4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Кн. 1. – М.: Энергоатомиздат, 1994. – 424 с.

5. Мельников Д.А. Информационные процессы в компьютерных сетях. – М.: Кудиц-Образ,1999. – 256 с.

6. Колесников А.В., Позднякова В.К. Исследование и оптимизация производительности баз данных / Луганск, НИПКИ «Искра». – Луганск, 2008 – 11 с.: Библиогр.: 8 назв. – Укр. – Деп. в ДНТИ Украины, от 12.05.08 г. № 47-Ук-2008.

7. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей. – М.: Лори, 2002. – 350 с.

ГЕНЕТИЧЕСКИЙ КРИПТОАЛГОРИТМ

© Тулегенов А.А.[1]

Евразийский национальный университет им. Л.Н. Гумилева,
Республика Казахстан, г. Астана

Рассматривается возможность применения генетического алгоритма как мощного инструмента в задачах криптографии. Описана схема работы ассиметричного генетического криптоалгоритма. Модель гарантирует получение достаточно хорошего результата за приемлемое время.

Ключевые слова: криптография; генетические алгоритмы; скрещивание; мутация; ассиметричные алгоритмы.

Введение

Информация является одной из самых главных ценностей в современном мире. Появление глобальных компьютерных сетей упростило и ускорило получение доступа к информации как для отдельных людей, так и для больших корпораций. Но легкость и скорость доступа к данным с помощью компьютерных сетей, таких как Интернет, также сделали значительными следующие угрозы безопасности информации при отсутствии мер для её защиты:

- Неавторизованный доступ к информации.
- Неавторизованное изменение информации.
- Неавторизованный доступ к сетям и другим сервисам.
- Другие сетевые атаки, такие как повтор перехваченных ранее транзакций и атаки типа «отказ в обслуживании».

В настоящее время при разработке информационных технологий, обеспечивающих информационную безопасность и защиту информации, широ-

[1] Магистрант.

кое применение находят криптографические методы защиты, которые предполагают разработку новых способов шифрования, сложных для вскрытия, и способов дешифрования для вскрытия существующих шифров.

Криптография

Криптография – это наука о методах обеспечения безопасности информации, которая занимается поисками решений четырех важных проблем безопасности [1]:

1) конфиденциальность (невозможность прочтения информации посторонним);
2) целостность (невозможность незаметного изменения информации);
3) аутентификация (проверка подлинности авторства или иных свойств объекта);
4) невозможности отказа от авторства и контроль абонентов взаимодействия.

Шифрование – это преобразование данных в нечитабельную форму, используя ключи шифрования-расшифровки. Шифрование позволяет обеспечить конфиденциальность, сохраняя информацию в тайне от того, кому она не предназначена. Кроме того, шифрование должно также обеспечивать возможность легкого получения исходной информации из зашифрованной легитимными пользователями, которым доступен ключ алгоритма расшифрования.

В настоящее время криптография включает в себе симметричные криптосистемы, асимметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управляющие ключами, получение скрытой информации, автоматную криптографию, квантовую криптографию, генетическую криптографию и нейрокриптографию.

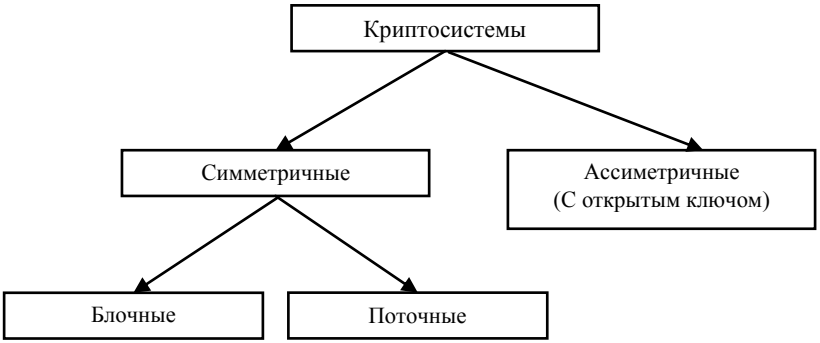

Рис. 1. Классификация криптосистемы

В симметричных криптосистемах зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Порядок использования симметричного шифра представлен на рис. 2.

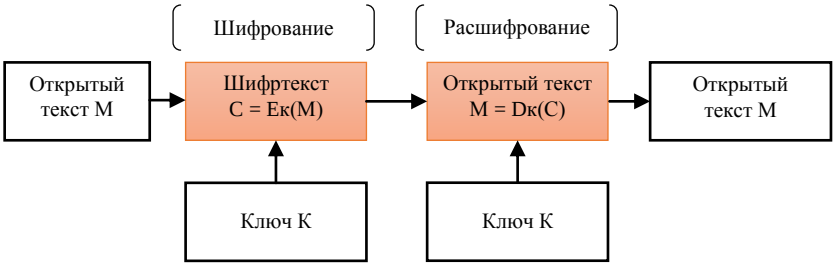

Рис. 2. Порядок использования симметричного шифра

При этом предполагается, что взаимодействующие абоненты осуществили обмен ключевой информацией по некоему надёжному каналу связи и обладают секретным ключом К.

Криптосистемы с открытым ключом, или асимметричные криптосистемы характерны тем, что в них используются различные ключи для зашифрования и расшифрования информации. Ключ для зашифрования можно сделать общедоступным, с тем чтобы любой желающий мог зашифровать сообщение для некоторого получателя. Получатель же, являясь единственным обладателем ключа для расшифрования, будет единственным, кто сможет расшифровать зашифрованные для него сообщения. Данный механизм проиллюстрирован на рис. 3.

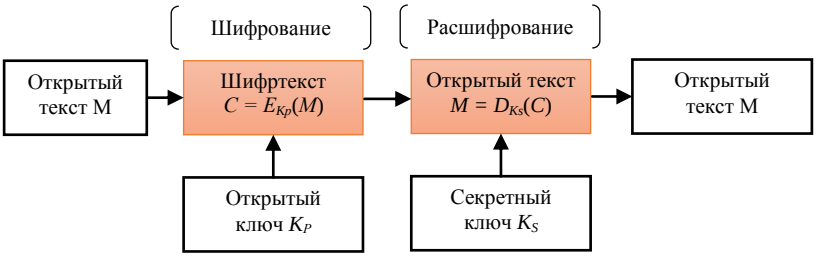

Рис. 3. Механизм зашифрования и расшифрования в ассиметричной криптосистеме

Безусловное преимущество данного подхода состоит в том, что отпадает необходимость организации защищённого канала для распределения ключей. К недостаткам можно отнести более низкую по сравнению с симметричными криптосистемами скорость шифрования, а также отсутствие строгого математического обоснования стойкости ряда используемых конструкций. Часто используются гибридные криптографические системы, когда обмен ключевой информацией производится с использованием асимметричной криптографии, а шифрование передаваемых данных – более быстрыми и не менее стойкими симметричными алгоритмами.

Генетические алгоритмы (ГА) [3] представляет собой стохастические и эвристические оптимизационные методы, предложенные Холландом, и основываются на идее эволюции с помощью естественного отбора, выдвинутой Дарвином. ГА работают с совокупностью «особей» – популяцией, каждая из которых представляет возможное решение данной проблемы. Каждая особь оценивается мерой ее «приспособленности» согласно тому, насколько «хорошо» соответствующее ей решение задачи. В природе это эквивалентно оценке того, насколько эффективен организм при конкуренции за ресурсы. Наиболее приспособленные особи получают возможность «воспроизводить» потомство с помощью «перекрестного скрещивания» с другими особями популяции. Это приводит к появлению новых особей, которые сочетают в себе некоторые характеристики, наследуемые ими от родителей. Наименее приспособленные особи с меньшей вероятностью смогут воспроизвести потомков, так что те свойства, которыми они обладали, будут постепенно исчезать из популяции в процессе эволюции. Иногда происходят мутации, или спонтанные изменения в генах.

Рассмотрим стандартные операторы, которые определены для всех типов генетических алгоритмов:

- **Селекция.** Оператор селекции осуществляет отбор хромосом в соответствии со значениями их функции приспособленности. Существуют как минимум два популярных типа оператора селекции: рулетка и турнир.
- **Скрещивание.** Оператор скрещивание осуществляет обмен частями хромосом между хромосомами в популяции. Может быть одноточечным или многоточечным. Одноточечный кроссовер работает следующим образом. Сначала, случайным образом выбирается одна из l-1 точек разрыва. Точка разрыва – участок между соседними битами в строке. Обе родительские структуры разрываются на два сегмента по этой точке. Затем, соответствующие сегменты различных родителей склеиваются и получаются два генотипа потомков.
- **Мутация.** Оператор мутации случайно (стохастический) изменяет части хромосом. Строке, которая подвергается мутации, каждый бит с вероятностью *P* (обычно очень маленькой) меняется на другой.

Ассиметричные криптоалгоритмы с применением генетических алгоритмов

Псевдокод генетического ассиметричного криптоалгортима состоит из шагов [4]:

Шаг 1. Генерация 4 точек для скрещивания и 3 для операции мутации в диапазоне от 0-15.

Шаг 2. Сортировка этих числа в порядке увеличения.

Шаг 3. Генерация случайного коэффициента перестановки в диапазоне 1-7.

Шаг 4. Генерация случайного закрытого ключа в диапазоне 0-15 числа.

Шаг 5. Генерация открытого ключа K_O, состоящего из точек скрещивания, мутации, коэффициента перестановки и закрытого случайного числа.

Шаг 6. Генерация закрытого ключа $K_З$, используя формулу $K_З = K_O \; \theta \; R$ Здесь R – 36 битное бинарное число, полученное путем повторения закрытого случайного числа 9 раз, а θ – операция «логического или»(xor) Так как. операции симметричны можно будет получить открытый ключ из закрытого: $K_O = K_З \; \theta \; R$.

Следовательно, если текст будет зашифрован открытым ключом значит он сможет быть расшифрован закрытым ключом с связи с зеркальностью задействованных операций.

Шаг 7. Запись пары ключей в файл.

Шаг 8. Чтение 2 блоков по 16 байт каждый из файла для шифрации.

Шаг 9. Если количество байтов достаточно переходим к шагу 11.

Шаг 10. Если байтов недостаточно добавляем пробелы, чтобы получить 16 байтные блоки.

Шаг 11. Производим перевод полученных байтовых блоков информации.

Шаг 12. Операции скрещивания и мутации над полученными блоками на 11 шаге.

Шаг 13. Запись зашифрованных блоков в файл.

Шаг 14. Если имеется дополнительная информации к шифрации, то повторить действие с 8 шага.

Шаг 15. Конец.

Пример работы алгоритма

Шаг 1. Извлекаем два 16-байтных блока из текстового файла. Пусть они будут представлены в виде массивов **b[0-15]** и **c[0-15]**, где каждый **b[i]** и **c[i]** это символ в файле.

Шаг 2. Производим перевод на выбранных блоках и представим их в виде **B[i]'** и **C[i]'.** Сгенерируем 4 случайных числа в пределах от 0-15, а также отсортируем их в порядке увеличения. Пусть эти числа будут 2, 7, 10 и 14. Эти числа будут точками скрещивания.

Шаг 3. Производим операцию скрещивания между этими точками:

$$C_1 = 2, C_2 = 7, C_3 = 10, C_4 = 14.$$

Шаг 4. Производим операцию мутации. Сгенерируем 3 случайных числа в пределах от 0-15. Эти 3 числа будут точками мутации. Для примера возьмем числа

$$M_1 = 1, M_2 = 7, M_3 = 12.$$

Шаг 5. Сгенерируем случайной фактор перестановки в промежутке 1-7. Пусть это число будет 4.

Шаг 6. Сгенерируем случайный «фактор случайности» в пределах 0-15. Пусть это будет число 9.

Шаг 7. На основе точек скрещивания, мутации, фактора перестановки и фактора случайности создаем ключ. В шестнадцатеричной системе счисления он будет представлен в виде **27AE17C49**. На этом действие с этими блоками закончено.

Шаг 8. Если имеются еще данные для шифрации, то числа в ключе шифрации сдвигаются влево на число фактора перестановки. В качестве примера возьмем наш ключ **27AE17C49** и фактор перестановки равен 4. Новый ключ будет **17C27AE49**(фактор перестановки и фактор случайности остаются нетронутыми) и проделывается операции на следующей парой блоков уже с новыми точками скрещивания и мутации. $C_1 = 1, C_2 = 7, C_3 = 12, C_4 = 2, M_1 = 7, M_2 = 10, M_3 = 14$ после сортировки $C_1 = 1, C_2 = 2, C_3 = 7, C_4 = 12, M_1 = 7, M_2 = 10, M_3 = 14$. Ключ при этом остается всегда неизменным (данные в нем не сортируется по увеличению).

Перспектива исследования

Генетические алгоритмы удачно использовались во многих научных статьях [5]. В одной из работ было проанализировано около 400 ключей и не было ни единого повторения ключей, следовательно, тест на частоту был пройден удачно. Коэффициент автокорреляции был рассчитан для от k = 1 до k = 10 и результат для k = 1 был равен 0.03, что говорит о хорошем «случайном показателе». Применение генетических алгоритмов в криптологии позволит получать улучшенные результаты. Исходя из аналитических результатов ключи, полученные с помощью генетических алгоритмов, были действительно случайными и неповторяющимися, что в разы увеличивает силу ключей и, следовательно, безопасность от попыток взлома.

Заключение

В данной статье предложен алгоритм генерации ассиметричных ключей, основанных на генетических операциях скрещивания и мутации для шифрации и дешифрации сообщений. Для демонстрации работы алгоритма использованы 4 точки скрещивания и 3 точки мутации, 1 байт перестановки, 1 байт случайного числа и длина ключа составила 36 бита. Алгоритм может быть усложнен для взлома, если стороны заранее утвердят секретный фактор перестановки. Это в купе с случайностью делает алгоритм сложным для взлома.

Список литературы:

1. Чандлер Дж. Cryptography 101.

2. Марков Алексей Сергеевич, Цирлов Валентин Леонидович Основы криптографии: подготовка к cissp // Вопросы кибербезопасности. – 2015. – № 1.

3. http://www.codenet.ru/progr/alg/ga/.

4. Dr. Poornima G. Naik, Asymmetric Key Encryption using Genetic Algorithm, International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 3 Issue 3 January 2014.

5. Sonia Goyat Cryptography Using Genetic Algorithms (GAs). IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 1, Issue 5 (May-June 2012)

6. Harsh Bhasin, Nakul Arora, Reliability Infocom Technology and Optimization 2010, Conference Proceedings pages 226-230.