ВОРОНЕЖСКИЙ ИНСТИТУТ ВЫСОКИХ ТЕХНОЛОГИЙ – АНОО ВПО

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ЛАБОРАТОРНЫХ РАБОТ

По дисциплине «Защита информации»

Лабораторная работа № 2

«РЕАЛИЗАЦИЯ ГЕНЕРАТОРА ПАРОЛЕЙ С ЗАДАННЫМИ ТРЕБОВАНИЯМИ»

Цель работы – реализация простейшего генератора паролей, обладающего основными требованиями к парольным генераторам.

Теоретический материал

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 идентификации/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.

1. Минимальная длина пароля должна быть не менее 6 символов. Сокращение длины пароля во многом повышает вероятность успешной атаки полным их перебором.
2. 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.

3. 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.

Для более высокой степени защищенности, задача выбора паролей для пользователей должна решаться не человеком, а некоторой программой – генератором паролей, так как при большом количестве пользователей человеку-администратору будет достаточно сложно формировать пароли, удовлетворяющие вышеперечисленным требованиям.

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.

Задание на лабораторную работу

1. В таблице 1 найти требования, которым должен удовлетворять генератор паролей, соответствующий Вашему варианту.

2. Написать программу-генератор паролей, в соответствие с требованиями Вашего варианта. Программа должна выполнять следующие действия:
   a. Ввод идентификатора пользователя с клавиатуры. Данный идентификатор представляет собой последовательность символов $a_1 a_2 .. a_N$, где N – количество символов идентификатора (может быть любым), a_i - i – ый символ идентификатора пользователя.
   b. Формирование пароля пользователя $b_1 b_2 ... b_M$ для данного идентификатора, где M – количество символов пароля, соответствующее Вашему варианту, и вывод его на экран. Алгоритм получения символов пароля b_i указан в перечне требований Таблицы 1 для Вашего варианта.
3. Оцените скорость генерации паролей для Вашего варианта (количество паролей в единицу времени).

Таблица 1

Вариант	Количество символов пароля	Перечень требований
1	6	1. b_1, b_2 - случайные заглавные буквы английского алфавита. 2. $b_3 = N^2 \bmod 10$ (где mod 10 – остаток от деления числа на 10). 3. b_4 - случайная цифра. 4. b_5 - случайный символ из множества {!,”,#,$,%,&,’,(,),*}. 5. b_6 - случайная малая буква английского алфавита.
2	7	1. b_1, b_2, b_3 - случайные малые буквы английского алфавита. 2. b_4, b_5 - случайные заглавные буквы английского алфавита. 3. $b_6 b_7$ - двузначное число, равное $N^4 \bmod 100$. (Если остаток – однозначное число, то $b_6 = 0$).
3	8	1. b_1, b_2, b_3 - случайные цифры. 2. b_4, b_5 - случайные символы из множества {!,”,#,$,%,&,’,(,),*}. 3. b_7 - случайная заглавная буква английского алфавита. 4. b_8 - P –ая по счету малая буква английского алфавита, где $P = N^2 \bmod 10 + N^3 \bmod 10 + 1$.
4	9	1. $b_1, ..., b_{1+Q}$ - случайные символы из множества {!,”,#,$,%,&,’,(,),*}, где $Q = N \bmod 5$. 2. Оставшиеся символы пароля, кроме b_9, - случайные малые

		буквы английского алфавита. 3. b_9 - случайная цифра.
5	10	1. $b_{10-Q},...,b_{10}$ - случайные цифры, где $Q = N \bmod 6$. 2. b_1, b_2 - случайные большие буквы английского алфавита. 3. $b_3,...,b_{10-Q-1}$ - случайные малые буквы английского алфавита.
6	11	1. b_1, b_2 - случайные цифры. 2. $b_3,...,b_{3+Q}$ - случайные большие буквы английского алфавита, где $Q = N \bmod 8$. 3. $b_{4+Q},...,b_{11}$ - случайные символы из множества {!,",#,$,%,&,',(,),*}.
7	11	1. b_1, b_2 - случайные цифры. 2. $b_3,...,b_{3+Q}$ - случайные малые буквы русского алфавита, где $Q = N \bmod 8$. 3. $b_{4+Q},...,b_{11}$ - случайные символы из множества {!,",#,$,%,&,',(,),*}.
8	12	1. $b_1,...,b_{1+Q}$ - случайные малые буквы английского алфавита, где $Q = N^3 \bmod 5$. 2. $b_{1+Q+1},...,b_{1+Q+1+P}$ - случайные заглавные буквы английского алфавита, где $P = N^2 \bmod 6$. 3. Оставшиеся символы пароля – случайные цифры.
9	12	1. $b_1,...,b_{1+Q}$ - случайные малые буквы русского алфавита, где $Q = N^3 \bmod 5$. 2. $b_{1+Q+1},...,b_{1+Q+1+P}$ - случайные заглавные буквы русского алфавита, где $P = N^2 \bmod 6$. 3. Оставшиеся символы пароля – случайные цифры.
10	10	1. $b_{10-Q},...,b_{10}$ - случайные цифры, где $Q = N \bmod 6$. 2. b_1, b_2 - случайные большие буквы русского алфавита. 3. $b_3,...,b_{10-Q-1}$ - случайные малые буквы русского алфавита.
11	9	1. $b_1, b_2 ... b_{1+Q}$ - случайные символы из множества {!,",#,$,%,&,',(,),*}, где $Q = N \bmod 5$. 2. Оставшиеся символы пароля, кроме b_9, - случайные малые буквы русские алфавита. 3. b_9 - случайная цифра.
12	8	1. b_1, b_2, b_3 - случайные цифры. 2. b_4, b_5 - случайные символы из множества {!,",#,$,%,&,',(,),*}. 3. b_7 - случайная заглавная буква русского алфавита. 4. b_8 - P –ая по счету малая буква русского алфавита, где $P = N^2 \bmod 15 + N^3 \bmod 15 + 1$.
13	7	1. b_1, b_2, b_3 - случайные малые буквы русского алфавита. 2. b_4, b_5 - случайные заглавные буквы русского алфавита.

		3. $b_6 b_7$ - двузначное число, равное $N^4 \bmod 100$. (Если остаток – однозначное число, то $b_6 = 0$).
14	6	1. b_1, b_2 - случайные заглавные буквы русского алфавита. 2. $b_3 = N^2 \bmod 10$ (где mod 10 – остаток от деления числа на 10). 3. b_4 - случайная цифра. 4. b_5 - случайный символ из множества {!,”,#,$,%,&,’,(,),*}. 5. b_6 - случайная малая буква русского алфавита.
15	6	1. b_1, b_2 - случайные заглавные буквы английского алфавита. 2. $b_3 = N^2 \bmod 10$ (где mod 10 – остаток от деления числа на 10). 3. b_4 - случайная цифра. 4. b_5 - случайный символ из множества {!,”,#,$,%,&,’,(,),*}. 5. b_6 - случайная малая буква русского алфавита.
16	7	1. b_1, b_2, b_3 - случайные малые буквы русского алфавита. 2. b_4, b_5 - случайные заглавные буквы английского алфавита. 3. $b_6 b_7$ - двузначное число, равное $N^4 \bmod 100$. (Если остаток – однозначное число, то $b_6 = 0$).
17	8	1. b_1, b_2, b_3 - случайные цифры. 2. b_4, b_5 - случайные символы из множества {!,”,#,$,%,&,’,(,),*}. 3. b_7 - случайная заглавная буква английского алфавита. 4. b_8 - P –ая по счету малая буква русского алфавита, где $P = N^2 \bmod 10 + N^3 \bmod 10 + 1$.
18	9	1. $b_1, ..., b_{1+Q}$ - случайные цифры, где $Q = N \bmod 5$. 2. Оставшиеся символы пароля, кроме b_9, - случайные малые буквы английского алфавита. 3. b_9 - случайная цифра.
19	10	1. $b_{10-Q}, ..., b_{10}$ - случайные цифры, где $Q = N \bmod 6$. 2. b_1, b_2 - случайные большие буквы английского алфавита. 3. $b_3, ..., b_{10-Q-1}$ - случайные малые буквы русского алфавита.
20	11	1. b_1, b_2 - случайные символы из множества {!,”,#,$,%,&,’,(,),*}. 2. $b_3, ..., b_{3+Q}$ - случайные большие буквы английского алфавита, где $Q = N \bmod 8$. 3. $b_{4+Q}, ..., b_{11}$ - случайные цифры.
21	11	1. b_1, b_2 - случайные символы из множества {!,”,#,$,%,&,’,(,),*}. 2. $b_3, ..., b_{3+Q}$ - случайные малые буквы русского алфавита, где $Q = N \bmod 8$. 3. $b_{4+Q}, ..., b_{11}$ - случайные цифры.
22	12	1. $b_1, ..., b_{1+Q}$ - случайные малые буквы русского алфавита, где $Q = N^3 \bmod 5$. 2. $b_{1+Q+1}, ..., b_{1+Q+1+P}$ - случайные заглавные буквы английского

		алфавита, где $P = N^2 \bmod 6$. 3. Оставшиеся символы пароля – случайные цифры.
23	12	1. $b_1,...,b_{1+Q}$ - случайные малые буквы английского алфавита, где $Q = N^3 \bmod 5$. 2. $b_{1+Q+1},...,b_{1+Q+1+P}$ - случайные заглавные буквы русского алфавита, где $P = N^2 \bmod 6$. 3. Оставшиеся символы пароля – случайные цифры.
24	10	1. $b_{10-Q},...,b_{10}$ - случайные цифры, где $Q = N \bmod 6$. 2. b_1, b_2 - случайные большие буквы английского алфавита. 3. $b_3,...,b_{10-Q-1}$ - случайные малые буквы русского алфавита.
25	9	1. $b_1, b_2 ... b_{1+Q}$ - случайная цифра.. 2. Оставшиеся символы пароля, кроме b_9, - случайные малые буквы русские алфавита. 3. b_9 - случайные символы из множества {!,”,#,$,%,&,’,(,),*}, где $Q = N \bmod 5$.
26	8	1. b_1, b_2, b_3 - случайные цифры. 2. b_4, b_5 - случайные символы из множества {!,”,#,$,%,&,’,(,),*}. 3. b_7 - случайная заглавная буква английского алфавита. 4. b_8 - P –ая по счету малая буква русского алфавита, где $P = N^2 \bmod 15 + N^3 \bmod 15 + 1$.
27	7	1. b_1, b_2, b_3 - случайные малые буквы русского алфавита. 2. b_4, b_5 - случайные заглавные буквы английского алфавита. 3. $b_6 b_7$ - двузначное число, равное $N^4 \bmod 100$. (Если остаток – однозначное число, то $b_6 = 0$).
28	6	1. b_1, b_2 - случайные заглавные буквы английского алфавита. 2. $b_3 = N^2 \bmod 10$ (где mod 10 – остаток от деления числа на 10). 3. b_4 - случайная цифра. 4. b_5 - случайный символ из множества {!,”,#,$,%,&,’,(,),*}. 5. b_6 - случайная малая буква русского алфавита.

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?

Пример оформления отчета по лабораторной работе

ЛАБОРАТОРНАЯ РАБОТА №

НАЗВАНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

ВЫПОЛНИЛ: ст. гр. ….. ФИО

ВАРИАНТ № …

ЦЕЛЬ ЛАБОРАТОРНОЙ РАБОТЫ

КОЛИЧЕСТВО СИМВОЛОВ ПАРОЛЯ = …..

При реализации генератора паролей использовался следующий перечень требований к нему:

1.

2.

3.

4.

ТЕКСТ ПРОГРАММЫ

Примеры сгенерированных программой паролей:

1) ИДЕНТИФИКАТОР1 ….. ПАРОЛЬ1 ……

2) ИДЕНТИФИКАТОР2 ….. ПАРОЛЬ2 ……

3) ИДЕНТИФИКАТОР3 ….. ПАРОЛЬ3 ……

4) ИДЕНТИФИКАТОР4 ….. ПАРОЛЬ4……

5) ИДЕНТИФИКАТОР5 ….. ПАРОЛЬ5……

Скорость генерации паролей = ……. паролей / сек