**Генерація S-Блока:**

Нелінійні вузли замін можливо представити у вигляді сукупності булевих фуекцій. S-бокс розмірності *n*x*m* можливо представити як сукіпність з *m* булевих функцій від *n* змінних. Також нелінійні вузли замін можливо представити у вигляді масиву десяткових чисел. Для збереження властивості бієктивності кожне десяткове число не повинно повторюсатися. В моїй реалізації для генерації вузла замін nxm використовується наступний алгоритм:

i = 0;

Поки (i < m){

k = випадкове число від 0 до 2n;

Якщо (k  A){

Почати генерацію спочатку

} інакше {

А[i++] = k;

}

}

**Алгоритм імітації відпалу:**

Пошук починається з деякого початкового стану S = S0. Параметр T­ – деякий контрольний параметр, відомий як температура. Т ініціюється високою температурою Т0 і з часом понижається. Для кожної темпераратури, виконується певна кількість кроків до нового стану (MIL – Moves in Inner Loop). Стан кандидата Y обирається випадковим чином із сусідів N(S) поточного стану. Віраховується зміна функції f, . Якщо значення f(S) покращується, то виконується крок відносно цього стану (S=Y); якщо ні, то він виконується з деякою вірогідністю. Чим гірше крок, тим менше вірогідність, що він буде прийнятий. Чим ниже температура T, тим иенш вірогідно, що гірший крок буде прийнято. Вірогідне прийняття рішення визначається генерацією випадкового чсла U в інтервалі (0…1) і виконанням нижчевказаного порівняння. Спочатку температура висока і кожен крок приймається. Зі зменшенням температури, стає все складніше приймати гірші кроки. У кінці приймаються тільки покращуючі кроки, і процес зупиняється. Алгоритм переривається, коли зустрічається критерій зупинки.Критерієм зупинки можуть бути очікувані значення автокореляції, нелінійності, тощо. В кожного внутрішнього циклу темература понижається. Найпростіший шлях зниження температури – помноження на сталу охолодження в інтервалі (0…1) (геометричне охолодження).

Алгоритм:

S=S0

T=T0

repeat (Повтор) {

for (int i = 0; i < MIL; i++)

{

обрати Y є N(S)

б = f(Y)-f(S)

якщо (б < 0), то

S = Y

иначе

генерація U = rnd(0,1)

якщо (U < exp(-б / T)), то S = Y

}

T = Txa

}

якщо (until) не досягнуто критерій зупинки.

**Генерація нащадка:**

Генерація нащадка вузла замін відбувається шляхом перестановки двух випадкових десяткових значень батьківського вузла, цей метод дожволяє зберегти властивість бієктивності.

**Функція cost:**

На даному етапі функція cost представляє собою