**Rozwiązanie zadania o entropii hasła**

**1. Czym jest entropia?**

**Entropia** w kontekście haseł i kryptografii to miara nieprzewidywalności lub losowości. Mówiąc prościej - określa, jak trudne jest odgadnięcie hasła przez atakującego.

Entropia jest mierzona w **bitach** i im wyższa wartość, tym bezpieczniejsze hasło. Entropia 256 bitów oznacza, że istnieje 2^256 możliwych kombinacji do sprawdzenia.

**2. Jak liczyć entropię?**

Entropia hasła obliczana jest według wzoru:

**$E = \log_2(N^L)$**

gdzie:

- **E** - entropia w bitach
- **N** - liczba możliwych znaków (rozmiar alfabetu)
- **L** - długość hasła
- **$\log_2$** - logarytm o podstawie 2

Wzór można uprościć do: **$E = L \times \log_2(N)$**

**Przykład:**

Jeśli mamy hasło składające się z 8 małych liter [a-z]:

- N = 26 (liczba liter w alfabecie)
- L = 8
- $E = 8 \times \log_2(26) = 8 \times 4{,}7 \approx 37{,}6$ bitów

**3. Czym jest klucz AES?**

**AES (Advanced Encryption Standard)** to symetryczny algorytm szyfrowania, który jest obecnie standardem w kryptografii.

AES może używać kluczy o długościach:

- **128 bitów** - podstawowy poziom bezpieczeństwa
- **192 bity** - zwiększone bezpieczeństwo
- **256 bitów** - najwyższy poziom bezpieczeństwa

**Klucz 256-bitowy AES** oznacza, że klucz szyfrujący ma długość 256 bitów, co daje 2^256 możliwych kombinacji (około 1,16 × 10^77 możliwości). Jest to uznawane za praktycznie nie do złamania przy obecnej mocy obliczeniowej.

**4. Rozwiązanie zadania**

Musimy znaleźć długość hasła **L**, które składa się tylko z małych liter [a-z], aby entropia wyniosła 256 bitów.

**Dane:**

- N = 26 (znaki od 'a' do 'z')
- E = 256 bitów (docelowa entropia)
- $\log_2(26) \approx 4{,}7004$

**Obliczenia:**

Z wzoru: $E = L \times \log_2(N)$

$256 = L \times \log_2(26)$

$L = 256 / \log_2(26)$

$L = 256 / 4{,}7004$

**$L \approx 54{,}46$**

**Odpowiedź:**

**Należy podać minimum 55 znaków [a-z]**, aby entropia hasła zbliżyła się do 256-bitowego klucza AES.

Dokładniej:

- 54 znaki dadzą entropię: 54 × 4,7 ≈ **253,8 bitów**
- 55 znaków dadzą entropię: 55 × 4,7 ≈ **258,5 bitów**

**5. Dodatkowe informacje praktyczne**

**Porównanie rozmiarów alfabetów:**

- Tylko małe litery [a-z]: 26 znaków → ~4,7 bitu na znak
- Małe i wielkie litery [a-zA-Z]: 52 znaki → ~5,7 bitu na znak
- Litery + cyfry [a-zA-Z0-9]: 62 znaki → ~6 bitów na znak
- Litery + cyfry + znaki specjalne: ~94 znaki → ~6,6 bitu na znak

**Ile znaków potrzeba dla różnych alfabetów, aby osiągnąć 256 bitów?**

- [a-z] (26): **55 znaków**
- [a-zA-Z] (52): **45 znaków**
- [a-zA-Z0-9] (62): **43 znaki**
- [a-zA-Z0-9 + znaki specjalne] (94): **39 znaków**

**Wnioski:**

1. Entropia rośnie logarytmicznie z rozmiarem alfabetu, ale liniowo z długością hasła
2. Używanie tylko małych liter wymaga bardzo długich haseł dla wysokiego bezpieczeństwa

3. Lepiej używać większego alfabetu (litery + cyfry + znaki specjalne) dla krótszych, ale równie bezpiecznych haseł
4. Hasło losowe o entropii 256 bitów jest równie bezpieczne jak klucz AES-256