Ёрмахмадзода Джаъфар

[jafaryor@gmail.com](mailto:jafaryor@gmail.com)

Крипто – алгоритмы

Межвузовский студенческий семинар на тему:

«Информационные технологии и программирование»

При развитии сетевых технологий всё актуальнее становится вопрос безопасности как в локальный сетях, так и в глобальной сети интернет. Безопасность особенно необходима в финансовых учреждениях, таких как банки (коммерческие и национальные), клиринговые палаты и др.

Шифрования данных является самым надёжным и простым видом защиты от взлома т.к. требует знания секретных ключей, а секретный ключ как известно знают только стороны, которые переписываются между собой.

Существуют также физический виды защиты такие как отделение локальной сети учреждения от глобальной сети.

Практически и теоритически доказано, что для взлома некоторых крипто-алгоритмов при нынешнем уровне развития технологий потребуется около 20 лет. Самые простые способы увеличение крипто стойкости алгоритма – это увеличение длины секретного ключа и последовательное применение одного и того же алгоритма несколько раз( например tripleDES = DES(DES(DES(Message, Key))) ).

Я в своей программе использовал следующие алгоритмы шифрования и архивации:

* Алгоритм транспортного кодирования BASE64
* Scrambler
* Алгоритм архивации Хаффмана
* Алгоритм архивации Лентеля – Зифа
* Алгоритм шифрования RSA
* Алгоритм шифрования tripleDES

В своём докладе я предлагаю использовать комбинацию этих алгоритмов шифрования и архивации, что даёт очень большую крипто стойкость и малый размер зашифрованного сообщение за счёт использования алгоритмов архивации.

Польза данного подхода в надёжности и малой размерности зашифрованного сообщения, что немаловажно в наше время.

Данный подход можно использовать при передаче очень важной информации по глобальной сети и не боятся за то, что кто - то его прочтёт или откорректирует.

Недостатки данного подхода заключаются в длительности этого процесса (как шифрования так и дешифрования), но этот недостаток компенсируется очень большой крипто стойкостью и малым размером зашифрованного сообщение.

В конце хочу заметить, что данный подход действительно работает и целесообразнее использовать его только в глобальной сети. Использования данного подхода в локальных сетях нежелательна из за длительности обработки входящих и исходящих данных каждого узла локальной сети.