ОГА ПОУ «Новгородский торгово-технологический техникум»

Проект

По теме: «История развития методов шифрования»

Секция 05 Технические науки

Выполнил:

студент 2 курса гр. 20-ГД

Егоренкова Анастасия

Руководитель: Попов В.С.

Великий Новгород

2022 г.

Оглавление

[Введение 3](#_Toc107060701)

[1. Основные методы шифрования 4](#_Toc107060702)

[2. Симметричный и ассиметричный метод шифрования 4](#_Toc107060703)

[3. Шифр Виженера и его практическое применение 4](#_Toc107060704)

[Заключение 6](#_Toc107060705)

[Список литературы 7](#_Toc107060706)

# Введение

Актуальность. Современное общество все в большей степени становится информационно–обусловленным, успех любого вида деятельности все сильней зависит от обладания определенными сведениями и от отсутствия их у конкурентов. И чем сильней проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере, и тем больше потребность в защите информации. Одним словом, возникновение индустрии обработки информации с железной необходимостью привело к возникновению индустрии средств защиты информации.

Объект исследования – методы шифрования

Предмет – история развития методов шифрования

Цель исследования – изучить историю развития методов шифрования.

Для данной цели, были поставлены задачи:

1. Познакомиться с основными методами шифрования
2. Понять отличия симметричного и ассиметричного метода шифрования
3. Практическое применение метода шифрования.
4. Сделать выводы.
5. Основные методы шифрования

Под шифрованием понимается такой вид криптографического закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения. Все известные способы шифрования можно разбить на пять групп с разновидностями:

1. Замена - Простая (одноалфавитная), многоалфавитная одноконтурная обыкновенная, многоалфавитная одноконтурная монофоническая, многоалфавитная многоконтурная
2. Перестановка – Простая, усложнённая по таблице, усложнённая по маршрутам
3. Аналитическое преобразование - с использованием алгебры матриц, по особым зависимостям
4. Гаммирование - с конечной короткой гаммой, с конечной длинной гаммой, с бесконечной гаммой
5. Комбинированные методы - замена и перестановка, замена и гаммирование, Перестановка и гаммирование

**Подстановка** – наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.

**Перестановка** – несложный метод криптографического преобразования. Используется, как правило, в сочетании с другими методами.

**Гаммирование** – этот метод заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

Шифрование с помощью аналитических преобразований. Достаточно надежное закрытие информации может обеспечить использование некоторых аналитических преобразований (с помощью функций). Например, можно использовать методы алгебры матриц - в частности умножение матрицы на вектор.

В качестве ключа задается квадратная матрица ||a|| размера n\*n. Исходный текст разбивается на блоки длиной n символов. Каждый блок рассматривается как n-мерный вектор. А процесс шифрования блока заключается в получении нового n-мерного вектора (зашифрованного блока) как результата умножения матрицы ||a|| на исходный вектор.

Расшифрование текста происходит с помощью такого же преобразования, только с помощью матрицы, обратной ||a||. Очевидно, что ключевая матрица ||a|| должна быть невырожденной.

При использовании методов шифрования используются ключи, по которым получатель в силах с лёгкостью преобразовать зашифрованную информацию в исходный, несущий смысл, вид. В зависимости от ключей алгоритм шифрования может симметричным и ассиметричным. В первом случае информация шифруется и дешифруется одним и тем же ключом, во втором же нужны разные ключи.  
Нередко используются средства сокрытия ключа вместе с шифруемой информацией.

1. Симметричный и ассиметричный метод шифрования

Симметричный метод шифрования

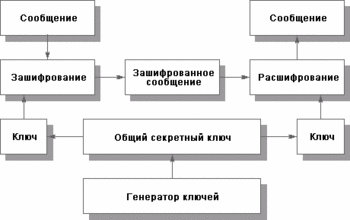


Рис. 1. Использование симметричного метода шифрования

Один и тот же ключ (хранящийся в секрете) используется и для зашифрования, и для расшифрования данных. Разработаны весьма эффективные (быстрые и надежные) методы симметричного шифрования. Существует и национальный стандарт на подобные методы - ГОСТ 28147–89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Рис.1 иллюстрирует использование симметричного шифрования. Для определенности мы будем вести речь о защите сообщений, хотя события могут развиваться не только в пространстве, но и во времени, когда зашифровываются и расшифровываются никуда не перемещающиеся файлы.

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это создает новую проблему распространения ключей. С другой стороны, получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать самостоятельно.

Ассимметричный метод шифрования

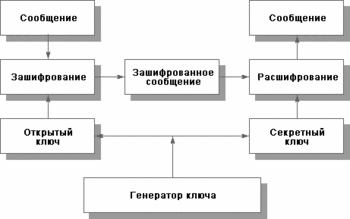


Рис. 2. Использование асимметричного метода шифрования

В асимметричных методах используются два ключа. Один из них, несекретный (он может публиковаться вместе с другими открытыми сведениями о пользователе), применяется для шифрования, другой (секретный, известный только получателю) - для расшифрования. Самым популярным из асимметричных является метод RSA (Райвест, Шамир, Адлеман), основанный на операциях с большими (скажем, 100-значными) простыми числами и их произведениями.

Проиллюстрируем использование асимметричного шифрования.

Существенным недостатком асимметричных методов шифрования является их низкое быстродействие, поэтому данные методы приходится сочетать с симметричными (асимметричные методы на 3–4 порядка медленнее). Так, для решения задачи эффективного шифрования с передачей секретного ключа, использованного отправителем, сообщение сначала симметрично зашифровывают случайным ключом, затем этот ключ зашифровывают открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети.

Рис.3 иллюстрирует эффективное шифрование, реализованное путем сочетания симметричного и асимметричного методов.



Рис.3 Эффективное шифрование сообщения

На рис.4 показано расшифрование эффективно зашифрованного сообщения.

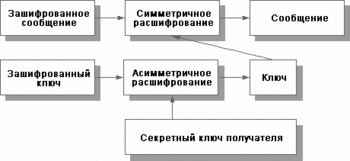


Рис.4 Расшифрование эффективно зашифрованного сообщения

Определенное распространение получила разновидность симметричного шифрования, основанная на использовании составных ключей. Идея состоит в том, что секретный ключ делится на две части, хранящиеся отдельно. Каждая часть сама по себе не позволяет выполнить расшифрование. Если у правоохранительных органов появляются подозрения относительно лица, использующего некоторый ключ, они могут в установленном порядке получить половинки ключа и дальше действовать обычным для симметричного расшифрования образом.

Порядок работы с составными ключами - хороший пример следования принципу разделения обязанностей. Он позволяет сочетать права на разного рода тайны (персональную, коммерческую) с возможностью эффективно следить за нарушителями закона, хотя, конечно, здесь очень много тонкостей и технического, и юридического плана.

Многие криптографические алгоритмы в качестве одного из параметров требуют псевдослучайное значение, в случае предсказуемости которого в алгоритме появляется уязвимость (подобное уязвимое место было обнаружено в некоторых вариантах Web-навигаторов). Генерация псевдослучайных последовательностей - важный аспект криптографии, на котором мы, однако, останавливаться не будем.

1. Шифр Виженера и его практическое применение

Шифр Виженера был очень популярен в 16 и 20 веке, в то время он считался очень сложным для расшифровки или же практически невозможным. В наше же время это один из самых ненадежных шифров. который используется крайне редко, чтобы зашифровать важные сообщения. Сейчас мы посмотрим на принцип его работы, и разберем пример шифрования.

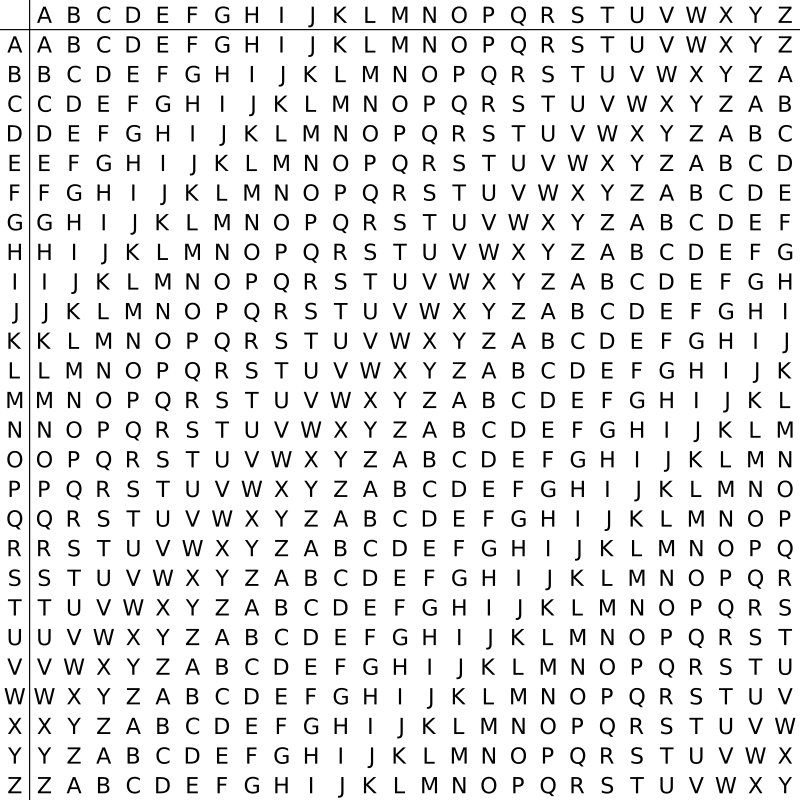


Рис. 5 Квадрат Виженера

На изображении представлен квадрат Виженера, он нам понадобится для шифрования нашего сообщения. Итак, для начала нам нужно использовать кодовое слово, с помощью которого мы зашифруем наше сообщение. Например, Star и само сообщение - сегодня будет дождь

Далее мы подставляем под каждую букву нашего сообщения, букву кодового слова, все буквы строго должны совпадать, иначе шифр может не получиться

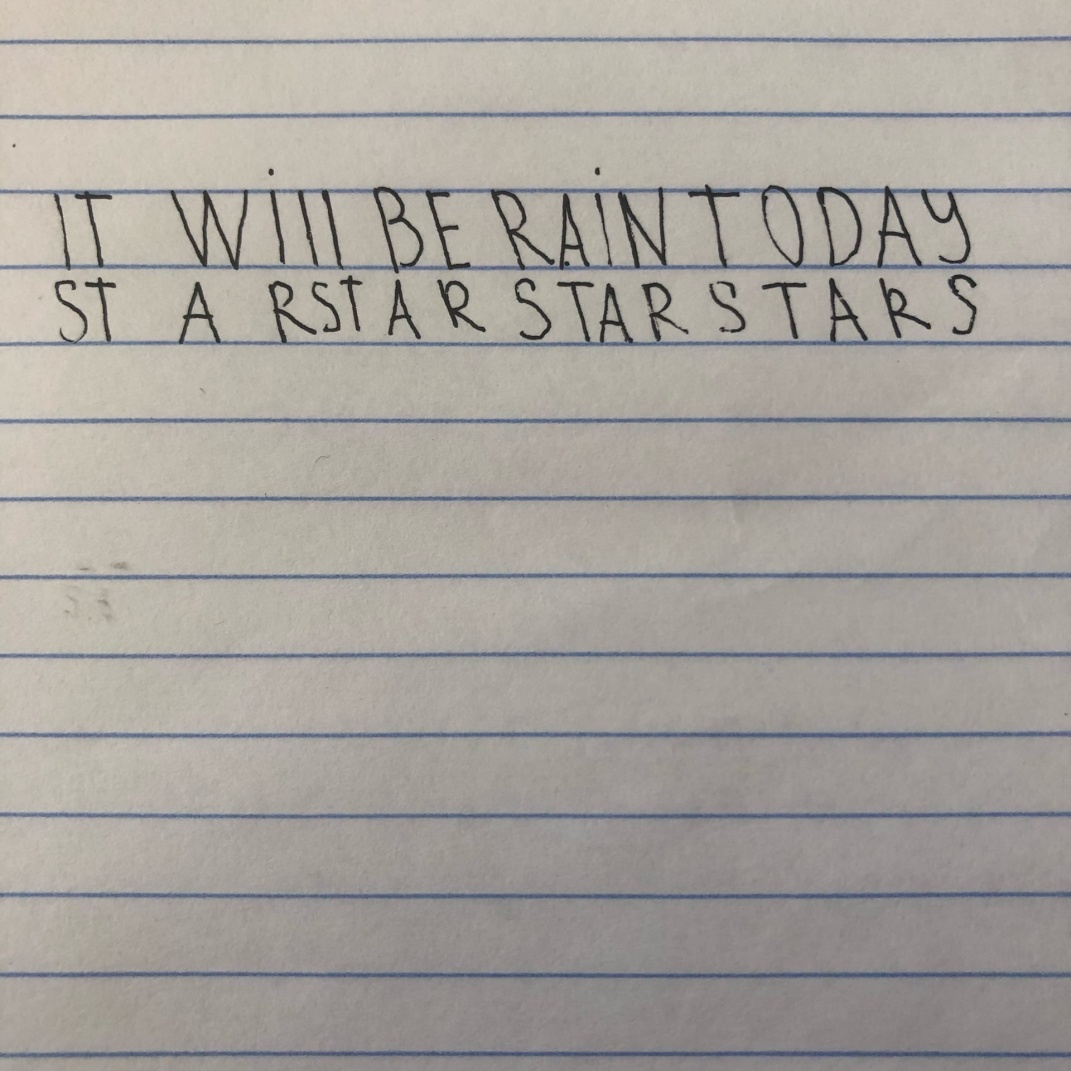
Запишите свое сообщение как показано ниже

Рис. 6 Исходное сообщение и пароль

Подставляем буквы кодового слова, пока не кончится сообщение

Далее нужно перейти к ряду первой буквы ключевого слова в квадрате Виженера и найти колонку с первой буквой нашего сообщения, далее нужно найти точку пересечения колонки и ряда, это и будет буквой нашего шифра. То есть, у нас первая буква будет А, это точка пересечения буквы I и буквы S. У нас получилось AMWZDEBVJTIELHDRQ

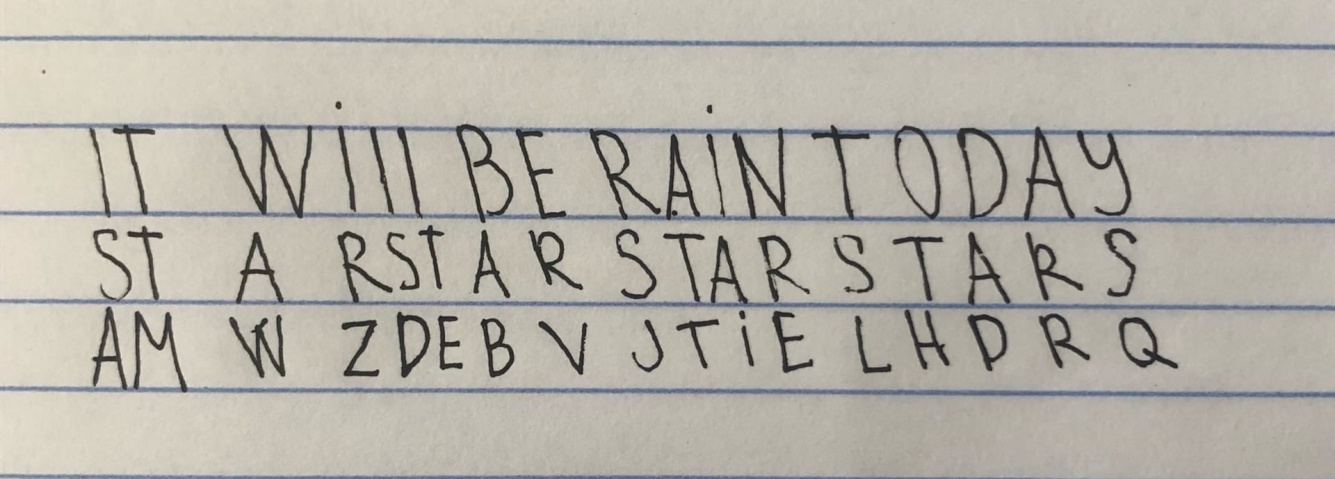


Рис. 7 Результат шифрования

# Заключение

Исходя из задач нашего исследования, мы пришли к следующим положениям:

Идея шифрования состоит в том, что злоумышленник, перехватив зашифрованные данные, и не имея к ним ключа, не может ни прочитать, ни изменить передаваемую информацию. Кроме того, в современных криптосистемах для шифрования, расшифрования данных могут использоваться разные ключи. Однако, с развитием криптоанализа, появились методики, позволяющие дешифровать закрытый текст без ключа. Они основаны на математическом анализе переданных данных.

Изученный в ходе практической части работы шифр Виженера – пример симметричного метода шифрования, который по мере развития техники перестал быть надежным

# Список литературы

1. А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин Основы Криптографии. - М.: Гелиос, 2005., с.5 - 53
2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. - М.: Горячая линия - Телеком, 2002., с. 4 - 8
3. Жельников В. Криптография от папируса до компьютера. - М.: ABF, 1996 - 756 с.
4. Ковалевский В., Криптографические методы. - СПб.: Компьютер Пресс, 1993 - 302 с.
5. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. ДМК. Москва, 2000 г.