# ФУНКЦИЯ ВЫРАБОТКИ КЛЮЧА

Пусть – степень параллельности, – сложность, соль должна быть 64 бита. Функция будет вырабатывать 256 битный ключ.

:

– здесь – это 1024-битное слово

Представим в виде матрицы байтов :

Определим при как

Где для

Для

Для

Здесь – биективное отображение, ставящее в соответствие двоичной строке элемент поля.

Поле Галуа строим по модулю

Функция возвращает .

# ФУНКЦИЯ ШИФРОВАНИЯ БЛОКА