**Лабораторная работа №1. Реализация генератора паролей с заданным параметром**

**Цель работы**: реализовать простейший генератор паролей, обладающий требуемой стойкостью ко взлому.

**Порядок выполнения работы:**

1. Изучить теоретический материал
2. Выбрать язык программирования
3. Выполнить практическую часть.
4. Оформить отчет. Отчет должен содержать:
   * наименование и цель работы;
   * ответы на контрольные вопросы;
   * код на выбранном языке программирования соответствующих заданий и скриншоты выполнения написанных программ;
   * выводы к выполненной лабораторной работе.

Отчет переименовать следующим образом: **ЗКИ\_ЛР1\_Фамилия\_№группы** и сдать на проверку преподавателю.

**Теоретическая часть**

Подсистемы идентификации и аутентификации пользователя играют очень важную роль в системах защиты информации.

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Парольные системы идентификации/аутентификации является одними из основных и наиболее распространенных в СЗИ методами пользовательской аутентификации. В данном случае, информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя является, как правило, передним краем обороны СЗИ. В связи с этим, модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель злоумышленника в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя являются наиболее простыми методами аутентификации и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

К паролю:

1. Минимальная длина пароля должна быть не менее 6 символов.
2. Пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.).
3. В качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

К подсистеме парольной аутентификации:

1. Администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, он должен быть сменен.

1. В подсистеме парольной аутентификации должно быть установлено ограничение числа попыток ввода пароля (как правило, не более 3).
2. В подсистеме парольной аутентификации должна быть установлена временная задержка при вводе неправильного пароля.

Как правило, для генерирования паролей в СЗИ, удовлетворяющих перечисленным требованиям к паролям, используются программы - автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации, единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае, оценка стойкости парольной защиты осуществляется следующим образом.

**Количественная оценка стойкости парольной защиты**

Пусть *A* – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля. Например, если пароль состоит только из малых английских букв, то A=26).

*L* – длина пароля.

 - число всевозможных паролей длины L, которые можно составить из символов алфавита A.

*V* – скорость перебора паролей злоумышленником.

*T* – максимальный срок действия пароля.

Тогда, вероятность *P* подбора пароля злоумышленником в течении срока его действия *V* определяется по следующей формуле.



Эту формулу можно использовать в обратную сторону для решения следующей задачи:

ЗАДАЧА. Определить минимальные мощность алфавита паролей *A* и длину паролей *L*, обеспечивающих вероятность подбора пароля злоумышленником не более заданной *P*, при скорости подбора паролей *V*, максимальном сроке действия пароля *T*.

Данная задача имеет неоднозначное решение. При исходных данных *V,T,P* однозначно можно определить лишь нижнюю границу *S\** числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по формуле

 (1)

где  - целая часть числа, взятая с округлением вверх.

После нахождения нижней границы *S\** необходимо выбрать такие *A* и *L* для формирования *S=AL*, чтобы выполнялось неравенство (2).

 (2)

При выборе *S*, удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленника (при заданных *V* и *T*) будет меньше, чем заданная *P.*

Необходимо отметить, что при осуществлении вычислений по формулам (1) и (2), величины должны быть приведены к одним размерностям.

Пример

Исходные данные – *P*=10-6, *T*=7 дней = 1 неделя, *V*=10 паролей / минуту = 10\*60\*24\*7=100800 паролей в неделю.

Тогда, .

Условию  удовлетворяют, например, такие комбинации *A* и *L*, как *A*=26, *L*=8 (пароль состоит из 8 малых символов английского алфавита), *A*=36, *L*=6 (пароль состоит из 6 символов, среди которых могут быть малые латинские буквы и произвольные цифры).

**Выбор пароля пользователя**

Большое значение при реализации СЗИ имеет реализация подсистемы идентификации и аутентификации пользователей. Как правило, на переднем крае обороны используются парольные подсистемы аутентификации пользователей. В данных подсистемах пользователь аутентифицируется по паролю, известному только ему и ни кому более.

Стойкость к взлому подсистемы парольной идентифика-ции/аутентификации во многом определяется тем, насколько правильно были сформированы пароли пользователей. При несоблюдении ряда требований к выбору паролей, данная стойкость в значительной степени уменьшается, и подсистема идентификации/аутентификации становится достаточно уязвима при правильно построенной атаке.

Ниже перечислены основные требования, которые должны быть учтены при выборе пароля пользователя.

Минимальная длина пароля должна быть не менее 6 символов. Сокращение длины пароля во многом повышает вероятность успешной атаки полным их перебором.

Пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.). Использование одной конкретной группы символов при формировании пароля в значительной степени повышает вероятность успешной атаки по маске.

В качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д. Использование в качестве паролей конкретных слов, имен в значительной степени повышает вероятность успешной атаки по словарю.

Иногда, генераторы паролей могут использовать при данном генерировании элементы, входящие в идентификатор пользователя (отдельные его символы, количество символов и т.д.). В отдельных вариантах, пароль может формироваться даже целиком из идентификатора на основе некоторого алгоритма. В последнем случае, заданному идентификатору пользователя ставится в соответствие единственный пароль, который формируется на основе идентификатора. Данный вариант формирования пароля используется во многих коммерческих программах, требующих регистрации пользователя (например, WinZip).

Например,

Идентификатор пользователя Vasilyev

Пароль 1Op(0Qp+

При этом, при формировании пароля 1Op(0Qp+ могут использоваться отдельные символы, входящие в идентификатор Vasilyev.

**Практическая часть**

**Задание 1.**

В таблице 1 найти для вашего варианта значения характеристик P,V,T.

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| Вариант | *P* | *V* | *T* |
| 1 | 10-4 | 15 паролей/мин | 2 недели |
| 2 | 10-5 | 3 паролей/мин | 10 дней |
| 3 | 10-6 | 10 паролей/мин | 5 дней |
| 4 | 10-7 | 11 паролей/мин | 6 дней |
| 5 | 10-4 | 100 паролей/день | 12 дней |
| 6 | 10-5 | 10 паролей/день | 1 месяц |
| 7 | 10-6 | 20 паролей/мин | 3 недели |
| 8 | 10-7 | 15 паролей/мин | 20 дней |
| 9 | 10-4 | 3 паролей/мин | 15 дней |
| 10 | 10-5 | 10 паролей/мин | 1 неделя |
| 11 | 10-6 | 11 паролей/мин | 2 недели |
| 12 | 10-7 | 100 паролей/день | 10 дней |
| 13 | 10-4 | 10 паролей/день | 5 дней |
| 14 | 10-5 | 20 паролей/мин | 6 дней |
| 15 | 10-6 | 15 паролей/мин | 12 дней |
| 16 | 10-7 | 3 паролей/мин | 1 месяц |

Вычислить по формуле (1) нижнюю границу S\* для заданных P,V,T.

Выбрать некоторый алфавит с мощностью A и получить минимальную длину пароля L, при котором выполняется условие (2).

Реализовать программу – генератор паролей пользователей. Программа должна формировать случайную последовательность символов длины L, при этом должен использоваться алфавит из A символов.

**Замечания:**

При реализации программы могут быть полезны следующие функции

RANDOM(N) – возвращает случайное число .

RANDOMIZE – сбрасывает начальное состояние датчика случайных чисел случайным образом.

CHR(X) – возвращает символ с ASCII кодом X. Коды различных групп символов приведены ниже.

Коды символов:

Коды английских символов : «A»=65,…,«Z»=90, «a»=97,…, «z» =122.

Коды цифр : «0» = 48, «9» = 57.

! - 33, “ – 34, # - 35, $ - 36, % - 37, & - 38, ‘ – 39, ( - 40, ) – 41, \* - 42.

Коды русских символов : «А» - 128, … «Я» - 159, «а» - 160,…, «п» - 175, «р» - 224,…, «я» - 239.

**Задание 2**

В таблице 2 найти требования, которым должен удовлетворять генератор паролей, соответствующий Вашему варианту.

Написать программу-генератор паролей, в соответствие с требованиями Вашего варианта. Программа должна выполнять следующие действия:

Ввод идентификатора пользователя с клавиатуры. Данный идентификатор представляет собой последовательность символов , где N – количество символов идентификатора (может быть любым),  - i – ый символ идентификатора пользователя.

1.4.2 Формирование пароля пользователя  для данного идентификатора, где M – количество символов пароля, соответствующее Вашему варианту, и вывод его на экран. Алгоритм получения символов пароля  указан в перечне требований Таблицы 2 для Вашего варианта.

Таблица 2

|  |  |  |
| --- | --- | --- |
| Вариант | Количество символов пароля | Перечень требований |
| 1 | 6 | 1.  - случайные заглавные буквы английского алфавита.  2. (где mod 10 – остаток от деления числа на 10).  3.  - случайная цифра.  4.  - случайный символ из множества {!,”,#,$,%,&,’,(,),\*}.  5.  - случайная малая буква английского алфавита. |
| 2 | 7 | 1.  - случайные малые буквы английского алфавита.  2. - случайные заглавные буквы английского алфавита.  3.  - двузначное число, равное . (Если остаток – однозначное число, то ). |
| 3 | 8 | 1.  - случайные цифры.  2.  - случайные символы из множества {!,”,#,$,%,&,’,(,),\*}.  3.  - случайная заглавная буква английского алфавита.  4.  - P –ая по счету малая буква английского алфавита, где . |
| 4 | 9 | 1.  - случайные символы из множества {!,”,#,$,%,&,’,(,),\*}, где .  2. Оставшиеся символы пароля, кроме , - случайные малые буквы английского алфавита.  3.  - случайная цифра. |
| 5 | 10 | 1.  - случайные цифры, где .  2.  - случайные большие буквы английского алфавита.  3.  - случайные малые буквы английского алфавита. |
| 6 | 11 | 1.  - случайные цифры.  2.  - случайные большие буквы английского алфавита, где .  3.  - случайные символы из множества {!,”,#,$,%,&,’,(,),\*}. |
| 7 | 11 | 1.  - случайные цифры.  2.  - случайные малые буквы русского алфавита, где .  3.  - случайные символы из множества {!,”,#,$,%,&,’,(,),\*}. |
| 8 | 12 | 1.  - случайные малые буквы английского алфавита, где .  2.  - случайные заглавные буквы английского алфавита, где .  3. Оставшиеся символы пароля – случайные цифры. |

Продолжение таблицы 2

|  |  |  |
| --- | --- | --- |
| 9 | 12 | 1.  - случайные малые буквы русского алфавита, где .  2.  - случайные заглавные буквы русского алфавита, где .  3. Оставшиеся символы пароля – случайные цифры. |
| 10 | 10 | 1.  - случайные цифры, где .  2.  - случайные большие буквы русского алфавита.  3.  - случайные малые буквы русского алфавита. |
| 11 | 9 | 1.  - случайные символы из множества {!,”,#,$,%,&,’,(,),\*}, где .  2. Оставшиеся символы пароля, кроме , - случайные малые буквы русские алфавита.  3.  - случайная цифра. |
| 12 | 8 | 1.  - случайные цифры.  2.  - случайные символы из множества {!,”,#,$,%,&,’,(,),\*}.  3.  - случайная заглавная буква русского алфавита.  4.  - P –ая по счету малая буква русского алфавита, где . |
| 13 | 7 | 1.  - случайные малые буквы русского алфавита.  2. - случайные заглавные буквы русского алфавита.  3.  - двузначное число, равное . (Если остаток – однозначное число, то ). |
| 14 | 6 | 1.  - случайные заглавные буквы русского алфавита.  2. (где mod 10 – остаток от деления числа на 10).  3.  - случайная цифра.  4.  - случайный символ из множества {!,”,#,$,%,&,’,(,),\*}.  5.  - случайная малая буква русского алфавита. |
| 15 | 6 | 1.  - случайные заглавные буквы английского алфавита.  2. (где mod 10 – остаток от деления числа на 10).  3.  - случайная цифра.  4.  - случайный символ из множества {!,”,#,$,%,&,’,(,),\*}.  5.  - случайная малая буква русского алфавита. |
| 16 | 7 | 1.  - случайные малые буквы русского алфавита.  2. - случайные заглавные буквы английского алфавита.  3.  - двузначное число, равное . (Если остаток – однозначное число, то ). |

ЗАМЕЧАНИЯ

1. Коды английских символов - «A»=65,…,«Z»=90, «a»=97,…, «z» =122.
2. Коды цифр – «0» = 48, «9» = 57.
3. Коды спец. символов ! – 33, “ – 34, # - 35, $ - 36, % - 37, & - 38, ‘ – 39, ( - 40, ) – 41, \* - 42.
4. Коды русских символов – «А» - 128, … «Я» - 159, «а» - 160,…, «п» - 175, «р» - 224,…, «я» - 239.

**Контрольные вопросы**:

1. В чем преимущество программных генераторов паролей по сравнению с выбором паролей человеком (пользователем либо администратором)?
2. Желательно либо нежелательно, по Вашему мнению, генерирование пароля пользователя на основании некоторого алгоритма из его идентификатора? Повысится либо понизится стойкость защиты при использовании такого алгоритма?
3. Чем определяется стойкость подсистемы идентификации и аутентификации?
4. Перечислить минимальные требования к выбору пароля.
5. Перечислить минимальные требования к подсистеме парольной аутентификации.
6. Как определить вероятность подбора пароля злоумышленником в течении срока его действия?
7. Выбором каким параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?