# *Лабораторная работа № 3.* парольний захист

*Мета роботи: реалізація генератора паролів, що володіє необхідною стійкістю до злому*.

## *Порядок виконання*

1. Ознайомитись з теоретичним матеріалом, пов'язаним з поняттями парольної аутентифікації користувачів і кількісною оцінкою стійкості парольного захисту (див. нижче).
2. У таблиці варіантів знайти значення характеристик *P, V, T* для вашого варіанту.
3. Обчислити нижню межу S \* для заданих *P, V, T* (формула (1)).
4. Вибрати деякий алфавіт з потужністю A і отримати мінімальну довжину пароля L, при якому виконується умова (2).
5. Написати програму для генерації паролів користувачів. Програма повинна формувати випадкову послідовність символів довжини L, з використанням алфавіту з A символів.

Для визначення кодів символів алфавіту А використовувати таблицю кодування ASCII -1250

1. Оформити звіт з лабораторної роботи.

*Вимоги до звіту:*

*1) Титульний аркуш*

*2) Введення (про особливості парольного захисту і його стійкість);*

*3) Основний розділ, в якому:*

*- сформулювати принципи обчислення нижньої межі числа паролів, і отримання мінімальної довжини пароля;*

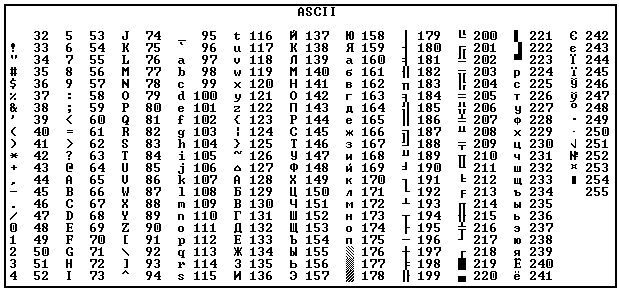
*- описати алгоритм і відобразити схеми генерації паролів користувачів;*

*- привести програмний код розробки з коментарями;*

*- відобразити отримані результати (випадкову послідовність символів довжини L, що є паролем, отриманим з алфавіту А), привести копії екранів.*

*4) Висновки*

Таблиця 1. Коди ASCII



**Таблиця 2. Варіанти завдань**

|  |  |  |  |
| --- | --- | --- | --- |
| Варіант | *P* | *V* | *T* |
| 1 | 10-4 | 20 паролів/ хвил | 2 тижні |
| 2 | 10-5 | 5 паролів/ хвил | 10 днів |
| 3 | 10-6 | 10 паролів/ хвил | 5 днів |
| 4 | 10-7 | 15 паролів/ хвил | 6 днів |
| 5 | 10-4 | 72 пароля/день | 12 днів |
| 6 | 10-5 | 24 пароля/день | 1 місяць |
| 7 | 10-6 | 20 паролів/хвил | 3 тижнеів |
| 8 | 10-7 | 15 паролів/хвил | 20 днів |
| 9 | 10-4 | 5 паролів/хвил | 15 днів |
| 10 | 10-5 | 10 паролів/хвил | 1 тиж. |
| 11 | 10-6 | 15 паролів/хвил | 2 тиж. |
| 12 | 10-7 | 120 паролів/день | 10 днів |
| 13 | 10-4 | 96 паролів/день | 5 днів |
| 14 | 10-5 | 20 паролів/хвил | 6 днів |
| 15 | 10-6 | 15 паролів/хвил | 12 днів |
| 16 | 10-7 | 2 пароля/хвил | 1 місяць |
| 17 | 10-4 | 10 паролів/хвил | 3 тиж. |
| 18 | 10-5 | 20 паролів/хвил | 20 днів |
| 19 | 10-6 | 144 пароля/день | 15 днів |
| 20 | 10-7 | 10 паролів/день | 1 тиж. |

**Теоретичні відомості до лабораторної роботи №3**

Парольні системи ідентифікації / аутентифікації - один з основних і найбільш поширених в системах захисту інформації методів розпізнавання користувачів.

Модуль аутентифікації по паролю найбільш часто піддається атакам з боку зловмисників, а методи парольної аутентифікації користувача при недотриманні вимог до вибору пароля є досить вразливими.

Основними мінімальними вимогами до вибору пароля і до підсистеми парольної аутентифікації користувача є нижчеперелічені:

1) в якості пароля не повинні використовуватися реальні дати, імена, прізвища та так далі.

2) пароль повинен складатися з різних груп символів (малі і великі латинські літери, цифри, спеціальні символи -, +, ', # і т.д.);

3) мінімальна довжина пароля повинна бути не менше, ніж N символів.

Рекомендації до підсистеми парольної аутентифікації:

1) в підсистемі парольної аутентифікації необхідно встановити обмеження числа спроб введення пароля (як правило, не більше трьох);

2) адміністратор системи повинен встановлювати максимальний термін дії пароля, після чого, пароль слід змінити;

3) в підсистемі парольної аутентифікації потрібно встановити ча-менную затримку в разі введення неправильного пароля.

Поширеним методом злому підсистеми пральний захисту є прямий перебір паролів (brute forcing).

Як правило, системні адміністратори використовують системи генерування паролів, які відповідають перерахованим вимогам. Генератори паролів використовуються як готові, так і самостійно розроблені.

**Кількісна оцінка стійкості парольного захисту**

Для проведення кількісної оцінки застосуємо позначення:

*A* – кількість символів, які можуть бути використані при складанні пароля (потужність алфавіту);

*L* – довжина пароля;

*S = AL* – кількість всіляких паролів довжини L, які можна скласти з символів алфавіту A;

*V* – швидкість перебору паролів зловмисником;

T - максимальний термін дії пароля.

*P – вірогідність* вибору пароля зловмисником протягом строку його дії:

*P =* (*V ∙ T*) */ S =* (*V ∙ T*) */ AL*.

Формула застосовується у різних випадках. Наприклад, якщо відомі значення *V, T та P вирішують задачу пошуку кількості можливих паролів. Далі, при наявності вимог на довжину паролю, знаходять мінімальну потужність алфавіту паролів A. Або вирішують задачу виявлення нижньої межі* числа всіляких паролів S\*.

Цілочисельне значення нижньої межі обчислюється за формулою

*S*\* = [*V∙P/T*], (1)

де [] – ціла частина числа, взята з округленням вгору.

Після визначення нижньої межі S \* необхідно вибрати такі A і L для формування S = AL, щоб виконувалася нерівність:

S \* ≤ S = AL. (2)

Тоді при виборі S, що задовольняє нерівності (2), можливість вибору пароля зловмисника (при заданих V і T) буде менше, ніж задана P.

*Зверніть увагу на необхідність узгодження розмірностей використовуваних в формулах параметрів.*

*Приклад*. Початкові дані: *P*= 10-6, *T*= 7 днів = 1 тиждень, *V*= 10 (паролів / хвилину) = 10 · 60·24·7 = 100800 паролів на тиждень.

Маємо: S\* = [(10800 ∙ 1) / 10-6] = = 108 ∙ 108.

Умові *S*\* ≤ *AL* задовольняють, наприклад, такі комбінації *A* і *L:*

*A* = 36, *L* = 6

*A* = 26, *L* = 8

**Контрольні питання**

1. Яким чином визначається стійкість підсистеми ідентифікації і аутентифікації та які параметри при цьому застосовуються?

2. Перерахуйте та поясніть вимоги до підсистеми парольної аутентифікації.

4. Сформулюйте та поясніть математичну модель визначення ймовірності підбору зловмисником пароля протягом строку його дії

5. Поясніть, вибір яких параметрів може вплинути на зменшення ймовірності підбору пароля зловмисником при відомій швидкості підбору пароля зловмисником і заданому терміні дії пароля?