ПОТОКОВАЯ КРИПТОСИСТЕМА.

Литвиненко А. В.

Криптография является практически единственным приемлемым средством защиты данных, передаваемых по коммуникационным сетям и хранимых на электронных носителях. Существуют различные криптосистемы, обеспечивающие достаточный уровень секретности информации. Но все надежные криптографические алгоритмы (DES, RSA и др.) требуют для работы значительных аппаратных ресурсов и зачастую не обеспечивают достаточную скорость шифрования информации. В то же время в ряде областей применения (например, в системах электронных расчетов), предъявляются очень высокие требования к надежности криптографических алгоритмов и накладываются жесткие ограничения на потребление ими аппаратных и временных ресурсов. На сегодняшний день проблема создания подобной криптосистемы не решена.

Автор видит выход в применении усовершенствованных потоковых криптосистем. Они основаны на формировании псевдослучайной последовательности битов или байтов (криптопотока), которые комбинируются с потоком шифруемых данных. Среди шифраторов данного класса выделяются алгоритмы, в которых для получения псевдослучайной последовательности применяется линейный сдвиговый регистр с обратной связью (LFSR). Эти шифраторы являются одними из самых быстрых и наименее требовательных к ресурсам. Однако они не обеспечивают достаточного уровня защиты данных вследствие слишком простой функциональной зависимости шифротекста от исходного текста и криптопотока. Это позволяет легко вычислить криптопоток и на основе его анализа получить характеристический полином сдвигового регистра, являющийся ключом алгоритма.

Автор предлагает метод усовершенствования таких криптосистем, позволяющий обеспечить достаточный уровень защиты информации за счет незначительного увеличения потребляемых ресурсов и небольшого уменьшения быстродействия. Идея состоит в том, чтобы комбинировать формируемый сдвиговым регистром криптопоток и исходный текст случайным образом. Символ исходного текста складывается по модулю 256 с некоторым байтом LFSR. Полученная сумма используется как индекс для выбора байта из массива, представляющего случайную перестановку из 256 символов. Полученное значение точно так же комбинируется с другим байтом LFSR, образуя индекс для выбора элемента из второго массива. Байт, полученный из третьего массива, представляет собой шифрокод исходного символа. Для кодирования каждого байта текста значение LFSR сдвигается на один такт. Ключом алгоритма являются три случайных перестановки из 256 символов, представленные в массивах, и характеристический полином LFSR. Такой метод комбинирования криптопотока и исходного текста делает неэффективными аналити-

ческие методы атаки против алгоритма и лишь незначительно снижает скорость шифрования.

Преимуществами предложенного метода шифрования данных являются малый объем необходимой памяти (менее 1 Кбайт) и высокая скорость кодирования информации. Аналитические методы атаки против данного алгоритма не дают результата, а поиск ключа прямым перебором неэффективен ввиду его большой длины $((256!)^3 \tilde{n} 2^N$, где 256 - количество байт в каждом массиве, 3 - число массивов, N - разрядность LFSR).

Таким образом, предлагаемая криптосистема представляет собой удачное сочетание высокой степени защиты данных с хорошей производительностью при потреблении незначительных ресурсов.

СОЗДАНИЕ ЭЛЕКТРОННОГО УЧЕБНИКА С ОТСЛЕЖИВАНИЕМ ОШИБОК ОБУЧЕНИЯ В СРЕДЕ MULTIMEDIA

Матюшков Л.П., Зудина Г.С.

Анализ литературных источников, статей и отчетов стажеров позволяет сделать вывод,что использование ПК в учебном процессе развивается в двух направлениях: использование промышленных систем производства работ (типа P-CAD, Auto CAD и других)и создания учебников в среде MULTIMEDIA.

Улучшение эргономических показателей экранов, нарастающая мощность компьютеров и ресурсов памяти позволяют создать электронный учебник со средствами контроля усвоения материала и возможностями корректировки усваивания. Обычно ошибки классифицируются по трем видам: нарушение принципа постепенности, отсутствие связи предмета с реальным физическим миром(отсутствие массы) и непроясненные слова.

При создании такого учебника автор строго определяет последовательность изучения материала, первое вхождение ключевых слов, которые должны быть прояснены в соответствии со спецификой предмета, и область действия мультипликационной вставки ,для обретения обучающимся массы.

Операционная система WINDOWS, с возможностью наложения окон и графическим экраном имеет эффективные средства для решения поставленной задачи.

Создание электронного учебника делится на несколько этапов:

-создание структурной схемы учебника с включением приложений;

-создание гипертекста учебника;

-создание библиотеки графических иллюстраций;

-создание интерактивной среды чтения учебника.

Каждый электронный учебник должен иметь доступ к толковому словарю языка на котором он написан.