Кафедра КиИИ

ЛЕКЦИЯ

Тема: Криптографические методы преобразования и защиты информации

Дисциплина: Основы кодирования

ОП Системы информационной безопасности

Авторы: Ассоц. проф. КиИИ Даненова Г.Т.
Ассоц. проф. КиИИ Коккоз М.М.
Ассоц. проф. КиИИ Кан О.А.
Ассоц. проф. СМиТ Ахметжанов Т.Б.

План лекции

1. Алгоритмы ассиметричного шифрования.
2. Анализ простых шифров.
3. Шифр замены.
4. Шифр перестановки.
5. Шифр Вернама.
6. Квадрат Полибия.
7. Контрольные вопросы.

Алгоритмы ассиметричного шифрования

Среди наиболее известных алгоритмов, реализующих асимметричное шифрование, можно назвать **RSA** (Rivest-Shamir-Adleman) и **DSA** (Digital Signature Algorithm).

Криптосистема RSA стала первой системой, пригодной и для ассиметричного шифрования, и для цифровой подписи.

Алгоритм DSA применяется для создания цифровой подписи.

Одним из наиболее известных алгоритмов асимметричного шифрования является RSA, названный аббревиатурами его создателей — Rivest, Shamir и Adleman. Алгоритм разрабатывался с середины 1970-х годов и был запатентован в США в 1983 году.

Математической базой алгоритма RSA является математическая задача факторизации произведения двух больших простых чисел.

В алгоритме RSA задействованы случайные простые числа n и q огромных размеров. Они перемножаются, и полученный результат n задействуется еще в нескольких математических операциях. В итоге получаются два значения: одно секретное (секретный ключ) и одно публичное (открытый ключ).

Что касается криптостойкости алгоритма RSA, то главной задачей потенциального взломщика алгоритма является вычисление двух простых множителей n и q.

В 2010 году с этой задачей успешно справилась группа ученых, которым удалось вычислить простые множители для криптографического ключа RSA размером 768 бит.

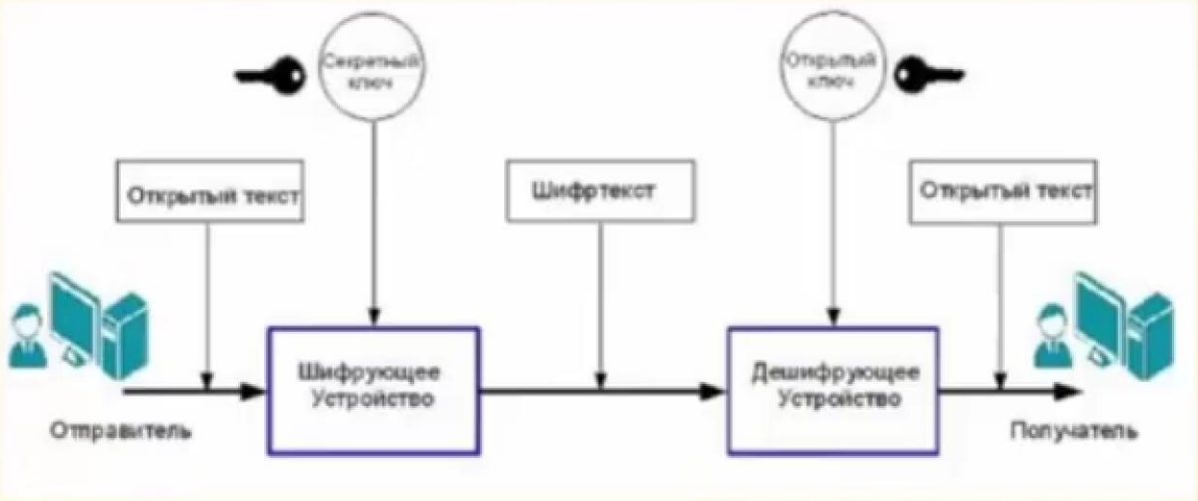
На вскрытие RSA-768 ушло два года и были задействованы сотни компьютеров.

Ученые пришли к выводу, что алгоритм RSA может быть стойким только при длине ключа не менее 1024 бит.

При использовании алгоритма RSA можно не только использовать открытый ключ для шифрования, а секретный для расшифрования, но и наоборот.

С помощью секретного ключа шифруется сообщение. Открытый ключ свободно доступен и любой может расшифровать информацию, но это дает способ поручиться за достоверность источника сообщения. Если открытый ключ правильно расшифровывает данные, значит, они были зашифрованы с помощью секретного ключа соответствующего отправителя.

Применение цифровой подписи



Как правило, при создании цифровой подписи шифруется не весь открытый текст, а определенный фрагмент, так называемый ***дайджест сообщения*** (message digest).

К фрагменту сообщения добавляется информация о том, кто подписывает документ. Получившаяся строка далее зашифровывается секретным ключом. Получившийся зашифрованный набор бит и представляет собой электронную подпись.

Таким образом, ЭЦП это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронно-цифровая подпись - это программно-криптографическое средство, которое обеспечивает:

- проверку целостности документов;
- конфиденциальность документов;
- установление лица, отправившего документ.

Шифрование с использованием ключа k=3. Буква «А» «сдвигается» на три буквы вперёд и становится буквой «Г». Буква «Я», перемещённая на три буквы вперёд, становится буквой «В».

Исходный алфавит: А Б В Г Д Е ..... Э Ю Я
Шифрованный: Г Д Е Ё Ж З ..... А Б В

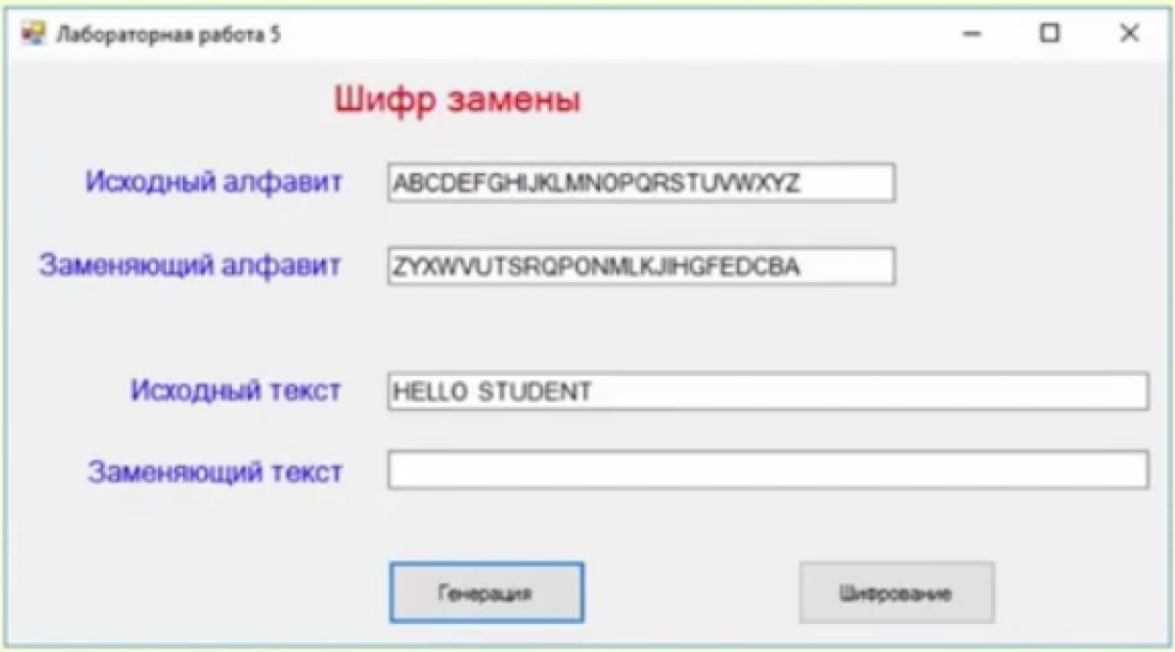
Пример.
Исходный текст:
Съешь ещё этих мягких французских булок.
Зашифрованный текст:
Фэзыя зьи ахлш пвёнлш чугрщцкфнлш дцосн.

Шифр замены

Шифр замены является простейшим. Как следует из самого названия, он осуществляет преобразование путем замены символов открытого текста в зашифрованный.

Пусть **X** и **Y** - два алфавита открытого и, соответственно, шифрованного текста, состоящие из одинаковых символов. Пусть g(x) взаимооднозначное отображение **X** в **Y**. Это означает, что каждой букве ***x*** алфавита **X**, однозначно соответствует определенная буква ***y*** алфавита **Y**.

Шифр замены



Шифр Вернама

Шифр является разновидностью криптосистемы одноразовых блокнотов. В нём используется булева функция «Сложение по модулю 2».

Шифр назван в честь Гильберта Вернама, который в 1917г. изобрёл, а в 1919г. запатентовал систему автоматического шифрования телеграфных сообщений.

Шифр Вернама является примером системы с абсолютной криптографической стойкостью. При этом он считается одной из простейших криптосистем.

Контрольные вопросы

1. Что является математической базой алгоритма RSA?
2. Для чего применяется ЭЦП?
3. Опишите алгоритм шифра замены.
4. Как работает шифр Вернама?
5. Как шифруется информация с помощью квадрата Полибия?

Спасибо за внимание!