ли сгенерированы случайные несимметричные матрицы для диапазонов [5,20], [5,25],…,[5,300]. Для проведения одного шага эксперимента при фиксированных значениях размерности и диапазона были сформированы 30 случайных несимметричных матриц стоимости. Для каждой матрицы было выполнено приведение, результат шага эксперимента – среднее количество нулей.

На рис.1 представлены результаты исследования зависимости количества нулей от диапазона значений в матрице стоимости. Нижний график (соответствующий размерности матрицы 15) показывает, что количество нулей практически не зависит от диапазона случайных значений в матрице. Верхний график показывает зависимость количества нулей для размерности матрицы 100.

Библиографический список

1. Сигал И., Иванова А. Введение в прикладное дискретное программирование: модели и вычислительные алгоритмы. – М.: ФИЗМАТЛИТ, 2003.
2. Макаркин С., Мельников Б., Мельникова Е. Задача коммивояжёра и проблема адекватности математических моделей. // Сборник трудов межд. научн. конф. «Образование, наука и экономика в вузах и школах. Интеграция в международное образовательное пространство», Ереван, Армения, 2014.

АНАЛИЗ КРИПТОСИСТЕМЫ МАШИНЫ «ЭНИГМА»

В. Абакумова, А. Шашкина
1 курс, факультет экономики и управления
Научный руководитель – доц. **Е.А. Мельникова**

Энигма – наиболее знаменитая из роторных шифровальных машин. Она состояла на вооружении Германских войск во время второй мировой войны [1]. Для механизации процесса шифрования брался полый диск с нанесенными с двух сторон контактами, соответствующими алфавитам открытого и шифрованного текста, причем контакты соединялись между собой по некоторой подстановке, называемой коммутацией диска. Эта коммутация определяла замену букв в начальном угловом положении. При изменении углового положения диска изменялась и соответствующая замена на сопряженную подстановку [2].

Принцип работы «Энигмы» заключался в постоянном изменении электрической цепи за счёт вращения внутренних роторов, через которые шёл ток. При каждом нажатии буквы на клавиатуре машина выдавала букву шифра, а роторы становились в новую позицию. Таким образом работал полиалфавитный шифр подстановки. Простой версией полиалфавитного шифра является шифр Вижнера [3]. За счет вращения дисков конкретная буква текста замещалась разными символами при каждом нажатии на кла-

вишу. Для двойной замены букв при каждом шифровании использовалась штекерная панель, что увеличивало сложность и добавляло еще 10^{14} возможных ключей [2].

При эксплуатации «Энигмы» немцы ежедневно меняли следующие установки:

- расположение штекеров,
- коммутационные диски и их компоновку,
- позиции колец,
- начальные угловые положения дисков.

Но шифрование слишком большого количества информации с одними и теми же установками оказалось неудачной практикой. Более правильным решением является смена ключа с передачей каждого нового сообщения. Именно этот недосмотр в режиме работы «Энигмы» позволил специалистам криптографического центра Блетчли-Парк, среди которых был известный математик Алан Тьюринг, раскрыть график передвижения германских войск. Причиной утечки являлась неверная эксплуатация машины, а не слабость криптостойкости алгоритма.

Другой недостаток «Энигмы» связан именно с нестойкостью системы шифрования. Штекерная панель и композиционные диски – ортогональные механизмы шифрования. Это дает возможность осуществить успешную атаку на отдельный достаточно большой шифротекст.

При наличии большого шифрованного сообщения игнорируется участие штекерной панели в алгоритме и идет поиск возможного положения всех коммутационных дисков и колец. Критерием корректности подбираемого расположения служит близость статистики частично расшифрованного текста к естественной. Как только достигнуто искомое значение, можно с достаточной долей вероятности утверждать, что найденные установки коммутационных дисков и колец действительно верные. После этого штекеры поочередно помещаются на панель до полной расшифровки текста.

Этот недостаток «Энигмы» был известен сотрудникам разведки, но данный подход к взлому не был использован в военных действиях, так как для его успешной реализации нужен был большой шифрованный текст, а большинство реальных перехваченных немецких сообщений были очень короткими.

Библиографический список

1. Смолевицкая М. Первые криптографические машины // Информатика, №5, 2007
2. Смарт Н. Криптография. – М.: Техносфера, 2005.
3. Шифровальная машина «Энигма» в Excel. – http://habrahabr.ru/post/142118