2.3. Классификация криптоалгоритмов и типы криптоатак

В отношении криптоалгоритмов существует несколько схем классификации, каждая из которых основана на группе характерных признаков. Таким образом, один и тот же алгоритм "проходит" сразу по нескольким схемам, оказываясь в каждой из них в какой-либо из подгрупп.

Основной схемой классификации всех криптоалгоритмов является следующая:

- Тайнопись.

Отправитель и получатель производят над сообщением преобразования, известные только им двоим. Сторонним лицам неизвестен сам алгоритм шифрования. Некоторые специалисты считают, что тайнопись не является криптографией вообще, и автор находит это совершенно справедливым.

- Криптография с ключом.

Алгоритм воздействия на передаваемые данные известен всем сторонним лицам, но он зависит от некоторого параметра – "ключа", которым обладают только отправитель и получатель.

Симметричные криптоалгоритмы

Для зашифровки и расшифровки сообщения используется один и тот же блок информации (ключ).

Асимметричные криптоалгоритмы

Алгоритм таков, что для зашифровки сообщения используется один ("открытый") ключ, известный всем желающим, а для расшифровки – другой ("закрытый"), существующий только у получателя.

В зависимости от *характера воздействий*, производимых над данными, алгоритмы подразделяются на:

1. Перестановочные
   Блоки информации (байты, биты, более крупные единицы) не изменяются сами по себе, но изменяется их порядок следования, что делает информацию недоступной стороннему наблюдателю.
2. Подстановочные
   Сами блоки информации изменяются по законам криптоалгоритма. Подавляющее большинство современных алгоритмов принадлежит этой группе.

В зависимости от размера блока информации криптоалгоритмы делятся на:

1. *Потоковые шифры*.

Единицей кодирования является один бит. Результат кодирования не зависит от прошедшего ранее входного потока. Наиболее распространенными представителями поточных шифров являются *скремблеры*.

2. *Блочные шифры*.

Единицей кодирования является блок из нескольких байтов (в настоящее время 4-32). Результат кодирования зависит от всех исходных байтов этого

блока. Схема применяется при пакетной передаче информации и кодировании файлов.

Существует четыре основных типа криптоаналитических атак. Конечно, все они формулируются в предположении, что криптоаналитику известны применяемый алгоритм шифрования и шифртексты сообщений.

1. Криптоаналитическая атака при наличии только известного шифртекста.
2. Криптоаналитическая атака при наличии известного открытого текста.
3. Криптоаналитическая атака при возможности выбора открытого текста.
4. Криптоаналитическая атака с адаптивным выбором открытого текста.

Кроме перечисленных основных типов криптоаналитических атак, можно отметить, по крайней мере, еще два типа.

5. Криптоаналитическая атака с использованием выбранного шифртекста.
6. Криптоаналитическая атака методом полного перебора всех возможных ключей.