

ГОСУДАРСТВЕННОЕ ПРОФЕССИОНАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ
«Техникум им. С.П. Королева»

Разработка программного продукта криптографической защиты данных

Выполнил:
Студент группы 202 Д
Руководитель: Соломатин Юрий Семенович

2017 год

Цель дипломной работы:

- Изучить типы и виды криптографических систем, а также написать программу для шифровки и расшифровки текста

Задачи дипломной работы:

- Изучить виды криптосистем
- Разобрать примеры работы этих систем
- Изучить виды шифров(с открытым и закрытым ключом)
- Написать универсальную программу

Актуальность дипломной работы:

- Криптография сейчас касается самых разных сторон жизни общества. Любой человек сейчас сталкивался со словом «шифр» «криптограмма» и «ключ». Даже чтобы правильно действовать на просторах интернета необходимо иметь представление хотя бы об основах криптографии.
- Современная криптография образует отдельное научное направление на стыке математики и информатики. Практическое применение криптографии стало неотъемлемой частью жизни современного общества - её используют в таких отраслях как электронная коммерция, электронный документооборот, телекоммуникации и других. Особенно развитию криптографии повлияли не только новые технические возможности, но и сравнительно широкое распространение криптографии для использования частными лицами.

Что такое криптография

Криптография - наука о методах обеспечения конфиденциальности, целостности данных и аутентификации.

Основные задачи криптографии

- Конфиденциальность
- Целостность передачи данных
- Аутентификация
- Невозможность отказа от авторства

Криптография разделена на две взаимодействующие части

- *Криптосинтез* - занимается разработкой и обоснованием стойкости криптографических средств защиты информации.
- *Криптоанализ* – исследование о том может ли злоумышленник расшифровать информации без знания ключа и как же.

Основные понятия в криптографии

- **Шифровка** - обратимое преобразование информации в целях скрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней.
- **Дешифровка** - обратный процесс шифрования.

Основные понятия в криптографии

- **Ключ** - это секретная информация, используемая криптографическим алгоритмом при зашифровании/расшифровании сообщений, постановке и проверке цифровой подписи.
- **Криптографическая стойкость** - это способность криптографического алгоритма противостоять криптоанализу.
- **Имитозащита** - это защита от внедрения ложной информации.
- **Имитовставка** - специальный набор символов, который добавляется к сообщению, предназначен для обеспечения его целостности и аутентификации источника данных.

Виды ключей

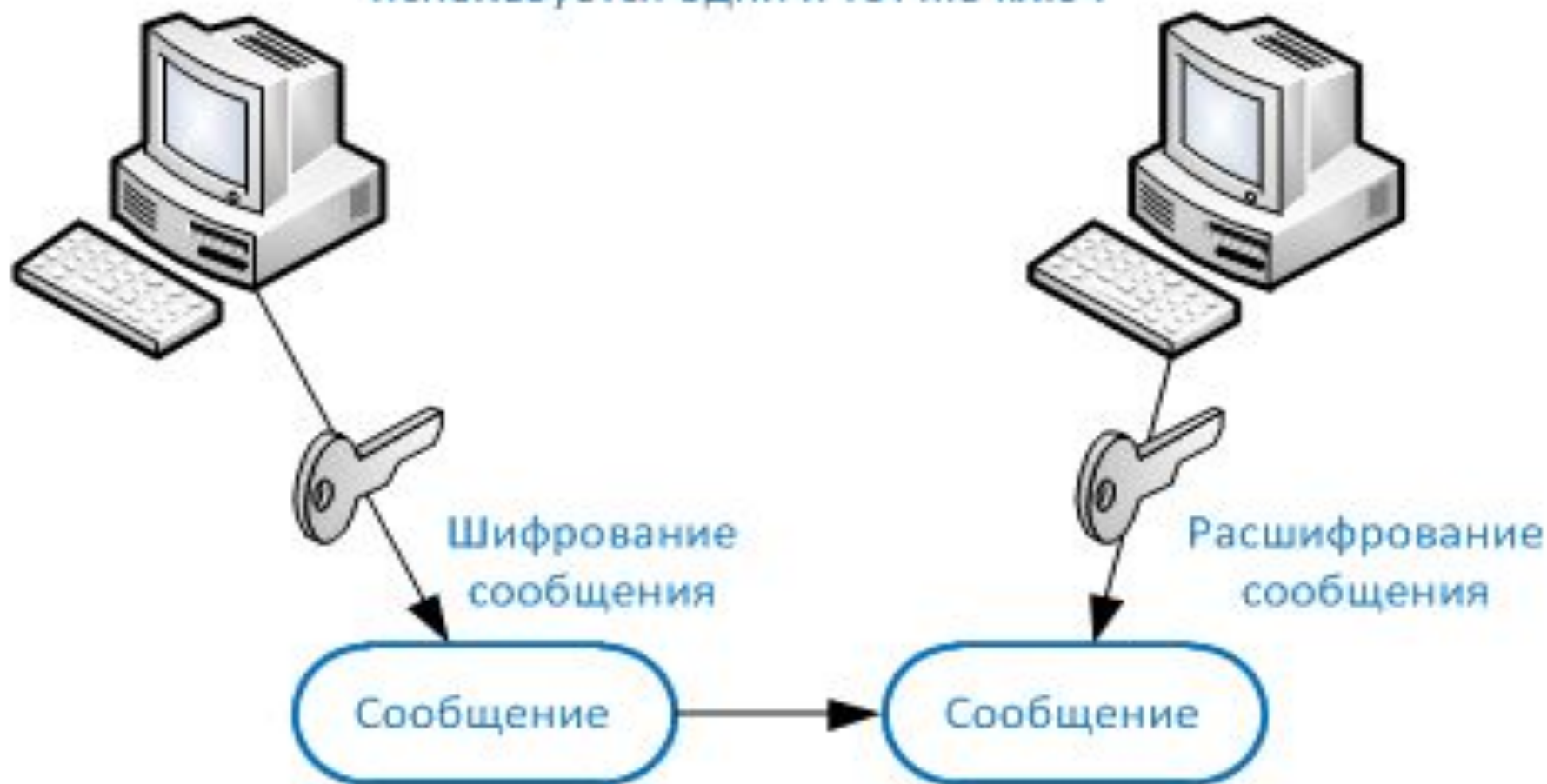
- Секретный ключ - специальный параметр криптографического алгоритма, знакомый одному или нескольким сообщникам и не знакомый неприятелю и оппоненту.
- Публичный ключ - специальный параметр криптографического алгоритма, знакомый всем сообщникам, охватывая конкурента и неприятеля. Находится в конкретном соотношении со скрытым ключом.

Алгоритмы криптосистем

1. Симметричные
2. Асимметричные

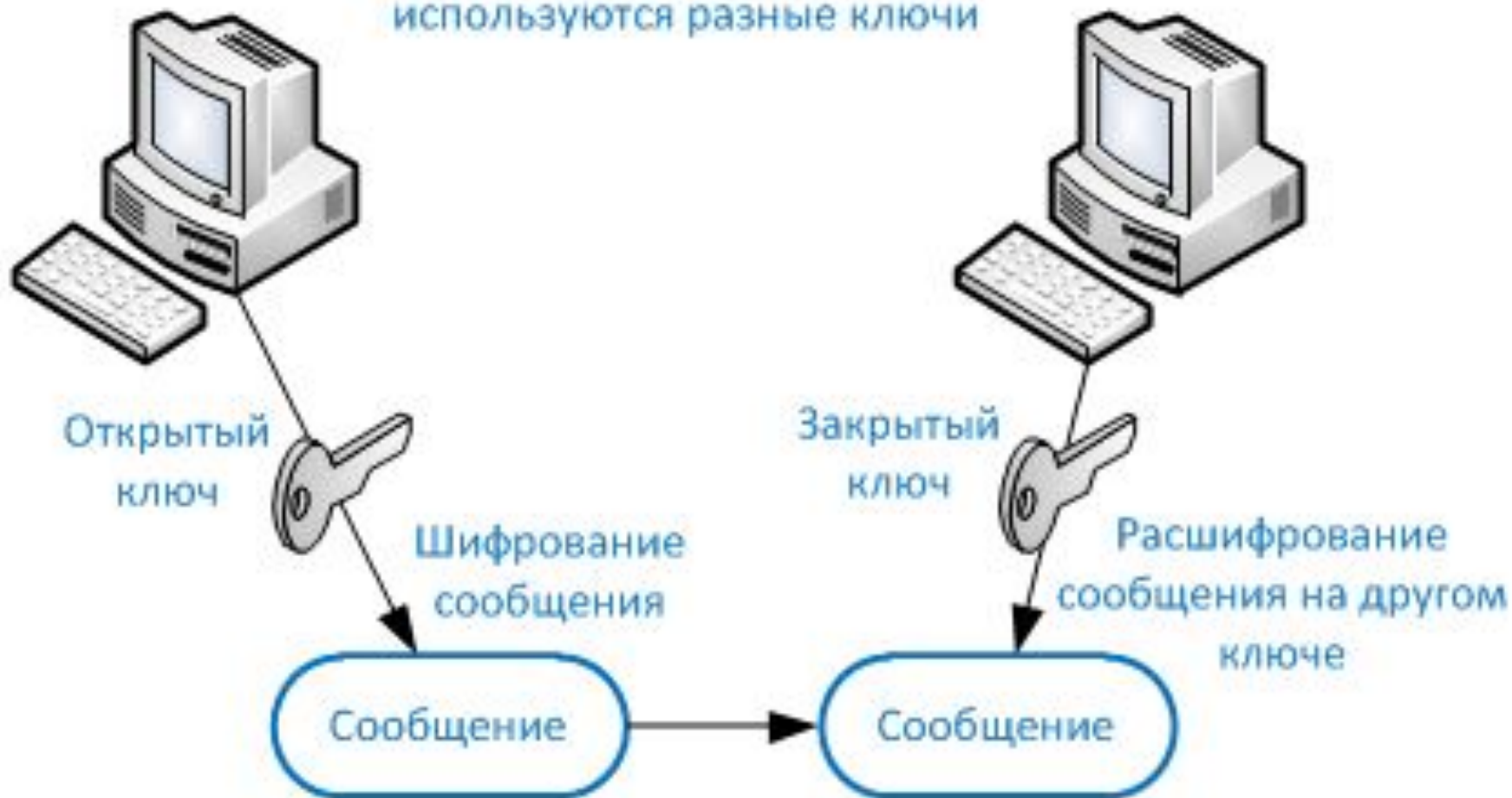
Симметричный алгоритм

В симметричных алгоритмах шифрования
используется один и тот же ключ



Асимметричный алгоритм

В асимметричных алгоритмах для зашифрования и расшифрования используются разные ключи



Модель исследуемой предметной области:



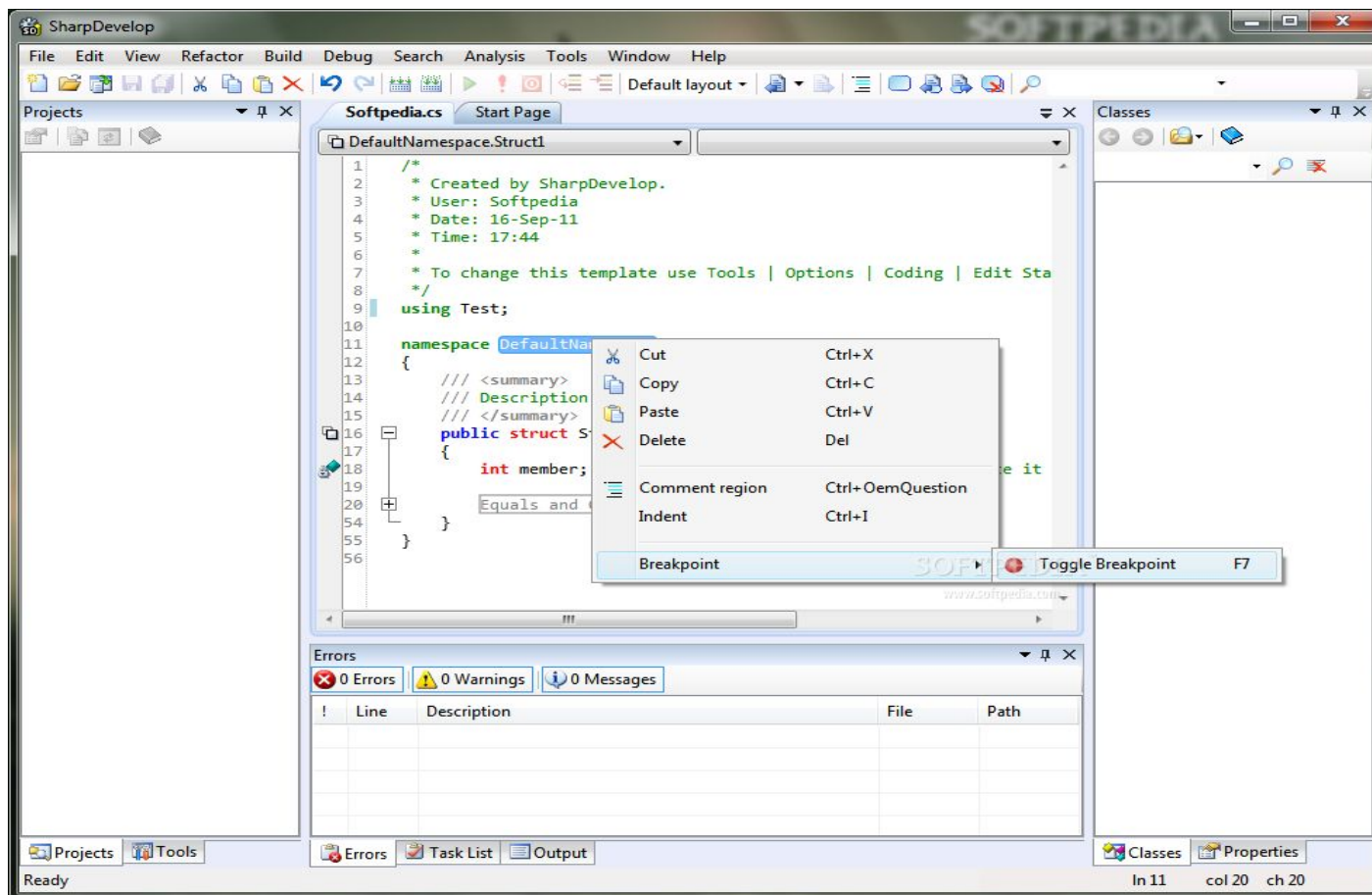
Обоснование выбора языка программирования:

В качестве языка программирования был выбран язык C#.

- C# является полностью объектно-ориентированным языком, где даже виды, встроенные в язык, представлены посредством классов;
- C# является мощным объектным языком с возможностями наследования и универсализации;
- C# является наследником языков C/C++, сохраняя лучшие черты этих популярных языков программирования. У C# общий с этими языками синтаксис, знакомые операторы языка облегчают переход программистов от C++ к C#;
- Сохранив основные черты своего великого родителя, язык стал надежнее и проще. Простота и надежность, главным образом, связаны с тем, что на C# хотя и допускаются, но не поощряются такие опасные свойства C++ как же указатели, адресация, разыменовывание, адресная арифметика;

Обоснование выбора среды разработки:

- В качестве среды разработки я выбрал свободно распространяемую среду SharpDevelop.



Интерфейс программного продукта

The screenshot shows a software window titled "ИВА" (IWA) with standard Windows window controls (minimize, maximize, close). The interface is divided into two main vertical panels. The left panel contains two large empty rectangular areas for file operations. Below these are two buttons: "Шифровать" (Encrypt) and "Дешифровать" (Decrypt). At the bottom of the left panel is a button with the text "<=====".

The right panel also contains two large empty rectangular areas. Below these are two input fields: "Введите ключ шифрования:" (Enter encryption key:) and "Язык шифрования и дешифрования:" (Encryption and decryption language:). The language field is currently set to "Русский" (Russian) with a dropdown arrow. At the bottom of the right panel is a button with the text "=====>".

At the top of the window, there is a menu bar with the following items: "Файл" (File), "Справка" (Help), and "Нет нужного формата?" (No required format?).

Пример работы

IBA

Файл

Справка

Нет нужного формата?

Зашифровано: 1 раз

привет

уфмжйц

Шифровать

Введите ключ шифрования:

4

Дешифровать

Язык шифрования и дешифрования:

Русский

<=====

=====>

Реализация шифрования

```
113 for (int i = 0; i < poluch.Length; i++)
114     {
115         if (((int)(poluch[i]) < 1040) || ((int)(poluch[i]) > 1103))
116             result += poluch[i];
117         if ((Convert.ToInt16(poluch[i]) >= 1072) && (Convert.ToInt16(poluch[i]) <= 1103))
118         {
119             if (Convert.ToInt16(poluch[i]) + shift > 1103)
120             {
121                 result += Convert.ToChar(Convert.ToInt16(poluch[i]) + shift - 32);
122             }
123             else
124             {
125                 result += Convert.ToChar(Convert.ToInt16(poluch[i]) + shift);
126             }
127         }
128         if ((Convert.ToInt16(poluch[i]) >= 1040) && (Convert.ToInt16(poluch[i]) <= 1071))
129         {
130             if (Convert.ToInt16(poluch[i]) + shift > 1071)
131                 result += Convert.ToChar(Convert.ToInt16(poluch[i]) + shift - 32);
132             else
133                 result += Convert.ToChar(Convert.ToInt16(poluch[i]) + shift);
134         }
135     }
```

Реализация дешифрования

```
231     for (int i = 0; i < poluch2.Length; i++)
232     {
233         if (((int)(poluch2[i]) < 1040) || ((int)(poluch2[i]) > 1103))
234             result2 += poluch2[i];
235         if ((Convert.ToInt16(poluch2[i]) >= 1072) && (Convert.ToInt16(poluch2[i]) <= 1103))
236         {
237             if (Convert.ToInt16(poluch2[i]) - shift > 1103)
238             {
239                 result2 += Convert.ToChar(Convert.ToInt16(poluch2[i]) - shift + 32);
240             }
241             else
242             {
243                 result2 += Convert.ToChar(Convert.ToInt16(poluch2[i]) - shift);
244             }
245         }
246         if ((Convert.ToInt16(poluch2[i]) >= 1040) && (Convert.ToInt16(poluch2[i]) <= 1071))
247         {
248             if (Convert.ToInt16(poluch2[i]) - shift > 1071)
249                 result2 += Convert.ToChar(Convert.ToInt16(poluch2[i]) - shift + 32);
250             else
251                 result2 += Convert.ToChar(Convert.ToInt16(poluch2[i]) - shift);
252         }
253     }
254     richTextBox1.Text=result2;
255 }
```

Структура затрат на создание дипломной работы

Затраты на выполнение проекта:

$$K = C_{\text{ЗАРП.}} + C_{\text{ОБ.}} + C_{\text{ОРГ.}} + C_{\text{НАКЛ.}}$$

$$K = 17024 + 887 + 13860 + 1964 = 33735$$

руб.

Затраты на внедрение проекта:

$$K_{\text{ВН.}} = C_{\text{ВН.ЗАРП.}} + C_{\text{ВН.НАКЛ.}}$$

$$K_{\text{ВН.}} = 1135 + 131 = 1266 \text{ руб.}$$

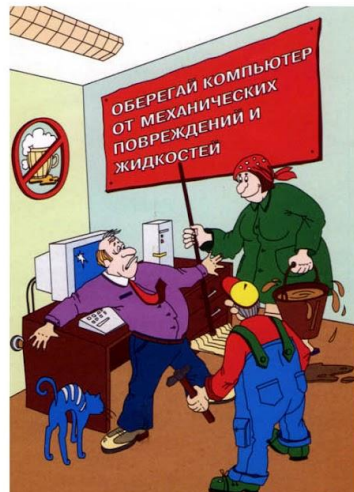
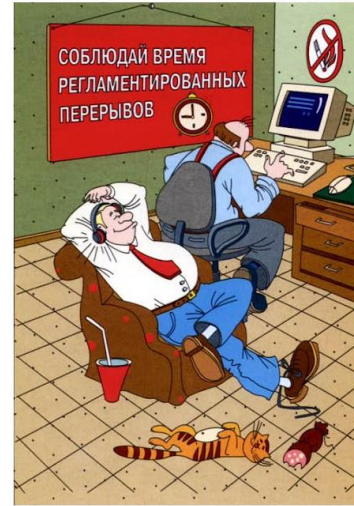
ОБЩИЕ ЗАТРАТЫ:

$$K_{\text{ОБ.}} = K_{\text{ВН.}} + K$$

$$K_{\text{ОБ.}} = 1266 + 33735 = 35001 \text{ руб.}$$



Охрана труда и безопасность жизнедеятельности



Доклад окончен.

Спасибо за внимание!