Министерство образования Республики Беларусь

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

Лабораторная работа

«Вероятностная оценка безопасности пароля»

Выполнила: Михнюк А.В.

Проверил: Шиман Д.В.

Минск 2017

# Общие теоретические сведения

Пароль - идентификатор субъекта доступа, который является его (субъекта) секретом. Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Можно встретить и такие толкования терминов идентификатор и пароль пользователя. Идентификатор - некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.  
Пароль - некоторое секретное количество информации, известное только пользователю и парольной системе, предъявляемое для прохождения процедуры аутентификации.  
Учетная запись - совокупность идентификатора и пароля пользователя.  
Одним из наиболее важных компонентов парольной системы является база данных учетных записей (база данных системы защиты). Возможны следующие варианты хранения паролей в системе:

* в открытом виде;
* в виде хэш-значений (hash (англ.) - смесь, мешанина);
* зашифрованными на некотором ключе.

Наибольший интерес представляют второй и третий способы, которые имеют ряд особенностей. Хэширование не обеспечивает защиту от подбора паролей по словарю в случае получения базы данных злоумышленником. При выборе алгоритма хэширования, который будет использован для вычисления хэш-значений паролей, необходимо гарантировать несовпадение хэш-значений, полученных на основе различных паролей пользователей. Кроме того, следует предусмотреть механизм, обеспечивающий уникальность хэш-значений в том случае, если два пользователя выбирают одинаковые пароли. Для этого при вычислении каждого хэш-значения обычно используют некоторое количество "случайной" информации, например, выдаваемой генератором псевдослучайных чисел. При шифровании паролей особое значение имеет способ генерации и хранения ключа шифрования базы данных учетных записей. Возможны следующие варианты:

* ключ генерируется программно и хранится в системе, обеспечивая возможность ее автоматической перезагрузки; ключ генерируется программно и хранится на внешнем носителе, с которого считывается при каждом запуске;
* ключ генерируется на основе выбранного администратором пароля, который вводится в систему при каждом запуске.

Наиболее безопасное хранение паролей обеспечивается при их хэшировании и последующем шифровании полученных хэш-значений, т.е. при комбинации второго и третьего способов хранения паролей в системе. Как пароль может попасть в руки злоумышленника? Наиболее реальными выглядят следующие случаи:

* записанный вами пароль найден злоумышленником;
* пароль был подсмотрен злоумышленником при вводе легальным пользователем;
* злоумышленник получил доступ к базе данных системы защиты.

Формула Андерсона:

*N* – мощность алфавита;

*S* – длина пароля;

*Ssi*– длина служебной информации;

*E = S+Ssi* – общая

*P* – вероятность того, что пароль будет взломан за М месяцев;

*R* – скорость передать;

*M* – количество месяцев для взлома.

# Разработка программного средства

Для реализации арифметического метода сжатия было разработано программное средство на языке программирования C#.

Необходимо задать значения мощности алфавита, длины пароля, длины проверочных символов, скорости передачи, количества месяцев для взлома пароля, вероятность взлома и нажать кнопку «Рассчитать».

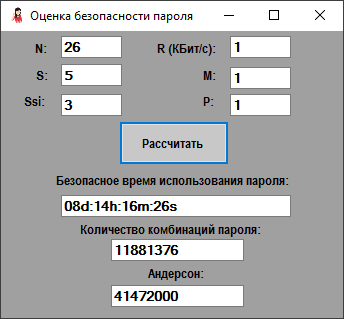


Рисунок 1 – Вид программы

После выполнения расчётов будут заполнены поля «Безопасное время использования пароля», «Количество комбинаций пароля, «Андерсон». А также появится окно, которое сообщит будет взломан пароль или нет.

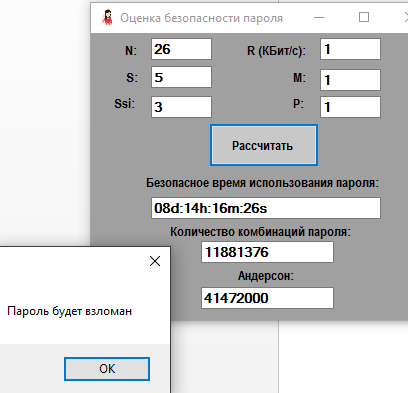


Рисунок 2 – Результат выполнения

# Заключение

В ходе выполнения лабораторной работы было разработано программное средство, реализующее расчет формулы Андерсона, а также формулы, для расчета безопасного времени использования пароля.

ы