Lab 4.2 Report

Хеші було взято з репозиторію: https://github.com/Yurwar/human-password-generator/tree/master/src/main/resources.
Для взлому хешів використовувалась програма hashcat та типи атак dictionary та brute-force.

MD5.

Для атакти dictionary використовуємо команду
hashcat.exe -m 0 -a 0 -o cracked-passwords2.txt md5.csv common-passwords.txt
Хеші md5 дуже слабкі і перебираются дуже швидко.

Для атаки brute-force використовуємо наступну команду ***hashcat.exe -m 0 -a 3 -o cracked-passwords-md-5-brute.txt md5.csv -1?l?u?d ?1?1?1?1?1?1?1?1?1?1?1?1?1?1?1?1 --increment --increment-min 4 --increment-max 16***
Маючи достатньо великі потужності можна підібрати великий відсоток паролів за відносно невеликий час.

SHA1 + salt.

Для атакти dictionary використовуємо команду
hashcat.exe -m 110 -a 0 -o cracked-passwords4.txt salted-sha1.csv common-passwords.txt

Для атаки brute-force використовуємо наступну команду

hashcat.exe -m 110 -a 3 -o cracked-passwords-sha1-brute.txt salted-sha1.csv -1?l?u?d ?1?1?1?1?1?1?1?1?1?1?1?1?1?1?1?1 --increment --increment-min 4 --increment-max 16
З достатньою потужністю обчислювальних систем можна підібрати хеші за реальний час.

Bcrypt

Для атакти dictionary використовуємо команду

hashcat -m 3200 -a 0 -o cracked-passwords4.txt bcrypt.csv common-passwords-long.txt

bcrypt також стійкий до dictionary атаки.

Атака brute-force не проводилась бо для моєї обчислювальної системи це неможливо виконати за розумний час.

Висновки

Bcrypt - :)

sha-1 і md5 - :(

При створенні паролю варто дотримуватися таких рекомендацій: ● Пароль не повинен бути коротким(довжина має бути більше 8 символів)

- Не використовувати реальні слова
- Використовувати спецсимволи, великі та малі літери, цифри для того, щоб збільшити кількість варіантів при bruteforce
- Не використовувати часто вживані паролі

При хешуванні паролю варто використовувати стійкі до злому алгоритми хешування(bcrypt, scrypt, argon2)