К ВОПРОСУ РОТАЦИИ БИТОВ В БЛОКЕ ШИФРОВАНИЯ

Главчев М.И., Носков В.И., Сахно Я.О.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

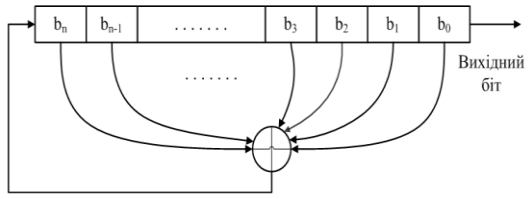
Используемые в криптографии симметричные системы в своих алгоритмах применяют различные структурные элементы. К таким элементам относятся:

– подстановки – замена одних элементов алфавита другими эквивалентными по длине;

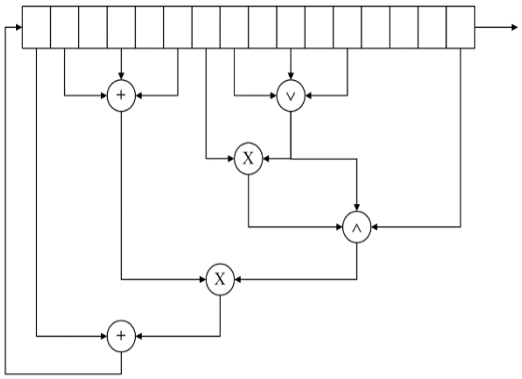
– перестановки – изменение положения элементов блока шифрования;

– мутации – изменение содержимого блока шифрования или ключа на основе преобразований;

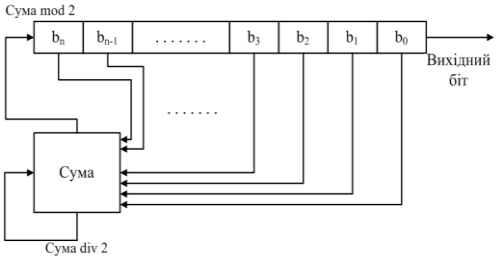
Одним из способов реализации мутации является ротация последовательности бит. Ротация бит может быть выполнена, к примеру следующими способами:



а) линейной обратной связью



в) нелинейной обратной связью



б) обратной связью по переносу

Все предложенные способы ротаций используют сдвиг бит после выполнения итерационного преобразования. Это позволяет использовать при программной реализации машинные команды, что значительно сокращает время выполнения криптоалгоритма. Использование ротации бит также актуально при необходимости аппаратной реализации криптоалгоритмов и основывается на использовании сдвиговых регистров.

В рамках выполнения работы было создано ротационное преобразования бит на основе использования нелинейной обратной связи с 3- и 5-битовыми последовательностями в пределах 512-рязрядного блока шифрования, которое также зависит от ключа шифрования.