Laboratorium 12

Entropia hasła

W sprawozdaniu zamieść zrzuty ekranu z istotnych etapów oraz odpowiedzi na pytania.

I. Wprowadzenie teoretyczne

Entropia hasła określa, jak trudne jest jego odgadnięcie metodą brute force.
Wyrażana jest w **bitach** i zależy od:

- liczby możliwych znaków (alfabetu),
- długości hasła,
- sposobu jego tworzenia (losowe vs. wymyślone przez człowieka).

Wzór:

$$\mathbf{Entropia} = \mathbf{N} \cdot \mathbf{log_2\, R}$$

Gdzie:

- N = liczba znaków hasła
- R = pula znaków, z których wybierane są znaki hasła

II. Zadanie 1 – **analiza haseł**

Dla poniższych haseł:

1. haslo123
2. Haslo123
3. Haslo123!
4. qwerty
5. Qwerty123
6. QwErTy!9
7. 12345678
8. 987654321
9. admin2024
10. Admin@2024
11. letmein!
12. pR7$kL2@
13. M4t3m@tykA
14. iloveyou
15. correcthorsebatterystaple
16. Tr0ub4dor&3
17. !QAZ2wsx
18. X9#f2L@p
19. ZaQ!2WsX
20. k0mpUt3r$
21. Student2024
22. Stud3nt!
23. Pa$$w0rd
24. Bezpieczenstwo!
25. R4nd0m#91

wykonaj:

1. Określ:
    a. długość hasła,
    b. użyty zbiór znaków (np. małe litery, duże, cyfry, znaki specjalne).
2. Oblicz entropię hasła w bitach.
3. Oceń jego odporność na atak brute force.
4. Porównaj otrzymane wyniki z rezultatami uzyskanymi za pomocą dedykowanych kalkulatorów entropii dostępnych w Internecie.

III. Zadanie 2 – **porównanie haseł**

Porównaj dwa hasła:

1. Password123!
2. losowe hasło o długości 12 znaków

Odpowiedz:

- które ma większą entropię?
- dlaczego hasło „wyglądające na skomplikowane” może być słabsze od losowego?

IV. Zadanie 3 – **projekt własnego hasła**

Zaprojektuj hasło spełniające warunki:

1. minimum 80 bitów entropii,
2. możliwe do zapamiętania przez człowieka,
3. nieużywane wcześniej w żadnym systemie.

Opisz:

- zastosowaną metodę,
- obliczenia,
- uzasadnienie wyboru.

V. **Uwagi końcowe**

- Nie używaj prawdziwych haseł.
- W sprawozdaniu stosuj hasła przykładowe lub fikcyjne.
- Entropia ≠ złożoność wizualna.
- Najsilniejsze hasła są losowe lub oparte na frazach losowych słów.