УДК 004.056.5

-

*Кулиш М.Н., Чернышова А.В.*
*Донецкий национальный технический университет, Украина*
*feniks_fire@yahoo.com, alla@pmi.dgtu.donetsk.ua*

*Рассмотрены проблемы безопасности, связанные с подбором паролей. Описаны существующие методы генерации и хранения паролей. Выполнен анализ алгоритмов для построения хеш-значений. Рассмотрены алгоритмы генерации псевдослучайных чисел. Предложены алгоритм генерации произвольного пароля.*

Проблемы безопасности, связанные с подбором паролей к учетным записям пользователей, существовали всегда. Повсеместное распространение интернета и развитие вычислительных средств с каждым годом повышает требования к сложности паролей. Увеличение сложности требует от пользователя не только заучивать более длинный и плохо запоминаемый пароль, но и тратить время на генерацию. Таким образом, становится актуальной разработка программ для генерации паролей произвольной длины на основе случайных либо специальных значений.

На данный момент существует огромное количество программ для генерации паролей. Их основные функции:

– Генерация произвольного пароля;
– Генерация пароля на основе определенных данных — так называемый хранитель пароля.

6

Криптографические приложения используют для генерации случайных чисел особенные алгоритмы. Эти алгоритмы заранее определены и, следовательно, генерируют последовательность чисел, которая теоретически не может быть статистически случайной. Такие числа называют псевдослучайными числами [1]. Таким образом, генерация произвольного пароля производится при помощи генератора псевдослучайных чисел.

Наиболее распространённым генератором псевдослучайных чисел является ГПСЧ LFSR (рис. 1).

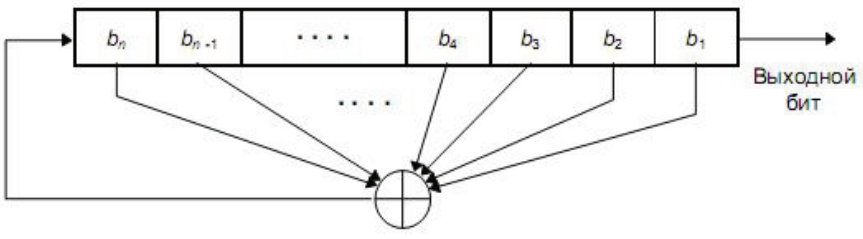


Рисунок 1. Сдвиговый регистр LFSR

LFSR – это линейный сдвиговый регистр с обратной связью. Сдвиговый регистр с обратной связью состоит из двух частей: сдвигового регистра и функции обратной связи. Всякий раз, когда нужно извлечь бит, все биты сдвигового регистра сдвигаются вправо на 1 позицию. Новый крайний левый бит является функцией всех остальных битов регистра. На выходе сдвигового регистра оказывается один, обычно младший значащий бит. Периодом сдвигового регистра называется длина получаемой последовательности до ее повторения. В LFSR обратная связь представляет собой XOR определённых битов сдвигового регистра. Перечень этих битов называется отводной последовательностью [2].

Основные недостатки LFSR [2]:

- Для обеспечения генерации псевдослучайной последовательности максимальной длины необходимо чтобы многочлен, образованный из отводной последовательности, был примитивным по модулю 2, что является сложной вычислительной задачей. Данная проблема решается либо перебором, либо использованием готовых таблиц.
- Многочлены, которые берутся из таблиц, являются сильно разреженными (т.е. имеют мало коэффициентов), что представляет источник слабости, достаточный для взлома.

Хранители пароля подразумевают в своей работе генерацию одного и того же пароля на основе одинаковых данных. Таким образом, удобно использовать для работы таких программ однонаправленные хеш-функции.

Однонаправленная функция H(M) применяется к сообщению произвольной длины M и возвращает значение фиксированной длины h, то есть h = H(M), где h имеет длину m. Многие функции позволяют вычислять значение фиксированной длины по входным данным произвольной длины, но у рассматриваемых хэш-функций есть дополнительные свойства, делающие их однонаправленными:

Зная M, легко вычислить h.

Зная H, трудно определить M, для которого H(M)=h.

Зная M, трудно определить другое сообщение M’ , для которого H(M) = H(M') [2].

Среди наиболее используемых алгоритмов можно выделить алгоритмы MD4,MD5. Алгоритм MD5 является улучшением алгоритма MD4.

Рассмотрим алгоритм MD5. После некоторой первоначальной обработки MD5 обрабатывает входной текст 512-битовыми блоками, разбитыми на 16 32-битовых подблоков. Выходом алгоритма является набор из четырех 32-битовых блоков, которые объединяются в единое 128-битовое хэш-значение. Переменные A, B, C, D инициализируются определенными значениями в соответствии с алгоритмом. Цикл работы алгоритма продолжается, пока не исчерпаются 512-битовые блоки сообщения [2].

Четыре переменных копируются в другие переменные: A в a, B в b, C в c и D в d.

Главный цикл состоит из четырех очень похожих этапов. На каждом этапе 16 раз используются различные операции. Каждая операция представляет собой нелинейную функцию над тремя переменными из набора a, b, c и d. Затем она добавляет этот результат к четвертой переменной, подблоку текста и константе. Далее результат циклически сдвигается вправо на переменное число битов и добавляет результат к одной из переменных a, b, c и d. Наконец результат заменяет одну из переменных a, b, c и d (рис. 2) [2].

Основным недостатком для генерации паролей при использовании алгоритма MD5 является то, что генерируемый пароль будет всегда одной и той же длины. Таким образом, в связке с MD5 необходимо использовать вспомогательные алгоритмы. В [5] предложена программа защищенного хранения паролей пользователей.

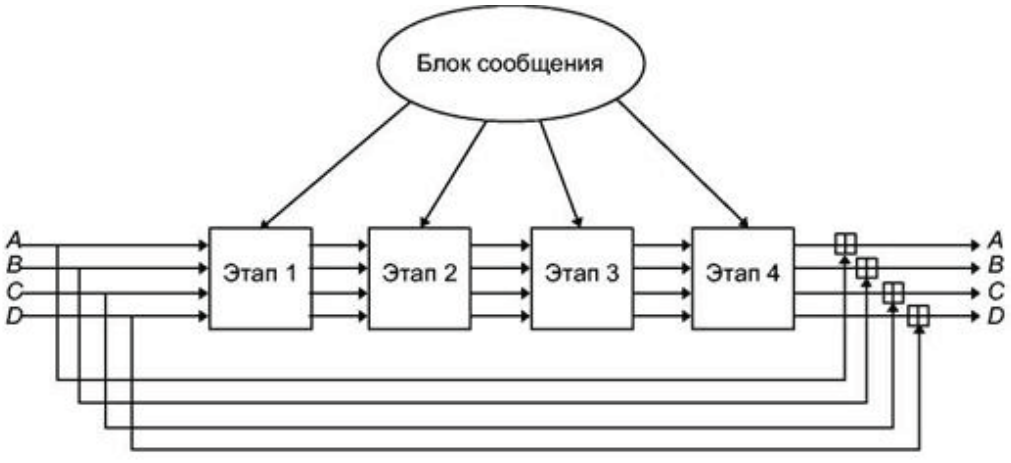


Рисунок 2. Главный цикл MD5

В данной работе предлагается схема генерации пароля произвольной длины на основе значений, полученных из генератора псевдослучайных числе LFSR или хеш-функций MD4/MD5 (рис. 3).

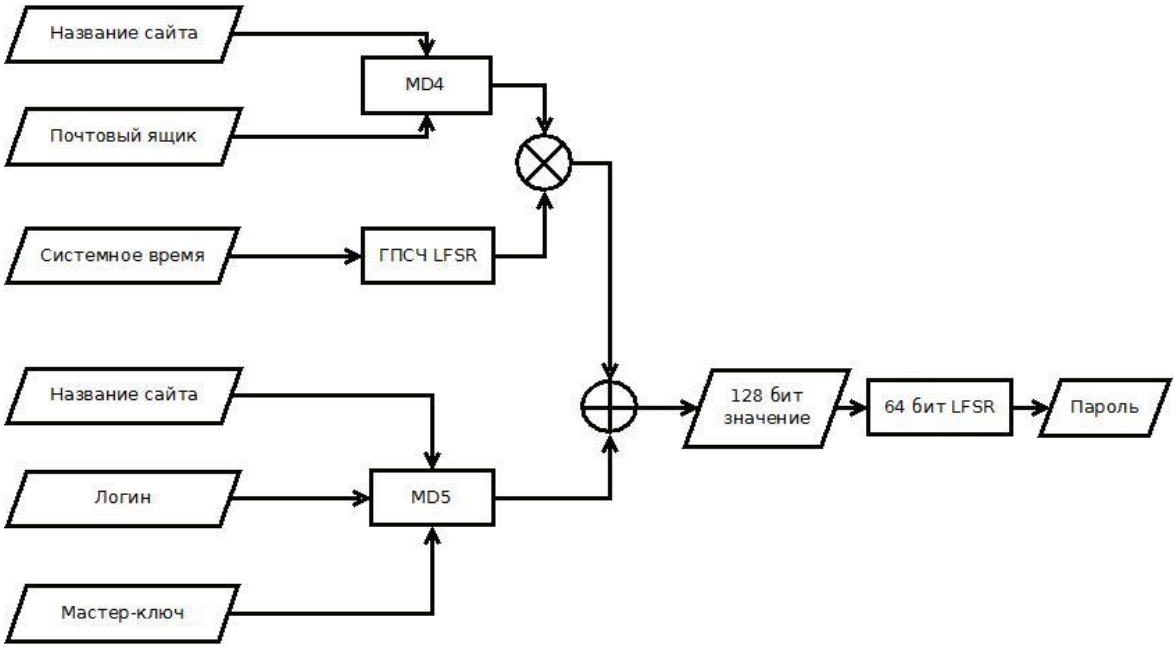


Рисунок 3. Схема генерации произвольного пароля

Первым слоем генерации в зависимости от опций является ГПСЧ LFSR (в случае с выбором дополнительных опций совмещается с хеш-функцией MD4) или хеш-функций MD5.

Входным значением для инициализации сдвигового регистра является текущее системное время. ГПСЧ LFSR работает до тех пор, пока не будет сформировано 128 битное значение.

В случае, если для генерации случайного пароля выбраны дополнительные опции (название сайта и/или почтовый ящик), то значение, полученное на выходе ГПСЧ LFSR побитово складывается с хешем на выходе MD4. Этот хеш строится на основе дополнительных данных.

Входными данными для алгоритма MD5 являются название сайта, логин и мастер-ключ (фраза либо файл). Выходом алгоритма MD5 является 128 битное значение.

Полученное на первом слое значение передается во второй слой, которым является 64 битный сдвиговый регистр LFSR. Первые 32 бита регистра заполняются нечетными битами из первых 64 бит значения, последние 32 – четными битами. Проинициализированный LFSR используется для генерации пароля произвольной длины.

Многие интернет-ресурсы имеют ограничения на виды символов, допускаемые в паролях. После генерации ГПСЧ LFSR на втором слое очередных 8 бит, они переводятся в символ и сравниваются с ограничениями. Если символ не удовлетворяет ограничениям, то производится повторная генерация.

Проблемой, которая возникает при генерации паролей, также является теоретическая вероятность создания очень простого пароля, который может быть подобран по словарю. Проверка при генерации пароля с помощью словаря является надежным методом, но значительно снижает скорость генерации. Предлагается упрощенный метод проверки, в соответствии с которым первые и последние два символа не могут быть буквами одновременно. Кроме того, длина самого пароля не должна быть меньше 8 символов. Генерация пароля продолжается, пока не будут выполнены все условия.

Сгенерированный пароль дополнительно может быть проанализирован на стойкость тремя

алгоритмами:

- Проверка пароля на множество качеств, обладая которыми пароль увеличивает или уменьшает свою стойкость к подбору [6].
- Алгоритм NIST (оценка энтропии) [7].
- Проверка пароля по мини-словарю [8].

В данной статье были рассмотрены алгоритмы генерации псевдослучайных чисел и хеш-значений. Предложена схема генерации пароля произвольной длины на основе рассмотренных алгоритмов. Описаны способы проверки стойкости пароля.

Предложенная схема генерации позволяет:

- Объединять достоинства хеш-функций и генераторов случайных чисел;
- Увеличить энтропию при генерации пароля;
- Повысить сложность подбора генерируемого пароля.

Схема может быть улучшена за счет:

- Увеличения числа слоев при генерации
- Вариации простых многочленов для генератора LFSR
- Разработки модуля генерации не разреженных многочленов.

[1] Генератор псевдослучайных чисел. Материал из Википедии - свободной энциклопедии. Электронный ресурс. Режим доступа: http://ru.wikipedia.org/wiki/ГПСЧ.

[2] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си- М.: Триумф, 2002. - 816 с.

[3] MD4. Материал из Википедии - свободной энциклопедии. Электронный ресурс. Режим доступа: http://ru.wikipedia.org/wiki/MD4.

[4] MD5. Материал из Википедии - свободной энциклопедии. Электронный ресурс. Режим доступа: http://ru.wikipedia.org/wiki/MD5.

[5] Пехотин Е.В. Хранитель паролей - программа защищенного хранения паролей пользователей//Информатика и компьютерные технологии (ИКТ-2009)/ Материалы V международной научно-технической конференции студентов, аспирантов и молодых ученых - 24-26 ноября 2009 г., Донецк, ДонНТУ. - 2009. - с. 377-383.

[6] Статья «Еще об оценке стойкости пароля» Электронный ресурс. Режим доступа: http://korzh.net/2011-04-eshhyo-ob-ocenke-stojkosti-parolya.html.

[7] Журнал «NIST's Special Publication 800-63 Information Security». Электронный ресурс. Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

[8] Статья «Алгоритм оценки стойкости пароля от Microsoft. Часть 2». Электронный ресурс. Режим доступа: http://habrahabr.ru/blogs/infosecurity/116425.