И.М. Шаяхметов

ИССЛЕДОВАНИЕ РАБОТЫ КРИПТОСИСТЕМ И СИСТЕМ УСТАНОВКИ ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ

(Казанский национальный исследовательский университет им. А.Н.Туполева-КАИ)

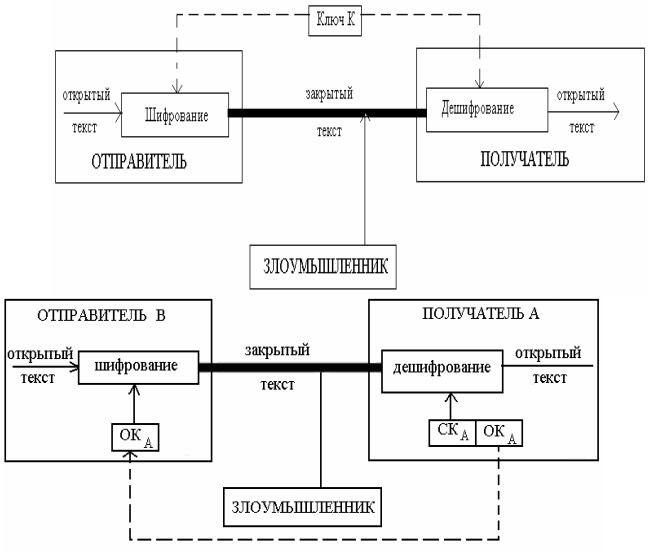
Симметричные криптосистемы применялись задолго до появления электронных информационных технологий.

В данных криптосистемах шифрование и дешифрование информации осуществляется на одном ключе, являющемся секретным. Рассекречивание ключа шифрования ведет к рассекречиванию всего защищенного обмена.

Другим классом криптографическим систем являются асимметричные криптосистемы, называемые также криптосистемами с открытым ключом. В асимметричных криптосистемах для шифрования информации используется один ключ, а для дешифрования – другой [2, с. 488].

Целью работы является проведение анализа зашифрованных текстов и определение распределенности символов в них.

Функциональные схемы взаимодействия участников симметричного и асимметричного криптографических обменов приведены на рис. 1.



а) б)

Рис. 1. Функциональная схема:
а) симметричной криптосистемы;
б) асимметричной криптосистемы;

При обмене электронными документами по открытым каналам возникает проблема аутентификации автора сообщения и контроля целостности документа. Собственно, сама информация в документе может быть открыта, однако ее изменение может привести к катастрофическим последствиям.

Для обычных, бумажных носителей указанные проблемы решаются путем жесткой привязки информации к физическому носителю, что позволяет использовать для защиты рукописные подписи, печати, водяные знаки и т.д. [3, с. 266]. Для электронных документов эта проблема решается путем привязки к ним особой цифровой последовательности – электронно-цифровой подписи (ЭЦП). Функциональная схема использования ЭЦП приведена на рис. 2.

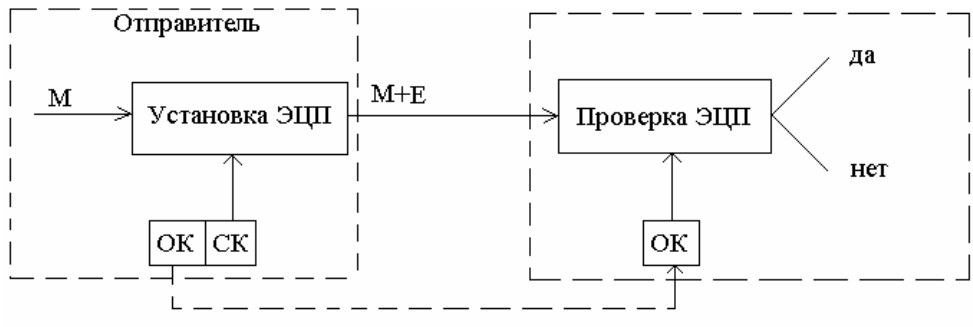


Рис. 2.Функциональная схема использования ЭЦП

Интерфейсы программы определения частоты символов представлены на рис.3., рис.4.

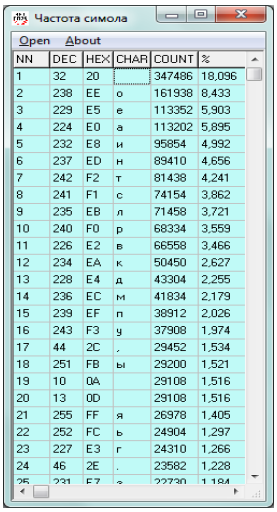


Рис.3. Частота символов исходного текста

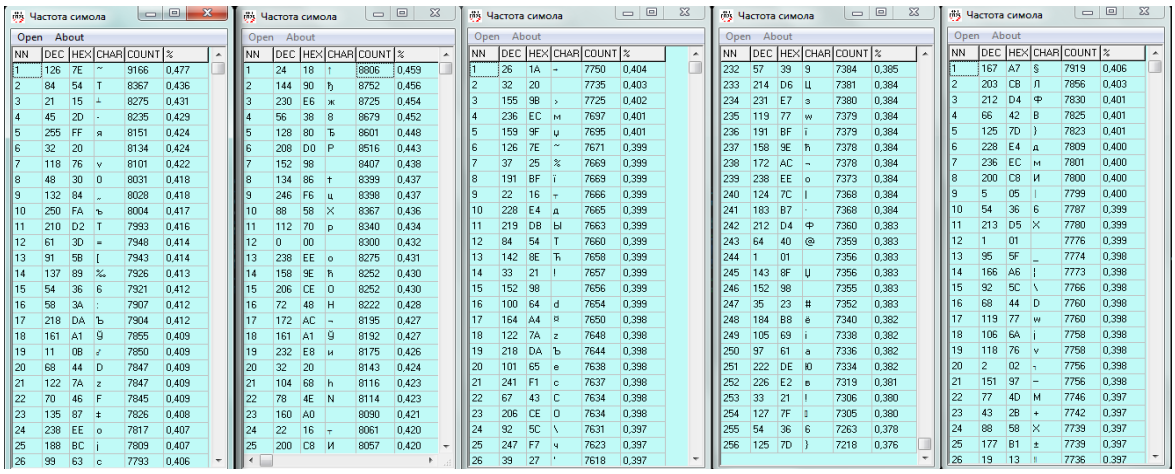


Рис.4. Частотности символов зашифрованных текстов.

На основе анализа зашифрованных текстов мы можем сделать вывод, что частотности символов в них равномерно распределены в отличии от частотности исходного текста.

Скорость шифрования по алгоритму RSAявляется большей, чем скорость шифрования в других алгоритмах.

После изменения одного символа в файле «Opentext.txt» и после проверки истинности ЭЦП система не смогла распознать изменения.

В качестве организации криптографического обмена между двумя абонентами в симметричных и асимметричных криптосистемах были проделаны нижеперечисленные операции в нашей программе.

a. Зашифровали некоторый файл по симметричному алгоритму DES и вместе с ключом шифрования передали зашифрованный файл соседу.

b. Получили от соседа файл, зашифрованный по алгоритму DES, а также ключ шифрования, и попытались расшифровать данный файл.

c. Зашифровали для соседа некоторый файл по асимметричному алгоритму RSA и передали зашифрованный файл соседу.

d. Получили от соседа файл, зашифрованный по алгоритму RSA на Нашем открытом ключе, и попытались расшифровать данный файл.

Так как все операции прошли успешно, можно сказать, что получилось реализовать организацию криптографического обмена между двумя абонентами в симметричных и асимметричных криптосистемах.

Литература

1. Теоретические основы компьютерной безопасности. Уч. Пособие для вузов по спец. "Компьютерная безопасность", "Компьютерное обеспечение информационной безопасности автоматизированных систем"/ П.Н. Девытин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербатов. – М.: Радио и связь.2000 – 190 с.

2. Основы информационной безопасности. Учебное пособие для вузов/Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов – М.: Горячая линия – Телеком, 2006-544 с.

3. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001 – 368 с.

П.К. Шиверов, В.М. Пахомов

ИСТОЧНИКИ ДОВЕРИЯ В КОНТЕКСТЕ СТОЙКОСТИ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ

(Самарский государственный университет)

Введение

Анализ стойкости протоколов аутентификации, во многом, зависит от возможности установить наличие доверия между двумя или более общающимися абонентами сети.