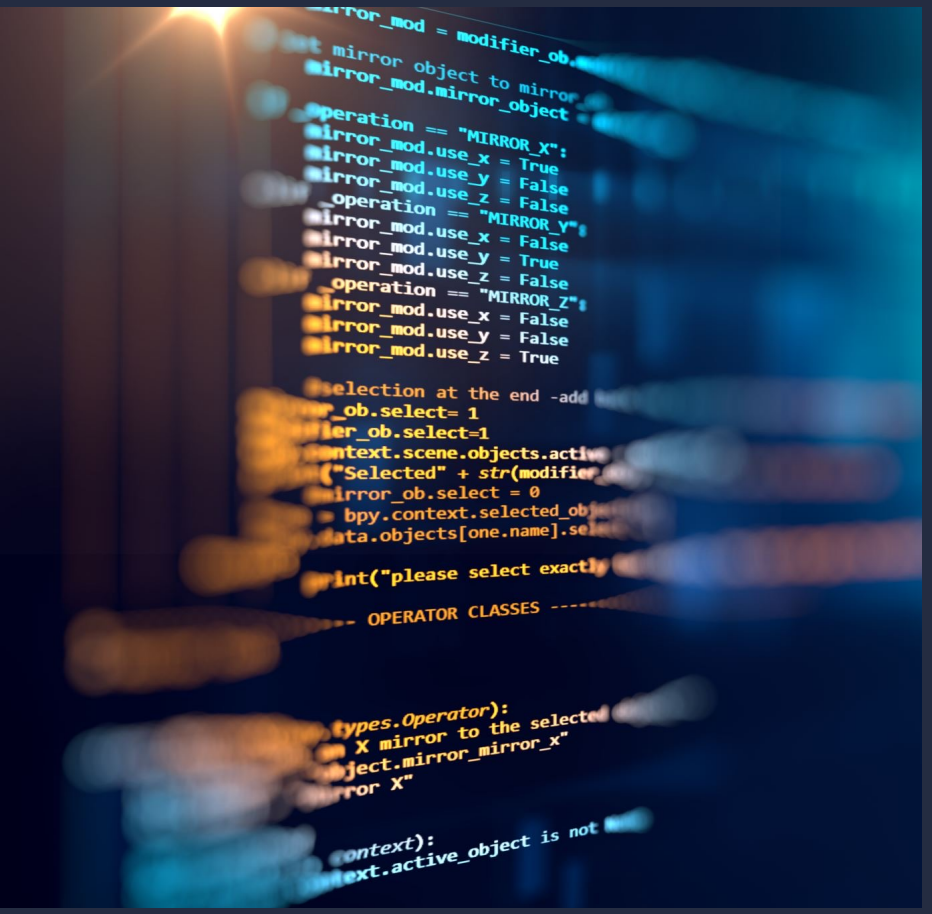


КРИПТОГРАФИЯ

Зачем нужна криптография?

Как передать нужную информацию нужному адресату в тайне от других?

- Создать абсолютно надежный, недоступный для других канал связи между абонентами.
- Использовать общедоступный канал связи, но скрыть сам факт передачи информации.
- Использовать общедоступный канал связи, но передавать по нему информацию в преобразованном виде, чтобы восстановить ее мог только адресат.

Что такое криптография?

Криптография («криптос» - тайна, «графэйн» - писать) - наука о методах обеспечения конфиденциальности и аутентичности информации

- конфиденциальность *(*невозможности прочтения информации посторонним*)*
- аутентичность *(*целостности и подлинности авторства*,* а также невозможности отказа от авторства*)*

Основные термины, используемые в криптографии

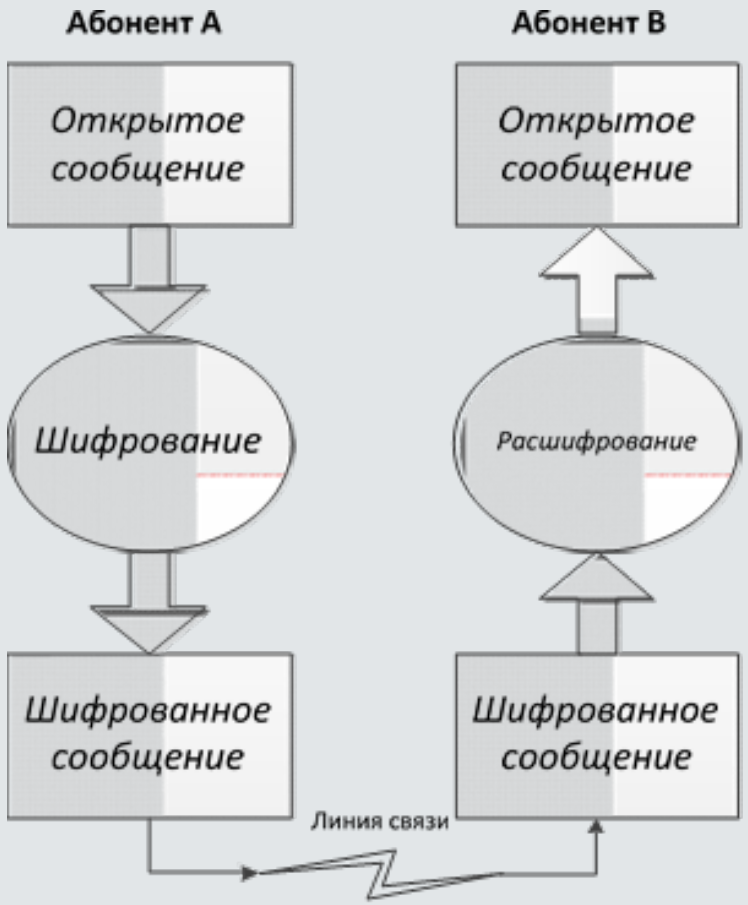
Сообщение, которое передается адресату, называется **открытым сообщением**.

Преобразованное криптографическими методами сообщение называется **шифрованным сообщением**, или **шифртекстом**.

Процесс преобразования открытого сообщения в шифрованное называется **шифрованием**, или **зашифрованием**.

Процесс преобразования шифртекста абонентом-получателем в открытое сообщение называется **расшифрованием** (не следует данный термин путать с термином «дешифрование»)

Дешифрование - получение открытых данных по зашифрованным в условиях, когда алгоритм расшифрования и его секретные параметры не являются полностью известными и расшифрование не может быть выполнено обычным путем


Абонент А
Абонент В
Открытое сообщение
Открытое сообщение
Шифрование
Расшифрование
Шифрованное сообщение
Шифрованное сообщение
Линия связи

Формализуем математически процесс зашифрования и расшифрования

Для этого введем следующие обозначения:

X - открытое сообщение,

Y - шифрованное сообщение,

f - правило шифрования (функция, определенная на множестве всех открытых текстов),

g - правило расшифрования (функция, определенная на множестве всех шифртекстов).

Зашифрование X в Y можно записать в виде

$f(X) = Y$.

Обратное преобразование (то есть получение открытого сообщения X п утем расшифрования Y) запишется в виде соотношения

$g(Y) = X$.

Ключ

Ключ — это секретная информация, используемая криптографическим алгоритмом при зашифровании/расшифровании сообщений. При использовании одного и того же алгоритма результат шифрования зависит от ключа.

Используя понятие ключа, процесс зашифрования можно описать в виде соотношения:

$$f_k(X) = Y$$

в котором k - выбранный ключ, известный отправителю и адресату.

Криптоанализ

Криптоанализ – наука о преодолении криптографической защиты информации. **Криптоаналитики** исследуют возможности расшифровывания информации без знания ключей. Успешно проведенный *криптоанализ* позволяет получить *ключ шифрования*, или *открытый текст*, или то и другое вместе.

Криптология

Иногда криптографию и *криптоанализ* объединяют в одну науку – **криптологию** (kryptos - тайный, logos - наука), занимающуюся вопросами обратимого преобразования информации с целью защиты от несанкционированного доступа, оценкой надежности систем шифрования и анализом стойкости шифров.

В настоящее время *криптография* прочно вошла в нашу жизнь. Перечислим лишь некоторые сферы применения криптографии в современном информатизированном обществе:

- ✓ шифрование данных при передаче по открытым каналам связи (например, при совершении покупки в Интернете сведения о сделке, такие как адрес, телефон, номер кредитной карты, обычно зашифровываются в целях безопасности);
- ✓ обслуживание банковских пластиковых карт;
- ✓ хранение и обработка паролей пользователей в сети;
- ✓ сдача бухгалтерских и иных отчетов через удаленные каналы связи;
- ✓ банковское обслуживание предприятий через локальную или глобальную сеть;
- ✓ безопасное от несанкционированного доступа хранение данных на жестком диске компьютера (в операционной системе Windows даже имеется специальный термин – шифрованная файловая система (EFS)).