 205

Prospective keys :

lilololololo | lololoaolildsololo | lolololo |

--------------------

Key : SAP

Possible key lengths for Kasiski are :

- Key length: 12 Occurences: 43

- Key length: 18 Occurences: 43

- Key length: 8 Occurences: 41

Text length to hack : 205

Prospective keys :

supsapsapsap | sapsaphapmaezapsap | sapwalea |

--------------------

Key : BOBA

Possible key lengths for Kasiski are :

- Key length: 12 Occurences: 43

- Key length: 18 Occurences: 43

- Key length: 8 Occurences: 41

Text length to hack : 205

Prospective keys :

bibabobaboba | bobablqabpboiabdbo | bobaboba |

--------------------

Key : LODKA

Possible key lengths for Kasiski are :

- Key length: 10 Occurences: 23

- Key length: 14 Occurences: 19

Text length to hack : 205

Prospective keys :

lodkalodka | etplrzzhbwvwkp |

--------------------

Key : SYSTEM

Possible key lengths for Kasiski are :

- Key length: 12 Occurences: 43

- Key length: 18 Occurences: 43

- Key length: 8 Occurences: 41

Text length to hack : 205

Prospective keys :

ssstemsystem | systemhysnebzystem | sistsysy |

--------------------

Key : SEVENTH

Possible key lengths for Kasiski are :

- Key length: 14 Occurences: 20

- Key length: 10 Occurences: 19

Text length to hack : 205

Prospective keys :

sejenthsevexth | zhotcexivn |

--------------------

Key : ZORACHKA

Possible key lengths for Kasiski are :

- Key length: 8 Occurences: 41

- Key length: 12 Occurences: 41

- Key length: 18 Occurences: 41

Text length to hack : 205

Prospective keys :

zorachka | zovardjanwba | oscmztjamugpjmrdrp |

--------------------

Key : VILKAZOOM

Possible key lengths for Kasiski are :

- Key length: 12 Occurences: 43

- Key length: 18 Occurences: 43

- Key length: 8 Occurences: 41

Text length to hack : 205

Prospective keys :

kunkawoamvaa | vilkazdompiarazoom | mwdtaiaa |

--------------------

Key : qwertyuiop

Possible key lengths for Kasiski are :

- Key length: 10 Occurences: 23

- Key length: 14 Occurences: 19

Text length to hack : 205

Prospective keys :

qwertyuiop | qmlgeyeuuinmrl |

--------------------

Key : PrivetLalka

Possible key lengths for Kasiski are :

- Key length: 11 Occurences: 4

- Key length: 10 Occurences: 3

- Key length: 5 Occurences: 1

- Key length: 6 Occurences: 1

- Key length: 19 Occurences: 1

Text length to hack : 205

Prospective keys :

privetlalka | kfmazlvekj | lleaz | alball | elbazzziasxtyzveuyb |

--------------------

Key : PRIVET

Possible key lengths for Kasiski are :

- Key length: 6 Occurences: 132598313

Text length to hack : 66004

Prospective keys :

privet |