***Generatory liczb pseudolosowych. Szyfry strumieniowe***

Ten kod jest implementacją synchronicznego strumieniowego szyfru z wykorzystaniem rejestru przesuwnego sprzężonego liniowo (Linear Feedback Shift Register - LFSR). Oto krótkie objaśnienie poszczególnych części kodu:

Importowanie biblioteki 'dart:math': potrzebna do generowania liczb losowych.



Funkcja główna main(): Jest to główna funkcja programu. Inicjalizuje ona zmienną message, która przechowuje wiadomość do zaszyfrowania, oraz listy key i seed, które zawierają klucz szyfrowania i nasiono rejestru przesuwnego. Następnie dodawany jest dodatkowy bit do klucza, a także tworzone są obiekty encryptionCipher i decryptionCipher reprezentujące szyfrowanie i deszyfrowanie wiadomości przy użyciu tego samego klucza i nasion. Następnie wiadomość jest szyfrowana i deszyfrowywana, a wyniki są wyświetlane na ekranie.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Klasa SynchronousStreamCipher: Jest to klasa reprezentująca synchroniczny strumieniowy szyfr. Konstruktor tej klasy tworzy obiekt encryptionRegister reprezentujący rejestr przesuwny sprzężony liniowo na podstawie podanych współczynników i nasiona.

Metoda encrypt: Szyfruje wiadomość przy użyciu rejestru szyfrowania. Wykorzystuje ona metodę map() do przetwarzania kodów Unicode poszczególnych znaków wiadomości. Każdy kod znaku jest zamieniany na odpowiednią wartość bitową (1 lub 0), a następnie XORowany z kolejnym bitem uzyskanym z rejestru szyfrowania. Wynikowy zaszyfrowany bit jest z powrotem zamieniany na kod ASCII i zwracany jako zaszyfrowany znak.

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

Klasa LinearFeedbackShiftRegister: Jest to klasa reprezentująca rejestr przesuwny sprzężony liniowo. Konstruktor tej klasy inicjalizuje rejestr na podstawie podanych współczynników wielomianu oraz opcjonalnego nasiona.

Metoda setSeed: Ustawia nasiono rejestru na podstawie podanego nasiona.

Metoda getNext: Pobiera kolejny bit z rejestru przesuwnego. W tej metodzie obliczany jest wynik na podstawie XORowania bitów rejestru z odpowiadającymi współczynnikami wielomianu. Następnie bity rejestru są przesuwane w prawo, a pierwszy bit jest aktualizowany na podstawie wyniku. Metoda zwraca wynik.

Metoda getRandomSeed: Generuje losowe nasiono o podanej długości.

Ten kod demonstruje działanie strumieniowego szyfrowania za pomocą rejestru przesuwnego sprzężonego liniowo. Klucz szyfrowania i nasiono rejestru determinują wynikowe zaszyfrowane i odszyfrowane wiadomości.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, System operacyjny

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

***Testy zgodnie z przykładami na Cez***

***Obraz zawierający tekst, Czcionka, zrzut ekranu, algebra

Opis wygenerowany automatycznie Obraz zawierający tekst, Czcionka, zrzut ekranu, Jaskrawoniebieski

Opis wygenerowany automatycznie***

***Wynik pokrywa się z poprawną odpowiedzią na Cez.***

Obraz zawierający tekst, Czcionka, biały, algebra

Opis wygenerowany automatycznieObraz zawierający Czcionka, tekst, zrzut ekranu, Jaskrawoniebieski

Opis wygenerowany automatycznie

***Wynik pokrywa się z poprawną odpowiedzią na Cez.***

Obraz zawierający tekst, Czcionka, zrzut ekranu, linia

Opis wygenerowany automatycznieObraz zawierający tekst, Czcionka, zrzut ekranu, Jaskrawoniebieski

Opis wygenerowany automatycznie

***Wynik pokrywa się z poprawną odpowiedzią na Cez.***