Балашов М.А.

СИСТЕМА РАЗДЕЛЕНИЯ СЕКРЕТА С АВТОМАТИЗИРОВАННЫМ ДИЛЕРОМ.   
Россия, Екатеринбург, УрГУПС  
bdinl2@mail.ru

**Введение**

В настоящее время существует множество систем и методов защиты информации. Я бы хотел поговорить о системе разделения секрета. Эта система используется сразу несколькими пользователями так, что какой-то один не может войти в систему. В системе есть параметры, они задаются еще одним человеком - дилером, который может не являться доверенным лицом. Минусом этой системы является то, что дилер должен быть доверенным лицом, ведь он может воспользоваться знанием формулы и создать пароли. Для его устранения можно автоматизировать процесс присвоения параметров.

Цель работы: усовершенствование системы разделения секрета, а именно ведение автоматизированного дилера

**Разделение секрета**

Задача разделения секрета заключается в представлении некоторой секретной информации в виде набора равнозначных фрагментов, распределяемых среди нескольких участников. При этом полный набор фрагментов должен однозначно определять исходную информацию, однако любое неполное их подмножество не должно предоставлять возможности восстановить секрет.

Главная проблема — безопасное управление распределением секретных ключей. Даже при использовании центра доверия необходим какой-нибудь способ получения ключа каждому его пользователю.

Один из возможных путей решения состоит в расщеплении ключа (более формально — разделении секрета), при котором ключ делится на несколько частей



Каждая его часть передается по своему каналу. Красота этого решения бросается в глаза: для определения ключа нападающий должен суметь подключиться ко всем каналам сразу. С другой стороны, если противнику удалось проникнуть в один из каналов, передающих части ключа, он может воспрепятствовать законному восстановлению ключа.

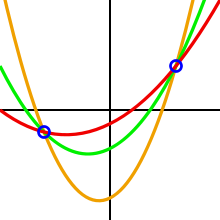
**Схема разделения секрета Шамира**

Схема интерполяционных полиномов Лагранжа, схема разделения секрета Шамира или просто схема Шамира — это схема разделения секрета, широко используемая на практике. Схема Шамира позволяет создать *(t, n)*-пороговое разделение секрета для любых *t*, *n*.

Однако данная схема не защищает от мошенничества со стороны владельцев секретов, а также не защищает от мошенников, выдающих себя за тех, кто владеет секретом.

Суть схемы разделения Шамира:

Через две точки можно провести неограниченное число полиномов степени 2. Чтобы выбрать из них единственный — нужна третья точка. Данные графики приведены только для иллюстрации идеи — в схеме Шамира используется конечное поле, полиномы над которым сложно представить на графике



Идея схемы заключается в том, что двух точек достаточно для задания прямой, трех точек — для задания параболы, четырех точек — для кубической параболы, и так далее. Чтобы задать многочлен степени  требуется  точек.



Если мы хотим разделить секрет таким образом, чтобы восстановить его могли только  человек, дилер «прячет» его в формулу -мерного многочлена. Восстановить этот многочлен можно по  точкам. Количество же различных точек многочлена не ограничено (на практике оно ограничивается размером числового поля, в котором ведутся расчёты).



**Замена дилера-человека автоматизированным дилером**

Допустим, есть группа из трех человек, которые являются равноправными хозяевами какой-либо компании с большим капиталом. Чтобы пользоваться этим капиталом все трое должны участвовать в открытии сейфа, т.к. они не доверяют друг другу, и соответственно дилеру тоже. Что же делать в этом случае?

Необходимо создать систему разделения секрета с автоматизированным дилером с достаточно дружелюбным интерфейсом, чтобы обычный пользователь смог ей воспользоваться. От пользователя (в данном случае от хозяев компании) на первом этапе работы данной системы требуется лишь ввести с произвольно следующие параметры системы:

p1 - любое целое число от 5 до 10000

p2 - любое целое число от 5 до 10000

p3 - любое целое число от 35 до 120

Надо дать возможность пользователям самим написать формулу для Rcv при условии, чтобы формула была достаточно сложной, и результат был не маленьким числом. Для написания формулы можно пользоваться действиями сложения, вычитания, умножения, деления нацело, возведения в степень и использовать параметры p1, p2 и значения текущих года, месяца, числа, часа.

Допустим, у пользователей получилась следующая формула:



Что такое Rcv и где используется параметр p1 поясню позже.

От пользователей также требуется зарегистрироваться в системе, но так чтобы каждый знал лишь свой логин и не распространял его. Тем самым создается база логинов.

Так как пользователей трое, то в системе будет использоваться парабола. Я решил использовать для генерации коэффициентов в уравнении параболы настоящую дату, то есть год, месяц, число и час. На практике можно использовать более мелкие единицы измерения времени.

Алгоритм работы схемы разделения секрета с автоматизированным дилером

**Алгоритм работы программы генератора пароля**

1. Система составляет уравнение параболы, генерируя коэффициенты a,b,c, используя дату.

2. Система имеет базу логинов, которые состоят из маленьких латинских букв. Если мы вводим верный логин, то система переходит к следующему действию, иначе выдает пароль похожий на верный, но не несущий в себе информации.

3. Посимвольно переводим логин в двоичный код. Предварительно был создан пятиразрядный двоичный алфавит для латинских букв. приложение4.

4. Полученный двоичный код переводим в десятичное число. Это число и будет являться абсциссой на графике с параболой.

5. Подставляем значение абсциссы в уравнение параболы и получаем соответствующее значение ординаты.

6. Это число переводим в двоичный вид.

7. Создаем псевдослучайное число Rcv от даты (год, месяц, число, час) и параметров p1 и p2.

8. Записываем это число в двоичном виде.

0110100011100101 - пример.

9. Сравниваем длину двоичной записи этого числа с длиной двоичной записи ординаты. Если количество символов в записи числа больше, чем в записи ординаты, то убираем справа по одному символу до тех пор, пока количество символов в записи числа не будет равным количеству символов в записи ординаты. Иначе если количество символов в записи числа меньше, чем в записи ординаты, то начинаем приписывать к имеющемуся числу справа снова это же число посимвольно, до тех пор, пока длины записи числа и ординаты не будут равны.

10. Далее создаем массив из n столбцов и трех строк, где n - количество символов в двоичной записи ординаты. В первой строке посимвольно записываем ординату, а во второй число. см приложение1

11. Проходим по столбцам массива, и для тех столбцов, в которых в первой строке записан 0, а во второй 1 используем логическую операцию ИЛИ (иначе далее нельзя будет расшифровать). Итог этого действия записываем в третью строку. В остальных столбцах в третью строку записываем значение из первой строки. Тем самым мы зашифровали значение ординаты.

12. Теперь третью строку записываем как число в двоичном виде. Далее это число буду называть "число2".

13. Следующим действием число2 делим по 5 символов и заменяем эти части буквами латинского алфавита и еще шестью символами из ранее созданного алфавита, состоящего из 32-ух символов (32=2^5). см приложение2

14. Двоичная запись числа 2 содержит большое количество 1, т.е. 1 более вероятна в этой записи, чем 0. И в символьной записи этого числа будут визуально видны более вероятные символы. Исправляем это следующим образом:

1) В символьной записи числа2 заменяем каждый символ номером этого символа в алфавите и записываем эти номера в массив из m столбцов и 7-и строк, где m - количество записи в символьной записи числа2. см приложение3

2) В первой строке записываем номер символа в алфавите.

3) Во второй позиция символа в символьной записи числа2.

4) В третьей остаток от деления на 32 выражения (19\*2+53-16), где 19 - текущий час, 2 - позиция символа в символьной записи числа2, 53 - параметр p3, 16 - номер символа в алфавите.

5) В четвертой число, полученное при целочисленном делении выражения (19\*2+53-16) на 32, оно необходимо далее для расшифрования. Максимальное значение этого числа 25.

6) В пятой пятиразрядную двоичную запись числа из четвертой строки. Пятиразрядную потому что 2^32>25.

7) В шестой символьную запись числа из пятой строки.

8) В седьмой символьную запись числа из третьей строки.

15. Создаем пароль следующим образом: Записываем из первого столбца и шестой строки символ, следующий символ из первого столбца и седьмой строки. Далее символ из второго столбца и шестой строки и т.д. до m-ного столбца. В данном случае получается пароль: axbkbrcadf.

16. Можно в этот пароль случайным образом добавить цифры, например ax1b93k5brca7df, чтобы пароль казался случайно сгенерированным, и чтобы заметить закономерность было сложнее. На выходе пользователь получает этот пароль.

17. Повторяем эти операции 3 раза с использованием разных верных логинов.

**Алгоритм работы "секрета"**

1. Один пользователь вводит логин и пароль, полученный на выходе первой программы.

2. Делаем все то же самое, что и в первой программе до 15-ого пункта включительно.

3. Отбрасываем цифры из полученного пароля и сравниваем его с паролем, полученным в этой программе.

4. То же самое делают второй и третий пользователи.

5. Если все операции со всеми логинами и паролями прошли успешно, то секрет раскрыт.

Условия, что система будет работать, заключается в том, что часы у пользователей и у секрета должны быть синхронизированы и что все действия должны выполняться в течение одного часа, иначе коэффициенты будут генерироваться не одинаковые. Это связано с тем, что в генерации используются текущие год, месяц, число, час.

На практике нужно использовать более мелкие единицы измерения времени, так как при этом чаще будут генерироваться новые коэффициенты, и взломать систему будет сложнее.

Достоинство системы: в ней нет дилера-человека. Даже те самые хозяева компании не считаются дилерами, т.к. вводили параметры, не зная при этом что вводят. Информация в паролях достаточно хорошо защищена и является одноразовой, т.к. каждый раз будут генерироваться новые пароли.

Список литературы:

1) С++ для людей. 11.01.2009. URL: <http://cppstudy.wordpress.com/2009/01/11/pseudo-random-numbers-in-cpp/> (Дата обращения: 02.11.2012)

2) It shop. /несколько слов о шифровании и алгоритмах. 20.05.2008. URL: <http://www.itshop.ru/efg735r-neskolko-slov-o-shifrovanii-i-algoritmah/l9i23195> (Дата обращения: 02.11.2012)

3) Citforum / Еще раз о разделении секрета. 12.07.2009. <http://citforum.ru/security/cryptography/yaschenko/23.html> (Дата обращения: 02.11.2012)

4)Masteroid / Разделение секрета 12.09.2010. <http://masteroid.ru/content/view/1269/49/> (Дата обращения: 02.11.2012)

5) Википедия, свободная энциклопедия / Схема разделения секрета Шамира. 02.07.2012. URL: <https://ru.wikipedia.org/wiki/Схема_разделения_секрета_Шамира> (Дата обращения: 02.11.2012)

Приложения

1)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |

2)011110111111011111111101

pp@^n

3) Таблица для создания пароля

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| символ из алфавита | 16 | 16 | 28 | 32 | 14 |
| номер в симв. записи | 1 | 2 | 3 | 4 | 5 |
| полученное число | 24 | 11 | 18 | 1 | 6 |
| частное | 1 | 2 | 2 | 3 | 4 |
| двоич. Запись частного | 1 | 10 | 10 | 11 | 100 |
| симв. Запись частного | a | b | b | c | d |
| симв. Запись полученного числа | x | k | r | a | f |

4) Алфавит

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | a | 1 | 17 | q | 10001 |
| 2 | b | 10 | 18 | r | 10010 |
| 3 | c | 11 | 19 | s | 10011 |
| 4 | d | 100 | 20 | t | 10100 |
| 5 | e | 101 | 21 | u | 10101 |
| 6 | f | 110 | 22 | v | 10110 |
| 7 | g | 111 | 23 | w | 10111 |
| 8 | h | 1000 | 24 | x | 11000 |
| 9 | i | 1001 | 25 | y | 11001 |
| 10 | j | 1010 | 26 | z | 11010 |
| 11 | k | 1011 | 27 | ! | 11011 |
| 12 | l | 1100 | 28 | @ | 11100 |
| 13 | m | 1101 | 29 | # | 11101 |
| 14 | n | 1110 | 30 | $ | 11110 |
| 15 | o | 1111 | 31 | % | 11111 |
| 16 | p | 10000 | 32 | ^ | 0 |