ПРОГРАММНЫЙ ПРОДУКТ ДЛЯ СОПРОВОЖДЕНИЯ КУРСА «КРИПТОГРАФИЯ И ОХРАНА КОММЕРЧЕСКОЙ ИНФОРМАЦИИ»

С. А. Голгофская, Ю. Р. Черницкая, П. В. Шумигай

Гродненский Государственный Университет имени Янки Купалы
Гродно, Беларусь
E-mail: sneghana2004@mail.ru

В докладе рассматриваются особенности и актуальность применения в процессе обучения программ-визуализаторов, иллюстрирующих работу алгоритмов по шифрованию данных. Формулируются требования к функциональности подобных программ, описывается разработанный авторами программный продукт, реализующий некоторые алгоритмы шифрования.

Ключевые слова: визуализатор, алгоритмы криптографии.

Обучение при помощи визуализаторов

С точки зрения системного подхода проведение занятий преподавателем можно рассматривать как систему, на которую влияет множество факторов. К факторам, имеющим наибольшую значимость, относятся: состав аудитории слушателей, техническая оснащенность лекционного помещения, затраты времени на подготовку лекционного материала. Задачей преподавателя является обеспечение наилучшего уровня подачи материала при минимизации трудозатрат по его подготовке. На сегодняшний день одно из решений данной задачи представляет собой использование визуализаторов при обучении.

Визуализатор — это программа, в процессе работы которой на экране компьютера динамически демонстрируется применение алгоритма к выбранному набору данных. При этом доступны режимы использования входных наборов, заготовленных заранее, либо вводимых с клавиатуры. Визуализаторы позволяют изучать работу алгоритмов в пошаговом режиме, аналогичном режиму трассировки программ.

Использование визуализаторов при обучении не только уменьшает затраты времени на подготовку лекционного материала, но и способствует улучшению трудоспособности как преподавателя, так и студентов. Преподаватель может продемонстрировать поведение алгоритма на различных наборах данных, что, в свою очередь, позволит учащимся получить более широкое представление о работе изучаемого алгоритма, его сложности и различии в функционировании. Визуализация алгоритма может помочь преподавателю охватить больше материала за меньшее время. Применение таких обучающих программ позволяет повысить заинтересованность и качество

подготовки учащихся, а также способствует улучшению понимания ими лекционного материала, что в дальнейшем может привести к использованию визуализатора для проведения собственных экспериментов над структурами наборов данных. Благодаря визуализатору значительно упрощается объяснение преподавателем тем курса учащимся, которые понимают объекты более легко при визуальном или графическом представлении по сравнению со словесным. Поскольку каждый шаг алгоритма визуализатор сопровождает словесным комментарием, то он идеально подходит для самостоятельного дистанционного изучения лекционного материала.

Визуализатор, как и любой другой программный продукт, должен удовлетворять определенные функциональные требования:

- Возможность ввода данных для демонстрации алгоритма;
- Быстрая и правильная обработка вводимых данных;
- Автоматический режим работы — без вмешательства пользователя;
- Наличие комментариев для шагов алгоритма;
- Простой и понятный пользователю интерфейс.

Идеальным для преподавателя будет нахождение или написание такой программы-визуализатора, которая включает в себя несколько родственных алгоритмов, что позволит наглядно продемонстрировать общую идею, а также различие в механизмах их действия. Одним из приемов обучения может стать написание собственного визуализатора по изучаемому алгоритму [1].

Программный продукт «алгоритмы кодирования»

При запуске программного продукта появляется главное окно, на нем отображены кнопки с названиями алгоритмов шифрования (Рис. 1).

Все алгоритмы сгруппированы по видам, в данном случае это шифры замены и шифры перестановки. В пределах одной группы (шифры замены) алгоритмы могут быть так же разбиты на подгруппы, в нашем случае шифры замены представлены шифрами однозначной замены и полиалфавитным шифром.

Рассмотрим шифры, вошедшие в программный продукт.

Лозунговый шифр. Для данного шифра построение таблицы шифрозамен основано на лозунге — легко запоминаемом слове. Вторая строка таблицы шифрозамен заполняется сначала словом-лозунгом (причем повторяющиеся буквы отбрасываются), а затем остальными буквами, не вошедшие в слово-лозунг, в алфавитном порядке.

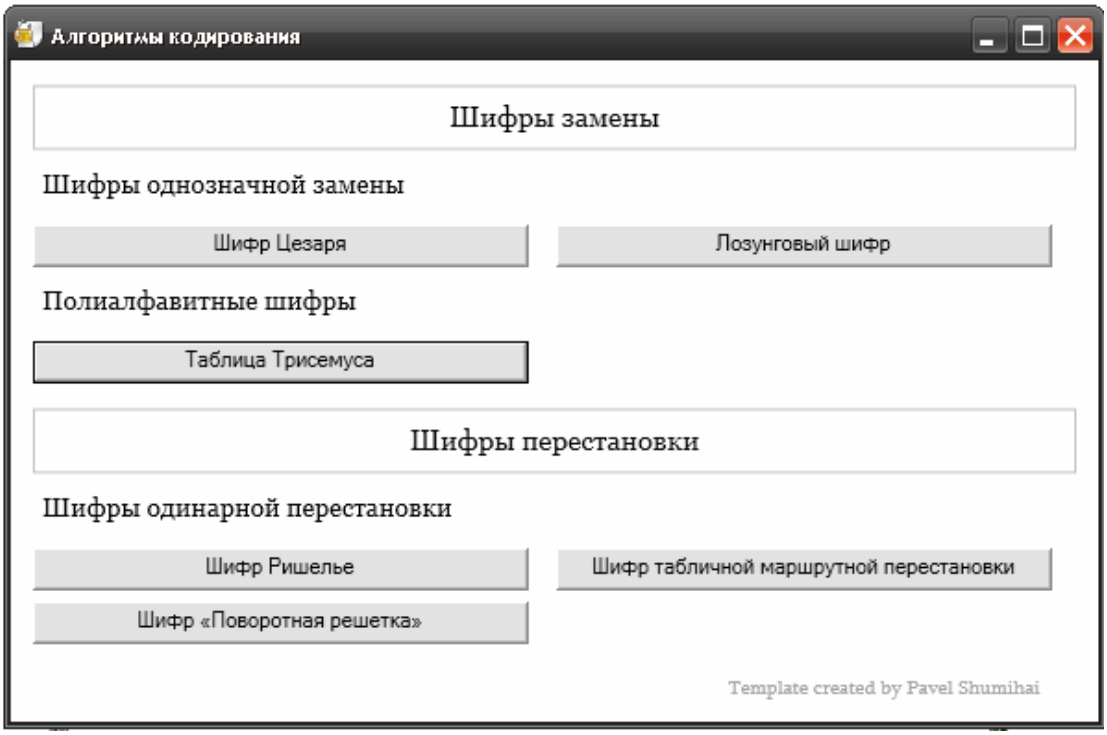

Рис. 1 — Главное окно программы

Таблица Трисемуса. В данной работе таблица Трисемуса имеет размерность 4x8. Заполняется она следующим образом: сначала записывается ключевое слово, с уже удаленными повторяющимися символами, а затем оставшиеся буквы алфавита по порядку. В данной программе используется только русский алфавит, буква «ё» заменяется на «е». При шифровании буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце. Если столбец последний, то берется буква из 1-й строки. При расшифровке берется буква на строку выше или из первой строки.

Шифр «Поворотная решетка». Для шифрования и дешифрования изготовляется трафарет с четным количеством строк и столбцов. В трафарете вырезаются клетки таким образом, чтобы при наложении его на таблицу того же размера четырьмя возможными способами, его вырезы полностью покрывали все ячейки таблицы ровно по одному разу. При шифровании трафарет накладывается на таблицу. В видимые ячейки таблицы выписываются буквы исходного текста слева-направо сверху-вниз. Далее трафарет поворачивается и вписывается следующая часть букв. Эта операция повторяется еще два раза. Шифрограмму выписывают из итоговой таблицы по определенному маршруту. Таким образом, ключом при шифровании является трафарет, порядок его поворотов и маршрут выписывания.

Шифр Ришелье. При использовании этого шифра из текста убираются все пробелы, затем на текст накладывается определенный ключ: (2741635) (15243) (671852493) (07) (28615)(943)(2741635). В соответствии с этим ключом текст разбивается на слова в соответствии с шифром если символов не хватает, вместо них добавляется знак «#», и внутри разбитых фрагментов буквы перестанавливаются соответственно заданному порядку.

Шифр табличной маршрутной перестановки. При шифровании в такую таблицу вписывают исходное сообщение по определенному маршруту, а выписывают (получают шифрограмму) — по другому. Для данного шифра маршруты вписывания и выписывания, а также размеры таблицы являются ключом.

Шифр Цезаря. Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит, затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево. При зашифровке буква А заменяется буквой Г, Б — на Д и т. д. Ключом в шифре Цезаря является величина сдвига нижней строки алфавита.

При нажатии на любую из кнопок с название шифра, открывается окно, представленное на рисунке 2. Название окна соответствует выбранному алгоритму.

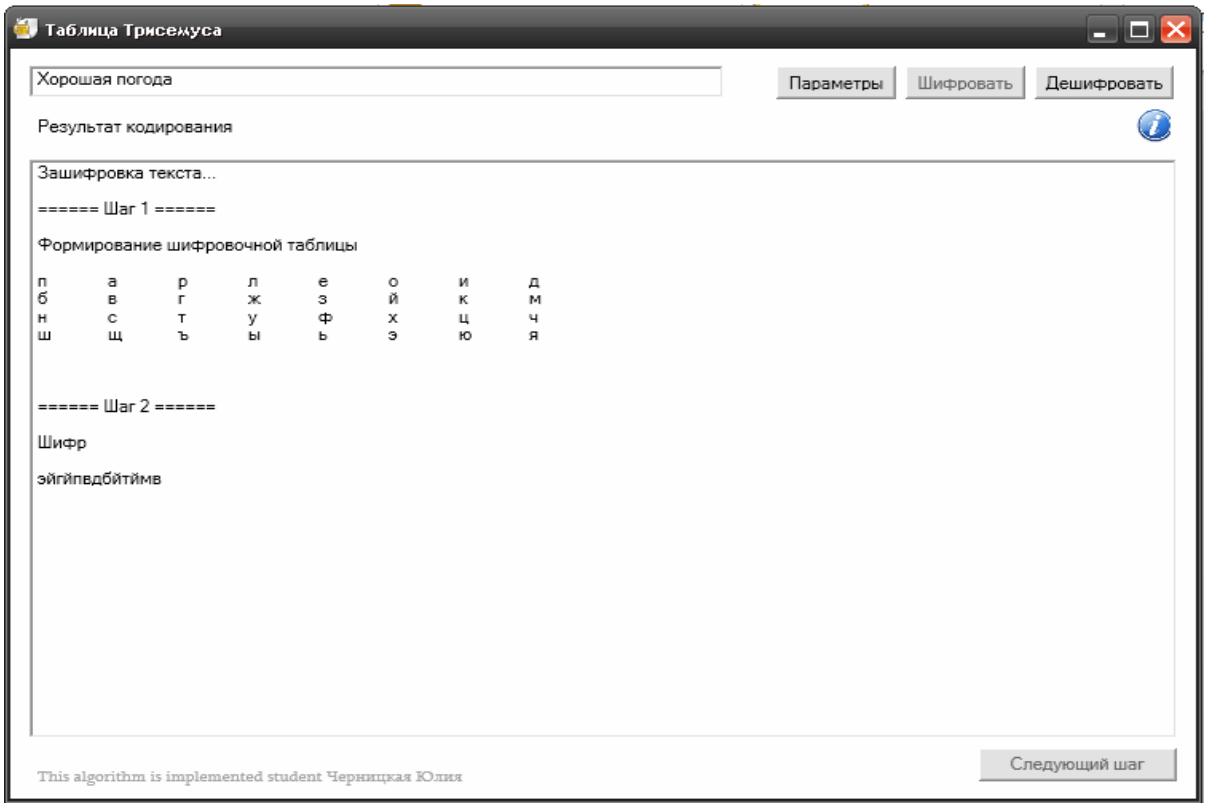

Рис. 2 — Окно алгоритма кодирования

Оно содержит два текстовых поля: для ввода строки для шифрования и поле для вывода результатов кодирования. Имеются также кнопки «Шифровать» и «Дешифровать» для зашифровки и расшифровки введенной строки соответственно. Если работа алгоритма происходит за некоторое число шагов, то внизу окна появляется кнопка «Следующий шаг», при нажатии на которую происходит пошаговое выполнение алгоритма.

Если алгоритм требует ввода дополнительных параметров, то необходимо кликнуть по кнопке «Параметры», при этом откроется окно для ввода параметров (Рис. 3).

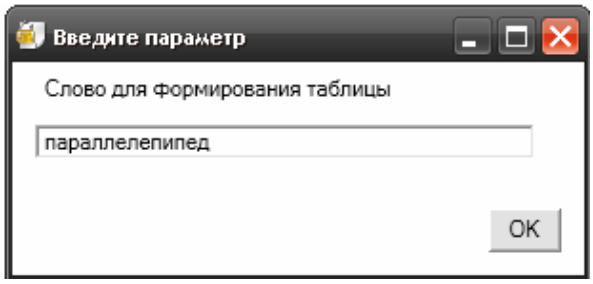

Рис. 3 — Окно ввода параметров

При нажатии на кнопку  открывается окно с описанием работающего алгоритма (Рис. 4).

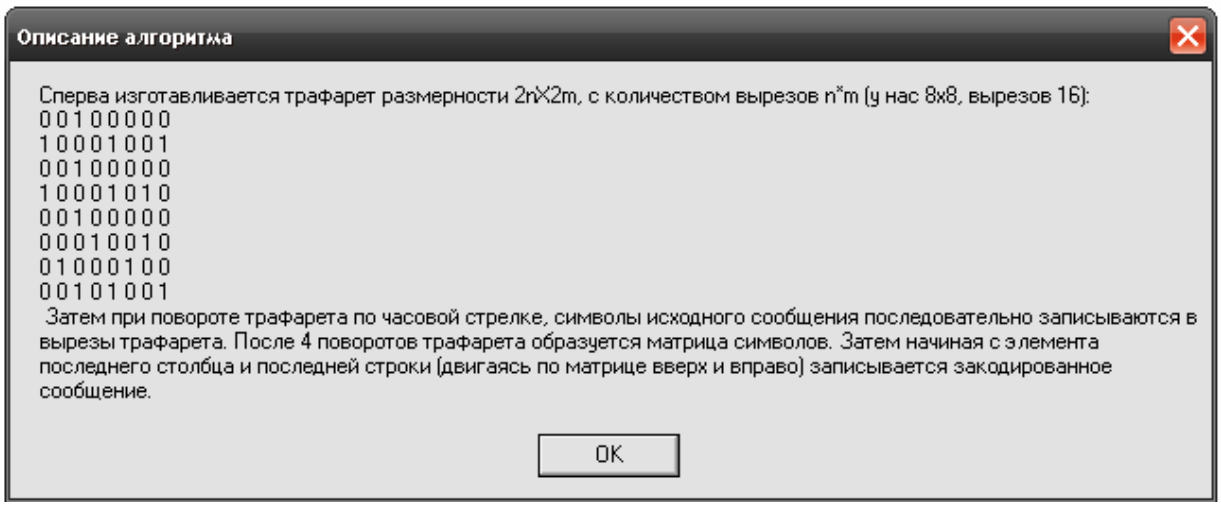

Рис. 4 — Информационное окно

Подведение итогов. Разработанный софт может использоваться преподавателем криптографии как дополнительный атрибут для проведения лекций, т.к. он позволяет наглядно демонстрировать работу различных алгоритмов.

Минимальные системные требования для работы визуализатора: операционная система Windows XP, оперативная память 256 Мб RAM, процессор 1,5 GHz, видеокарта 128 Мб.

Перспективами развития данной темы является внедрение в нашу программу большего числа алгоритмов шифрования.

Литература

1. Баричев С.Г, Серов Р.Е. Основы современной криптографии: Учебное пособие. - М.: Горячая линия - Телеком, 2002. – 76.
2. Голгофская, С.А. Обучающая программа – визуализатор алгоритма направленного перебора по векторной решетке / С.А. Голгофская, О.Б. Цехан // Информатизация образования – 2012: педагогические основы разработки и использования электронных образовательных ресурсов. Материалы межд. научн. конф. Мн., 2012. С. 79-84.
3. Нечаев В.И. Элементы криптографии (Основы теории защиты информации). М.: Высшая школа, 1999. – 109 с.
4. Рябко Б.Я., Фионов Ф.Н. Криптографические методы защиты информации: Учебное пособие для вузов. – М: Горячая линия – Телеком, 2005. – 229с.