Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»

Кафедра защиты информации

ШИФРОВАНИЕ И РАСШИФРОВАНИЕ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ШИФРА ЦЕЗАРЯ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к практическим занятиям по дисциплине
«Методология информационной безопасности»

для студентов специальности
1-98 01 02 «Защита информации в телекоммуникациях»

Минск 2021

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5
«ШИФРОВАНИЕ И РАСШИФРОВАНИЕ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ШИФРА ЦЕЗАРЯ»

Цель занятия: изучение способов криптографического преобразования информации и получения базовых практических навыков шифрования сообщений, а также криптоанализа шифротекста на примере шифра Цезаря.

1 Краткие теоретические сведения

Взаимодействие двух субъектов информационных отношений обеспечивается посредством телекоммуникаций, поэтому передача сообщений от одного субъекта к другому реализуется по каналу связи. **Телекоммуникации** (от греческого теле – далеко, от латинского комуникато - общение) - комплекс технических средств, предназначенных для передачи информации на большое расстояние.

Для организации процесса перехвата информации, передаваемой по каналу связи, необходимо иметь доступ к физической среде передачи информации. В качестве такой среды выступают электрические и оптические кабели связи, воздушная среда. Процесс несанкционированного получения информации из канала связи называется **перехватом информации** (рисунок 1).

Рисунок 1. – Схематичное изображение перехвата информации в канале связи

Ввиду того, что канал связи имеет значительную протяженность - обеспечить контроль физического доступа к нему является сложной организационно-технической проблемой. Поэтому для обеспечения безопасности информации передаваемой по каналам связи необходимо решить ряд задач:

1. Обеспечить ее конфиденциальность;
2. Обеспечить ее целостность;

3. Обеспечить ее подлинность.

4. Усложнить анализ потока сообщений.

Для решения таких задач используют криптографические методы защиты информации.

Криптография (от греческого криптос – скрытый, графо - пишу) – наука о методах, алгоритмах, программных и аппаратных средствах преобразования информации в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования.

Информация, передаваемая по каналу связи и подлежащая шифрованию - называется **открытым (исходным) текстом** (обозначается M от английского message), а криптографически преобразованная информация называется **шифротекстом** (обозначается C от английского ciphertext). Криптографическое преобразование открытого текста в шифротекст реализуется по некоторому алгоритму. Отправитель выполняет криптографическое преобразование (шифрование) открытого текста и формирует, таким образом, шифротекст передавая его в канал связи, а получатель выполняет обратное криптографическое преобразование шифротекста (расшифрование) в открытый текст. Система, в которой осуществляется шифрование и расшифрование информации называется **криптосистемой** или **шифром**.

Нарушитель, получив доступ к физической среде передачи информации, перехватит шифротекст и будет выполнять его расшифрование для получения открытого текста. Расшифрование шифротекста будет успешным при условии, что нарушитель знает шифр. Для противодействия нарушителю при шифровании сообщений используется некоторый секрет, который называется криптографическим ключом. **Криптографический ключ** (обозначается K от английского Key) – информация, хранимая в секрете и используемая в криптосистемах. Стойкость любой криптографической системы определяется стойкостью используемого криптографического ключа. Необходимо выбрать не только его соответствующую длину, но и обеспечить режим секретности при его хранении и применении.

Исходя из особенностей применения криптографического ключа криптосистемы делят на симметричные и ассиметричные. В симметричных криптосистемах для шифрования и расшифрования сообщений используют один и тот же криптографический ключ (рисунок 2).

В криптографических системах одной из проблем является обмен криптографическими ключами между отправителем и получателем сообщений, для которого нельзя использовать канал связи, так как в канале связи всегда

ведется перехват сообщений. Ключ может быть передан только при личном контакте отправителя и получателя сообщений.

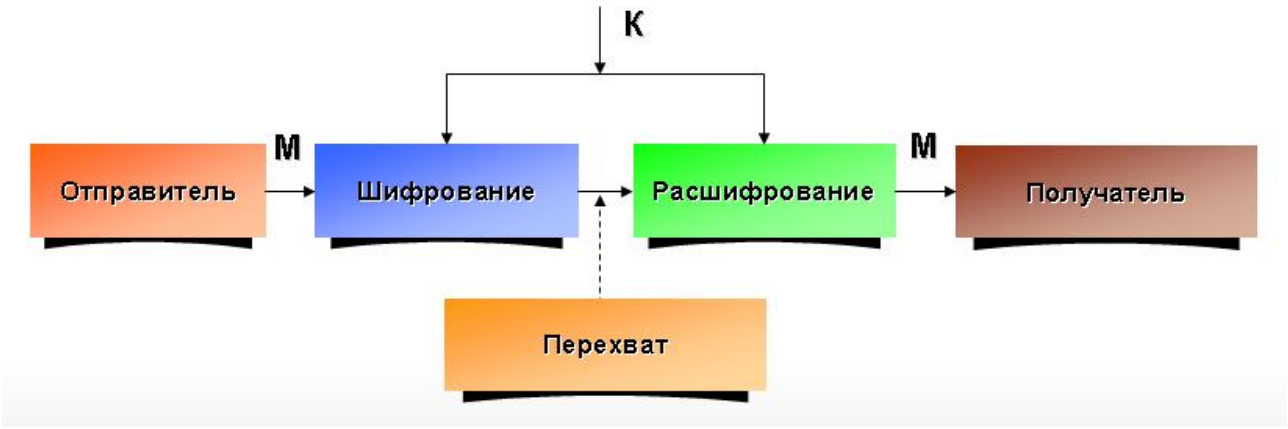

Рисунок 2. – Схематичное изображение симметричной криптосистемы

В ассиметричных криптосистемах (криптосистемах с открытым ключом) для шифрования сообщений (рисунок 3) используется один криптографический ключ (К1), а для расшифрования – другой (К2). Такой подход упрощает процедуру обмена криптографическими ключами, так как отправитель информации получает ключ для его шифрования (К1) от получателя по каналу связи, по которому впоследствии будет передавать шифротекст. Передача криптографического ключа по каналу связи становится возможной, так как этот ключ позволяет только шифровать сообщение. Второй криптографический ключ (К2) используется получателем информации только для ее расшифрования и по каналу связи не передается.

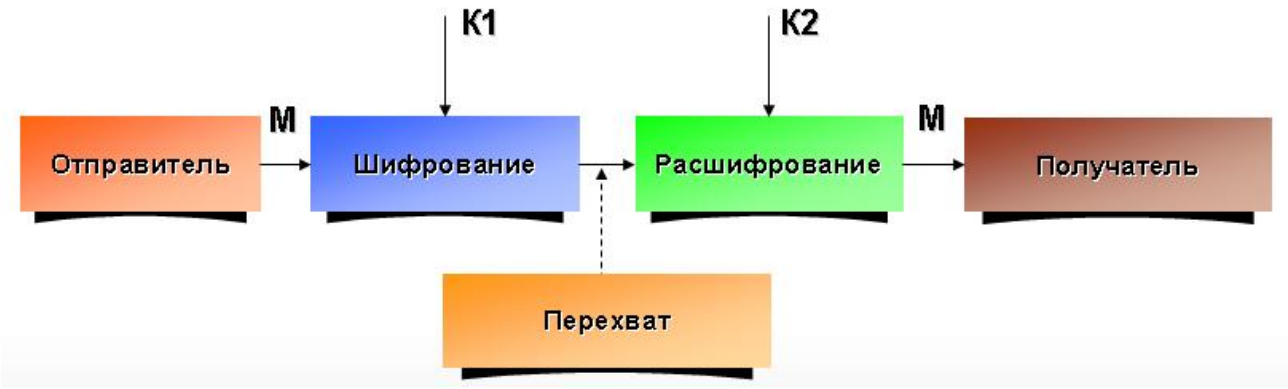

Рисунок 3. – Схематичное изображение асимметричной криптосистемы

В телекоммуникационных системах используют линейное (канальное) и абонентское шифрование информации. При линейном шифровании информации абонент (отправитель информации) формирует открытый текст и

передает его на узел связи, где шифровальная аппаратура (аппаратно-программный комплекс для шифрования и расшифрования информации) выполняет криптографическое преобразование сообщения и передает шифротекст в канал связи. На приемном узле связи шифровальная аппаратура получает шифротекст и выполняет его расшифрование. При этом используются поточные шифры, и между узлами связи поддерживается постоянный поток шифротекста, непрерывность которого обеспечивается передачей пустых (незначащих) сообщений, что затрудняет нарушителю вести анализ потока сообщений. При таком способе связи нарушитель, для того, чтобы получить открытый текст будет вынужден получить доступ к узлу связи, так как на нем обрабатываются сообщения в открытом виде. Поэтому оба узла связи должны быть защищены от несанкционированного доступа.

Практическая реализация абонентского шифрования предполагает, что каждое сообщение шифруется в его источнике и расшифровывается только получателем. Сообщение, зашифрованное отправителем, может еще подвергаться и линейному шифрованию. Таким образом, абонентское шифрование обеспечивает конфиденциальность передаваемого сообщения, линейное – конфиденциальность и защиту сообщений от анализа. Успешный анализ шифротекста может привести к раскрытию криптографического ключа или получению открытого текста без знания криптографического ключа.

При абонентском шифровании за счет использования соответствующих режимов функционирования криптосистемы, попутно, решается и задача контроля целостности сообщения, а также проверки подлинности сообщения и его источника.

Шифр Цезаря - одна из самых простых и наиболее известных криптосистем, которая относится к шифрам подстановки. В этой криптосистеме каждый символ открытого текста заменяется символом, находящимся на некотором постоянном числе позиций левее или правее в алфавите заменяемого символа открытого текста. Число, которое характеризующее количество позиций сдвига влево или вправо по алфавиту относительно позиции преобразуемого символа открытого текста является криптографическим ключом и определяется выражением: n-1 (где n – число символов в алфавите).

Поэтому для шифрования информации необходимо иметь кроме открытого текста еще и алфавит. Рассмотрим пример шифрования сообщения, используя алфавит, изображенный на рисунке 4.

Зашифруем сообщение в качестве, которого используем слово «криптография». Для упрощения процедуры шифрования используем ключ К=10. Так как мы шифруем сообщение, то сдвиг будем выполнять вправо.

Первая буква в шифруемом сообщении «К». Для удобства шифрования буквы в алфавите пронумерованы. Порядковый номер буквы «К» - 12. Так как сдвиг выполняется вправо, то прибавим к числу 12 ключ 10. Получим число – 22. Ему соответствует буква «Ф». Исходя из чего первая буква шифротекста – «Ф». Преобразование всех остальных букв сообщения выполняется аналогично. В итоге получится шифротекст «фътщьшмъйюти».

1. А	2. Б	3.В	4. Г	5. Д	6. Е	7. Ё	8.Ж	9. З	10.И	11.Й
12.К	13.Л	14.М	15.Н	16.О	17.П	18.Р	19.С	20.Т	21.У	22.Ф
23.Х	24.Ц	25.Ч	26.Ш	27.Щ	28.Ъ	29.Ы	30.Ь	31.Э	32.Ю	33.Я

Рисунок 4. – Алфавит

Для расшифрования шифротекста необходимо выполнить обратное его преобразование. Первая буква в шифротексте «Ф». Ее порядковый номер – 22. Зная ключ, необходимо от 22 вычесть значение криптографического ключа 10. Получим 12 и соответственно букву «К».

Наука о раскрытии открытого текста зашифрованного сообщения без доступа к криптографическому ключу называется **криптоанализом**.

Понимая шифр Цезаря можно выполнить криптоанализ шифротекста и не зная криптографический ключ его вычислить, а потом расшифровать весь шифротекст. Такую процедуру можно выполнить следующим образом. Необходимо взять шифротекст, например «Уё йзфцк шцёзё Уё шцёзк йцфзё» и из него выбрать слово длиной порядка 5 букв. Перебирая все возможные значения криптографических ключей можно определить тот, при котором слово будет осмысленным.

Возьмем слово из шифротекста «йзфцк»:

Ключ 1 – ижухй;

Ключ 2 – зётфи;

Ключ 3 – жесуз;

Ключ 4 – ёдртж;

Ключ 5 – егпсё;

Ключ 6 – дворе.

При криптографическом ключе равном 6 мы получили слово «дворе». Криптографический люч вычислен, можно расшифровать весь шифротекст.

«Уё йзфцк шцёзё Уё шцёзк йцфзё» - «На дворе трава На траве дрова».

Существуют и другие способы криптоанализа шифра Цезаря.

2 Практическое задание

1. Зашифровать сообщение в соответствии с индивидуальным заданием.
2. Расшифровать сообщение в соответствии с индивидуальным заданием.

3 Контрольные вопросы

1. Что называется перехватом информации?
2. Какое условие необходимо выполнить для организации процесса перехвата информации?
3. Какое наименование носите прямое и обратное криптографическое преобразование информации.
4. В чем особенности симметричной и ассиметричной криптосистем?
5. Как противодействуют анализу потока сообщений?