ВИБІР БАГАТОЧЛЕНІВ З МАКСИМАЛЬНИМ ПЕРІОДОМ ГЕНЕРАЦІЇ СТАНІВ

Рисований О.М., Ігнатьєв К.І., Рибалка Р.В., Рудаковський Д.Р.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Важливою задачею при скремблюванні є дослідження впливу різних ключів на результат скремблювання. В роботі використано шифрування за модулем як з використанням псевдовипадкової послідовності [1, 2], так й з використанням ключей з інкрементацією попередніх значень.

Головною частиною скремблера є лінійний n-каскадний регістр зсуву зі зворотними зв'язками, що генерує псевдовипадкову послідовність максимальної довжини (2^n-1). В роботі розроблена програма шифрування як з використанням ПВП з degP(x) = 4 в GF(2), так й з використанням ключів з інкрементацією попередніх значень. Крім того обчислені перевірочні матриці для degP(x) = 6 в GF(3).

Розроблено програмне створено за допомогою мови програмування C++. Для отримання основної частини коду використані середовища masm32, masm64. Для використання сучасних можливосте ОС Windows в галузі створення інтерфейсу використано файл маніфесту додатка, який написано на мові XML. Крім того, в файлі ресурсів використані структури опису версій програми.

Література:

1. Рисований О.М., Радченко М.О., Семененко С.В., Внуков В.В. Удосконалення захисту каналу управління безпілотного літального апарату на основі використання поліномів з кінцевих полів Галуа // Проблеми інформатизації. Тези доповідей одинадцятої міжнародної науково-технічної конференції. 16 – 17 листопада 2023 року / Черкаси – Харків – Баку – Бельсько-Бяла – 2021. Том 1. – С. 61.

2. Рисований О.М., Коломійцев Л.В., Альошин Г.В. та інш. Метод підвищення ефективності управління безпілотним літальним апаратом на основі використання нелінійного псевдовипадкового генератора // Scientific Collection "InterConf", (149): with the Proceedings of the 11 th International Scientific and Practical Conference "International Forum: Problems and Scientific Solutions" (April 6-8, 2023; Melbourne, Australia) by the SPC "InterConf". CSIRO Publishing House, – 2023. – P. 330.