

## МЕТОД ФОРМУВАННЯ ПРАВИЛ ПЕРЕСТАНОВКИ

Горбенко І.С.

Науковий керівник- д.т.н., професор Лужецький В.А.

Розробка є генератором псевдовипадкових чисел для реалізації операції перестановки блоків в алгоритмі блокового шифрування.

Оскільки перестановці підлягає кількість блоків, яка є змінною (залежить від довжини повідомлення і псевдовипадкового характеру довжини блоків), то жоден з відомих генераторів псевдовипадкових послідовностей (ПВП) не може бути використаний для формування правил перестановок, оскільки не завжди можна підібрати параметри стійкого генератора для заданого періоду послідовності для одних типів генераторів або не існує загальних методик побудови генераторів інших типів. Тому пропонується оригінальний метод генерування ПВП, який є основою правил перестановок.

Цей метод полягає в такому. Нехай кількість блоків  $N$ , їх номери  $n_i \in \{1, 2, \dots, N\}$ . Послідовність номерів блоків розбивається на дві групи –  $G_0 = \{1, \dots, \lfloor \frac{N}{2} \rfloor\}$  та  $G_1 = \{\lfloor \frac{N}{2} \rfloor + 1, \dots, N\}$ . Черговий номер блоку визначається символом  $s_i$  ПВП, що вказує на групу, з якої вибирається цей номер. Якщо символ ПВП «0», то номер вибирається з групи  $G_0$ , а якщо «1», то з групи  $G_1$ .

Підрахунок символів стану генератора ПВП здійснюють лічильники –  $СТ_0$  та  $СТ_1$  (для груп  $G_0$  та  $G_1$  відповідно), які працюють на зменшення.

Для отримання чергового номеру блоку використовується поточний стан відповідного лічильника ( $СТ_0$  або  $СТ_1$ ), порядок вибору номерів (від min до max або навпаки), кількість позицій зміщення номерів  $m$  та напрям зміщення (вліво або вправо). Обчислення здійснюється за модулем кількості блоків  $N$ .

В методі використовуються критерії зупинки, а саме:

– якщо лічильник  $СТ_0$  встановився в 0, то всі номери з групи  $G_0$  вичерпані і в подальшому символи  $s_i = 0$  пропускатимуться;

– якщо лічильник  $СТ_1$  встановився в 0 – завершення роботи з групою  $G_1$  і пропуск символів  $s_i = 1$ .

– якщо обидва лічильники встановились в 0, генератор зупиняється, оскільки використані всі номери блоків.

Параметрами генератора (ключовою складовою) є:

1) початковий стан генератора РЗЗЗ –  $S_0$  (64 розряди). Незвідний твірний поліном задається в самому алгоритмі.

2) Коди напрямків руху в групах  $G_0$  та  $G_1$  – 2 розряди (по 1 на групу):

3) циклічне зміщення номерів: кількість позицій  $m$  (13 розрядів) та напрям (1 розряд).

Загалом: 80 розрядів.