1. ЛАБОРАТОРНАЯ РАБОТА № 1. РЕАЛИЗАЦИЯ ПРОСТЕЙШЕГО ГЕНЕРАТОРА ПАРОЛЕЙ

Цель работы: получение основных теоретических сведений и практических навыков по оценке стойкости парольной защиты.

1.1. Ход работы

1. Ознакомиться с теоретической частью данной работы.
2. Составить программу-генератор паролей.
3. Составить отчет по проделанной работе.
4. Защитить работу.

1.2. Содержание отчета

1. Тема.
2. Цель работы.
3. Ход работы.
4. Постановка задачи.
5. Листинг программы.
6. Результат выполнения программы.

1.3. Теоретическая справка

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.

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.

1.4. Задание к лабораторной работе № 1

Реализовать простейший генератор паролей, обладающий основными требованиями к парольным генераторам.

Программа должна выполнять следующие действия.

1. 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-й символ идентификатора пользователя.

2. 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 для вашего варианта (таблица 1).

Таблица 1

Варианты заданий на лабораторную работу № 1

Вариант	***M***	**Перечень требований**
1	6	b_1, b_2 — случайные заглавные буквы английского алфавита; $b_3 = N^2 \bmod 10$ (где mod 10 — остаток от деления числа на 10); b_4 — случайная цифра; b_5 — случайный символ из множества {!, ”, #, $, %, &, ’, (,), *}; b_6 — случайная малая буква английского алфавита
2	7	b_1, b_2, b_3 — случайные малые буквы английского алфавита; b_4, b_5 — случайные заглавные буквы английского алфавита; b_6, b_7 — двузначные числа, равные $N^4 \bmod 100$ (если остаток — однозначное число, то $b_6 = 0$)
3	8	b_1, b_2, b_3 — случайные цифры; b_4, b_5 — случайные символы из множества {!, ”, #, $, %, &, ’, (,), *}; b_6, b_7 — случайные заглавные буквы английского алфавита; b_8 — P-ая по счету малая буква английского алфавита, $P = N^2 \bmod 10 + N^3 \bmod 10 + 1$

Продолжение табл. 1

Вариант	*M*	Перечень требований
4	9	b_1, ..., b_{1+Q} — случайные символы из множества {!, ”, #, $, %, &, ’, (,), *}, где $Q = N\text{mod}5$. Оставшиеся символы пароля, кроме b_9, — случайные малые буквы английского алфавита; b_9 — случайная цифра
5	10	b_{10-Q}, ..., b_{10} — случайные цифры, где $Q = N\text{mod}6$; b_1, b_2 — случайные большие буквы английского алфавита; b_3, ..., b_{10-Q-1} — случайные малые буквы английского алфавита
6	11	b_1, b_2 — случайные цифры; b_3, ..., b_{3+Q} — случайные большие буквы английского алфавита, где $Q = N\text{mod}8$; b_{4+Q}, ..., b_{11} — случайные символы из множества {!, ”, #, $, %, &, ’, (,), *}
7	11	b_1, b_2 — случайные цифры; b_3, ..., b_{3+Q} — случайные малые буквы русского алфавита, где $Q = N\text{mod}8$; b_{4+Q}, ..., b_{11} — случайные символы из множества {!, ”, #, $, %, &, ’, (,), *}
8	12	b_1, ..., b_{1+Q} — случайные малые буквы английского алфавита, где $Q = N^3\text{mod}5$; b_{1+Q+1}, ..., $b_{1+Q+1+P}$ — случайные заглавные буквы английского алфавита, где $P = N^2\text{mod}6$. Оставшиеся символы пароля — случайные цифры
9	12	b_1, ..., b_{1+Q} — случайные малые буквы русского алфавита, где $Q = N^3\text{mod}5$; b_{1+Q+1}, ..., $b_{1+Q+1+P}$ — случайные заглавные буквы русского алфавита, где $P = N^2\text{mod}6$. Оставшиеся символы пароля — случайные цифры
10	10	b_{10-Q}, ..., b_{10} — случайные цифры, где $Q = N\text{mod}6$; b_1, b_2 — случайные большие буквы русского алфавита; b_3, ..., b_{10-Q-1} — случайные малые буквы русского алфавита
11	9	b_1, b_2, ..., b_{1+Q} — случайные символы из множества {!, ”, #, $, %, &, ’, (,), *}, где $Q = N\text{mod}5$. Оставшиеся символы пароля, кроме b_9, — случайные малые буквы русского алфавита; b_9 — случайная цифра
12	8	b_1, b_2, b_3 — случайные цифры; b_4, b_5 — случайные символы из множества {!, ”, #, $, %, &, ’, (,), *}; b_6, b_7 — случайные заглавные буквы русского алфавита; b_8 — P-ая по счету малая буква русского алфавита, где $P = N^2\text{mod}15 + N^3\text{mod}15 + 1$
13	7	b_1, b_2, b_3 — случайные малые буквы русского алфавита; b_4, b_5 — случайные заглавные буквы русского алфавита; b_6, b_7 — двузначные числа, равные $N^4\text{mod}100$ (если остаток — однозначное число, то $b_6 = 0$)
14	6	b_1, b_2 — случайные заглавные буквы русского алфавита; $b_3 = N^2\text{mod}10$ (где mod 10 — остаток от деления числа на 10); b_4 — случайная цифра; b_5 — случайный символ из множества {!, ”, #, $, %, &, ’, (,), *}; b_6 — случайная малая буква русского алфавита

Продолжение табл. 1

Вариант	*M*	Перечень требований
15	6	b_1, b_2 — случайные заглавные буквы английского алфавита; $b_3 = N^2 \bmod 10$ (где mod 10 — остаток от деления числа на 10); b_4 — случайная цифра; b_5 — случайный символ из множества {!, ”, #, $, %, &, ’, (,), *}; b_6 — случайная малая буква русского алфавита

1.5. Пример реализации лабораторной работы

Входным параметром здесь является произвольный идентификатор. Далее, в соответствии с перечнем требований, происходит генерация пароля.

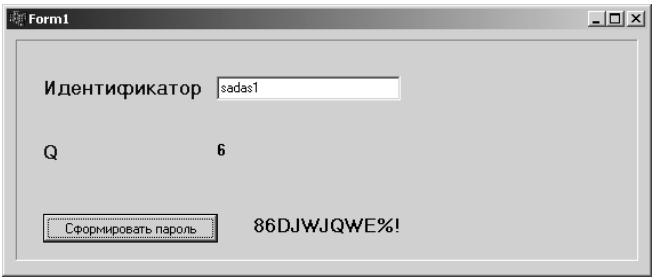

Рис. 1

Результат работы программы, реализующей простейший генератор паролей с заданными требованиями

Контрольные вопросы

1. Дать определение стойкости пароля к взлому. Написать формулу.
2. Дать определение мощности алфавита паролей.
3. Перечислить основные задачи, которые могут решаться с использованием определения стойкости пароля.
4. Перечислить основные требования к выбору пароля.