СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ УСТРОЙСТВА ФАЗОВОЙ СИНХРОНИЗАЦИИ

Лисай А.И.
Кафедра вычислительных методов и программирования
Научный руководитель: Шилин Л.Ю., ассистент кафедры ВМиП
e-mail: aliakseilisai@gmail.com

***Аннотация* — Работа посвящена разработке симметрично – поточной криптосистемы с использованием системы фазовой автоподстройки частоты в качестве генератора гамма – последовательности.**

Ключевые слова: криптосистема; шифр; ключ; автоподстройка частоты

Шифрование — способ преобразования открытой информации в закрытую и обратно. Применяется для хранения важной информации в ненадёжных источниках или передачи её по незащищённым каналам связи.В зависимости от структуры используемых ключей методы шифрования подразделяются насимметричное шифрование: посторонним лицам может быть известен алгоритм шифрования, но неизвестна небольшая порция секретной информации — ключа, одинакового для отправителя и получателя сообщения;асимметричное шифрование: посторонним лицам может быть известен алгоритм шифрования, и, возможно, открытый ключ, но неизвестен закрытый ключ, известный только получателю.

Разработанная система представляет собой симметрично − поточную криптосистему, в которой шифрование проводится над каждым байтом исходного текста с использованием гаммирования. Источником гамма–последовательности является система фазовой автоподстройки частоты, работающая в режиме детерминированного хаоса [1,3,4]. С точки зрения шифрования процесс генерации необходимых последовательностей лучше представить следующим образом. На вход подаётся некоторый ключ, представляющий собой конечное множество чисел $\{a_1,a_2,...,a_k\}$. На выходе получаем последовательность $\{x_1,x_2,...,x_n\}$, которую можно использовать, например, для сложения с открытым текстом. В качестве ключевого пространства используется множество $A=A_1\times A_2\times...\times A_k$, представляющее собой множество ключей, при которых выходная последовательность имеет достаточную степень случайности.

Безопасность системы полностью зависит от свойств генератора потока ключей. Если он реализуется на конечном автомате (т.е. на компьютере), последовательность со временем повторится. Практически все генераторы псевдослучайных последовательностей за исключением одноразовых блокнотов являются периодическими. Поэтому, поток ключей должен иметь более длинный период, чем количество битов, выдаваемых между сменой ключей [5]. Генератор должен выдавать одну и ту же гамма − последовательность и для шифрования, и для дешифрирования. Поэтому важным моментом является однократное использование гамма – последовательности, а следовательно, необходима синхронизация передающего и принимающего устройств. Для этих целей предлагается использовать самосинхронизирующееся потоковые шифрование. Так ка внутреннее состояние генератора потока ключей является функцией предыдущих N битов шифротекста, торасшифрующий генератор потока ключей, приняв N битов, автоматически синхронизируется с шифрующим генератором. Реализация этого режима происходит следующим образом: каждое сообщение начинается случайным заголовком длиной N битов; заголовок шифруется, передаётся и расшифровывается; расшифровка является неправильной, зато после этих N бит оба генератора будут синхронизированы.

Последовательности чисел, получаемые при помощи генератора на основе устройства фазовой автоподстройки частоты, работающем в режиме детерминированного хаоса, были протестированы на случайность. Был рассмотрен группированный статистический ряд (рис. 1).

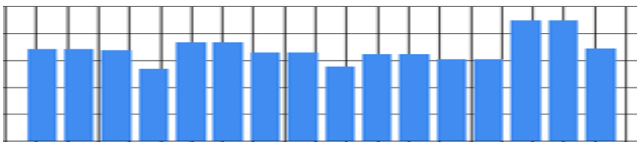

Рис. 1. Гистограмма статического ряда, построенная равноинтервальным способом

Были использованы статистические NIST, DIEHARD. Также тестирование проводилось по критериям сериальной корреляции, частот, интервалов, серий [2]. В исследовании использовались выборки объемом до 400 тыс бит. При расмотрении массива ключей большего объема наблюдалась периодичность выпадения значений.

[1] Кузнецов А.П., Батура М.П., Шилин Л.Ю. Анализ и параметрический синтез импульсных систем с фазовым управлением. Минск, 1993.

[2] Кнут Д. Искусство программирования, том 2 // М. Наука, 2001, -788 с.

[3] Шахгильдян В.В., Ляховкин А.А. Системы фазовой автоподстройки частоты // М.: Связь, 1972. -447 с.

[4] Акимов В.Н., Белюстина Л.Н., Белых В.Н. Системы фазовой синхронизации // М.: Радио и связь, 1982. -288 с.