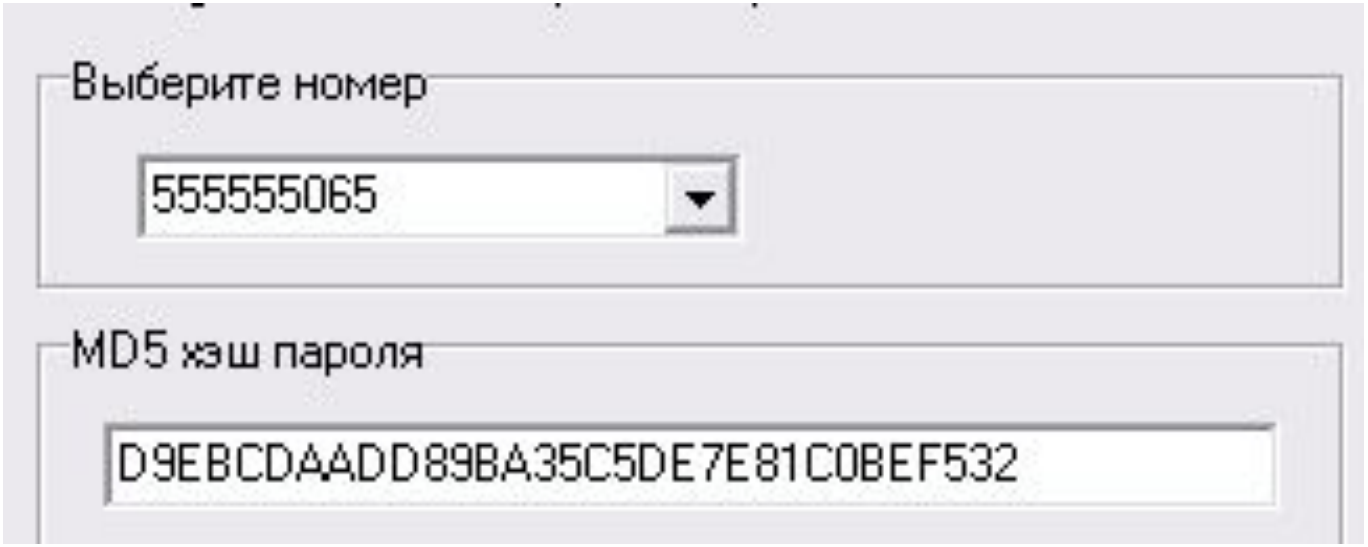
Правильные пароли

Руководство к пользованию

Пароль — условное слово или набор знаков, предназначенный для подтверждения личности или полномочий.

Пароли использовались в компьютерах с первых их дней. Например, CTSS от MIT, появившаяся в 1961 году, была одна из первых открытых систем. Она использовала команду LOGIN для запроса пароля пользователя

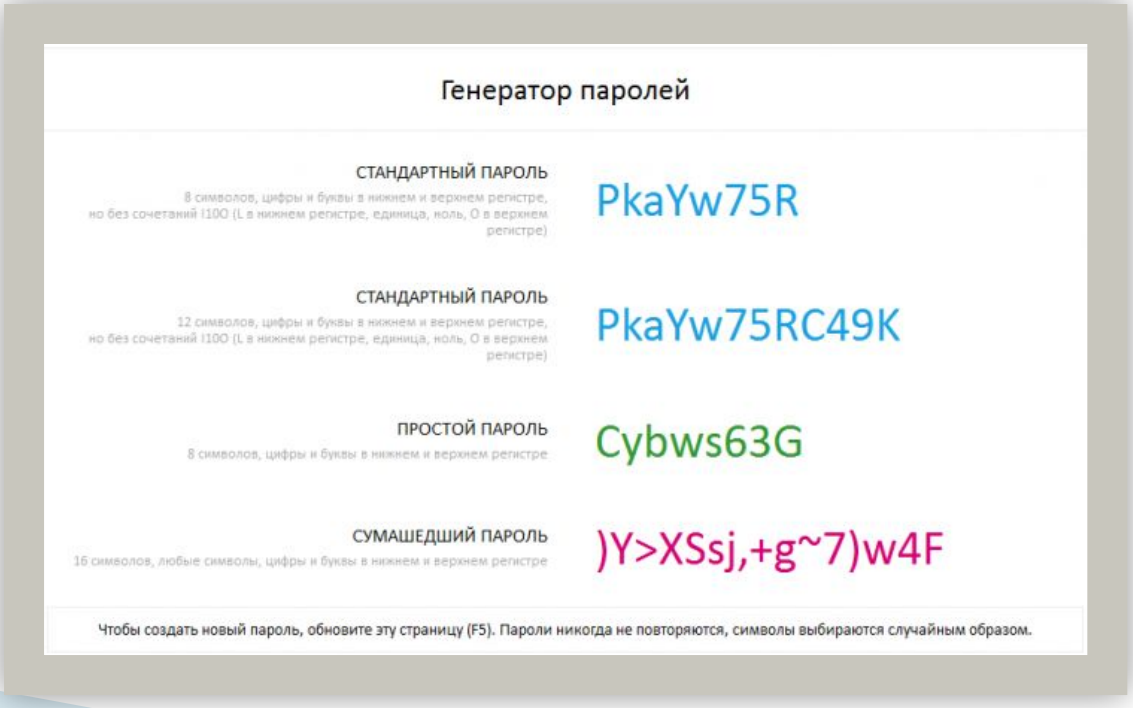
Роберт Моррис предложил идею хранения паролей в хэш-форме для операционной системы UNIX. Его алгоритм, известный как crypt, использует 12-битный salt и связывается для изменения формы с алгоритмом DES, снижая риск перебора по словарю



В конце 2017 года корпорация SplashData опубликовала 100 самых ненадежных паролей года. Первое место, уже 4 год подряд, занимает пароль - 123456. Его используют около 17% пользователей сети Интернет

Исходя из подходов к проведению атаки можно сформулировать критерии стойкости пароля к ней

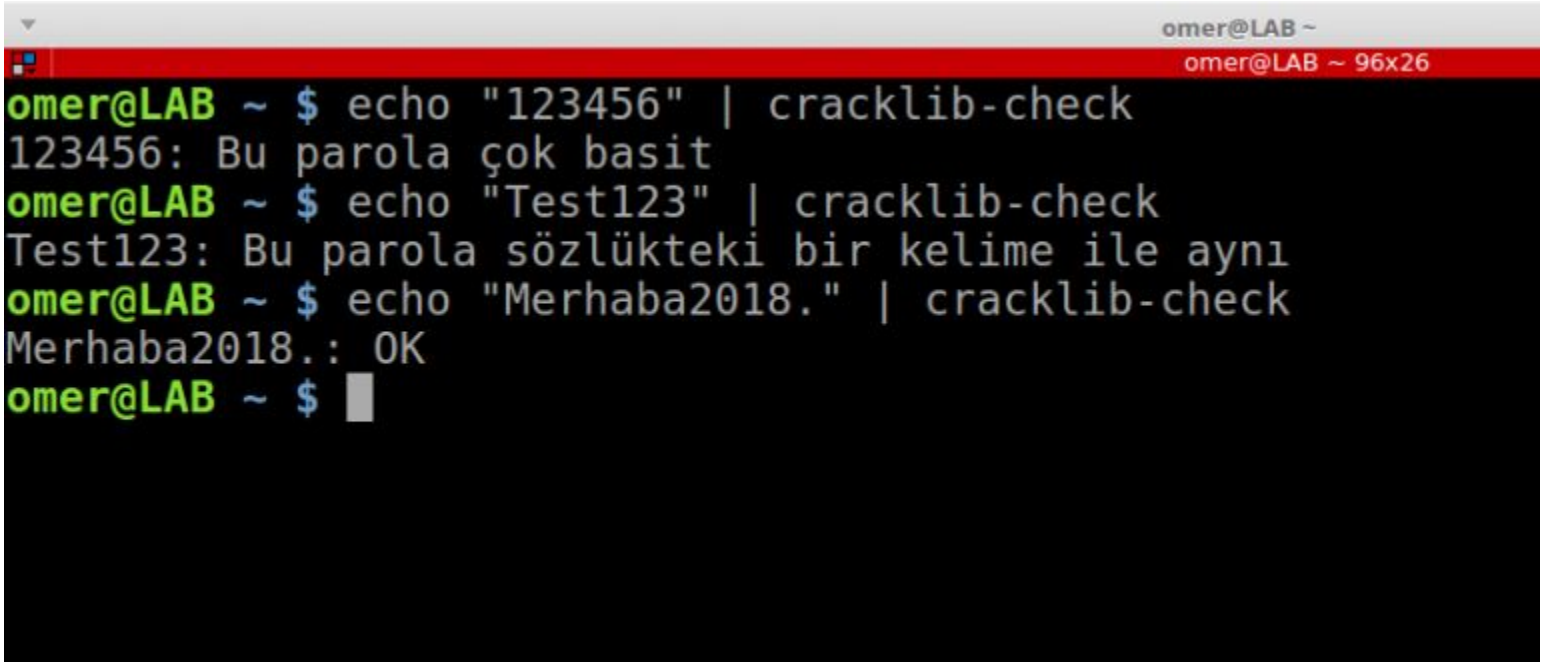
- 1. Должен быть длинным.
- 2 Не должен быть словарным словом.
- 3. Не должен состоять только из общедоступной информации о пользователе.



В качестве популярных рекомендаций к составлению пароля можно назвать использование сочетания слов с цифрами и специальными символами (#, $, * и т. д.)

Методы защиты можно разделить на две категории: обеспечение стойкости к взлому самого пароля, и предотвращение реализации атаки

Первая цель может быть достигнута проверкой устанавливаемого пароля на соответствие критериям сложности. Для такой проверки существуют автоматизированные решения, как, например, cracklib.



Вторая цель — предотвращение захвата хэша передаваемого пароля и защиту от многократных попыток входа в систему. Обычно накладывают ограничение на число попыток в единицу времени (fail2ban)