Ochrona danych

Paweł Gliwny

pawel.gliwny@fis.uni.lodz.pl

Pokój 555

Zaliczenie

- Utworzyć katalog *Ochrona danych 2024 lato dzienne Imię Nazwisko* i dać dostęp pawel.gliwny@fis.uni.lodz.pl
- Na ostatnich zajęciach kolokwium gdzie można będzie korzystać ze swoich programów i notatek.

Szyfr Cezara

- Jedna z najstarszych znanych technik szyfrowania.
- Nazwa pochodzi od Juliusza Cezara, który używał tej metody do przesyłania tajnych wiadomości.
- Metoda ta polega na przesunięciu każdej litery w przesłanej wiadomości o ustaloną liczbę miejsc w alfabecie.
- Na przykład, przy użyciu przesunięcia o 3, litera A zostanie zamieniona na D, B na E, C na F, itd.

Jak działa szyfr Cezara?

- W szyfrze Cezara klucz szyfrowania określa wielkość przesunięcia. Aby zaszyfrować wiadomość, każdą literę tekstu jawnego przesuwamy w prawo o liczbę miejsc określoną przez klucz.
- Aby odszyfrować wiadomość, wykonujemy operację odwrotną, przesuwając litery w lewo.
- Szyfr jest prosty w implementacji, ale również łatwy do złamania ze względu na niską liczbę możliwych kluczy (w języku angielskim tylko 25).

Różne kombinacje

Występują kombinacje różniące się głównie zakresem i kolejnością znaków, co może mieć znaczenie w różnych kontekstach, takich jak sortowanie, kodowanie lub bezpieczeństwo danych.

- **a-z0-9**: Ten zakres zaczyna się od liter małych alfabetu angielskiego (od a do z), a kończy na cyfrach (od 0 do 9). W systemach sortowania, gdzie stosowana jest kolejność alfabetyczna, najpierw pojawią się litery, a po nich cyfry.
- **0-9a-z**: Tutaj najpierw pojawiają się cyfry (od 0 do 9), a następnie litery małe alfabetu angielskiego (od a do z). W kontekście sortowania lub kodowania, najpierw będą brane pod uwagę cyfry, a dopiero później litery.
- **a-zA-Z**: Ten zakres obejmuje wszystkie litery alfabetu angielskiego, najpierw małe (od a do z), a następnie duże (od A do Z). W tym przypadku nie są uwzględniane cyfry. W systemach sortowania najpierw pojawią się litery małe, a po nich litery duże.