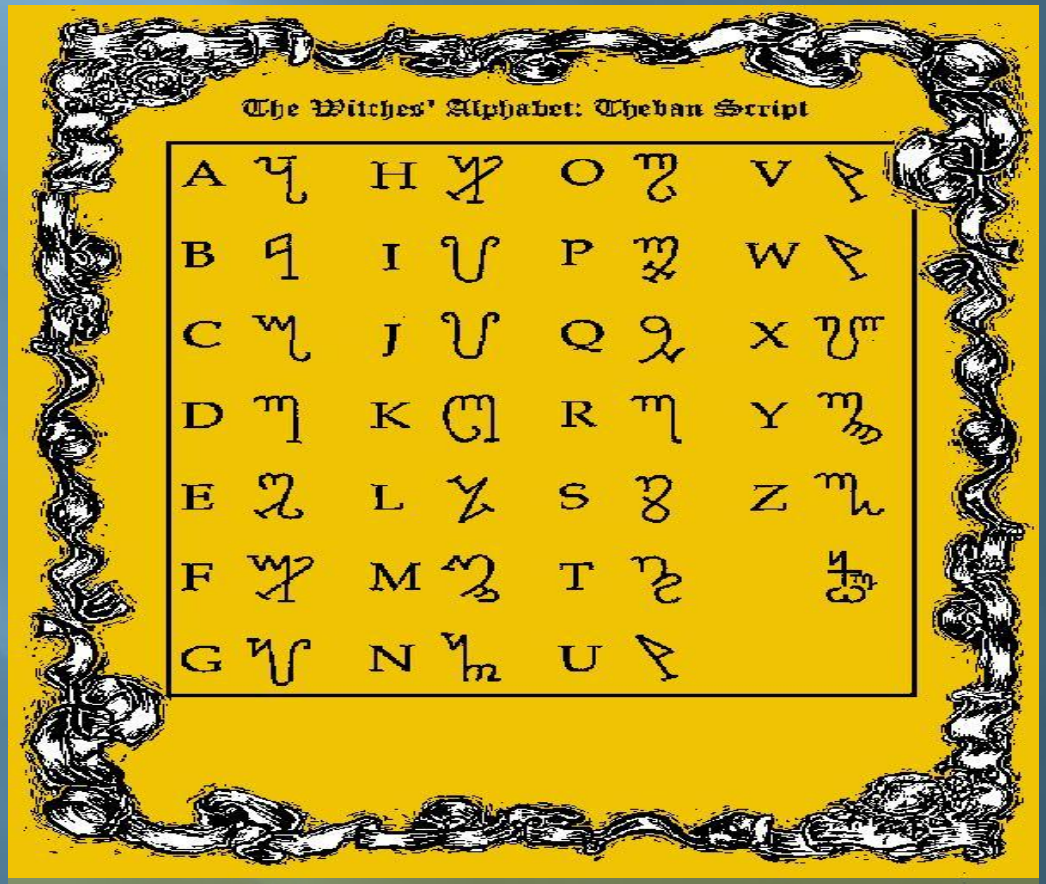
ШИФРЫ И ИХ ОСНОВНЫЕ ТРЕБОВАНИЯ



Криптография

Криптография - это область знаний, относящаяся к средствам и методам преобразования сообщений в непонятную для посторонних форму, а также к средствам и методам проверки подлинности сообщений.

Цель криптографии:

сделать понятное (т.е. "открытое") сообщение всецело непонятным (т.е. "закрытым") для непосвященного. Подобный трюк осуществляется при помощи кодирования и шифрования, а то, что получается в итоге - зовется криптограммой.

Шифрование – процесс применения шифра к защищаемой информации, т.е. преобразование открытого текста в шифрованное сообщение (шифротекст, криптограмму) с помощью определенных правил (ключей), содержащихся в шифре.

Шифр - разновидность кодирования секретной информации для безопасной передачи по открытым каналам, в целях исключения нежелательного ее получения или изменения третьими лицами. В состав шифра входят алгоритмы шифрования и дешифрования.

Все шифры различают, прежде всего, на шифры замены, шифры перестановки и композиционные шифры. Классификация шифров:

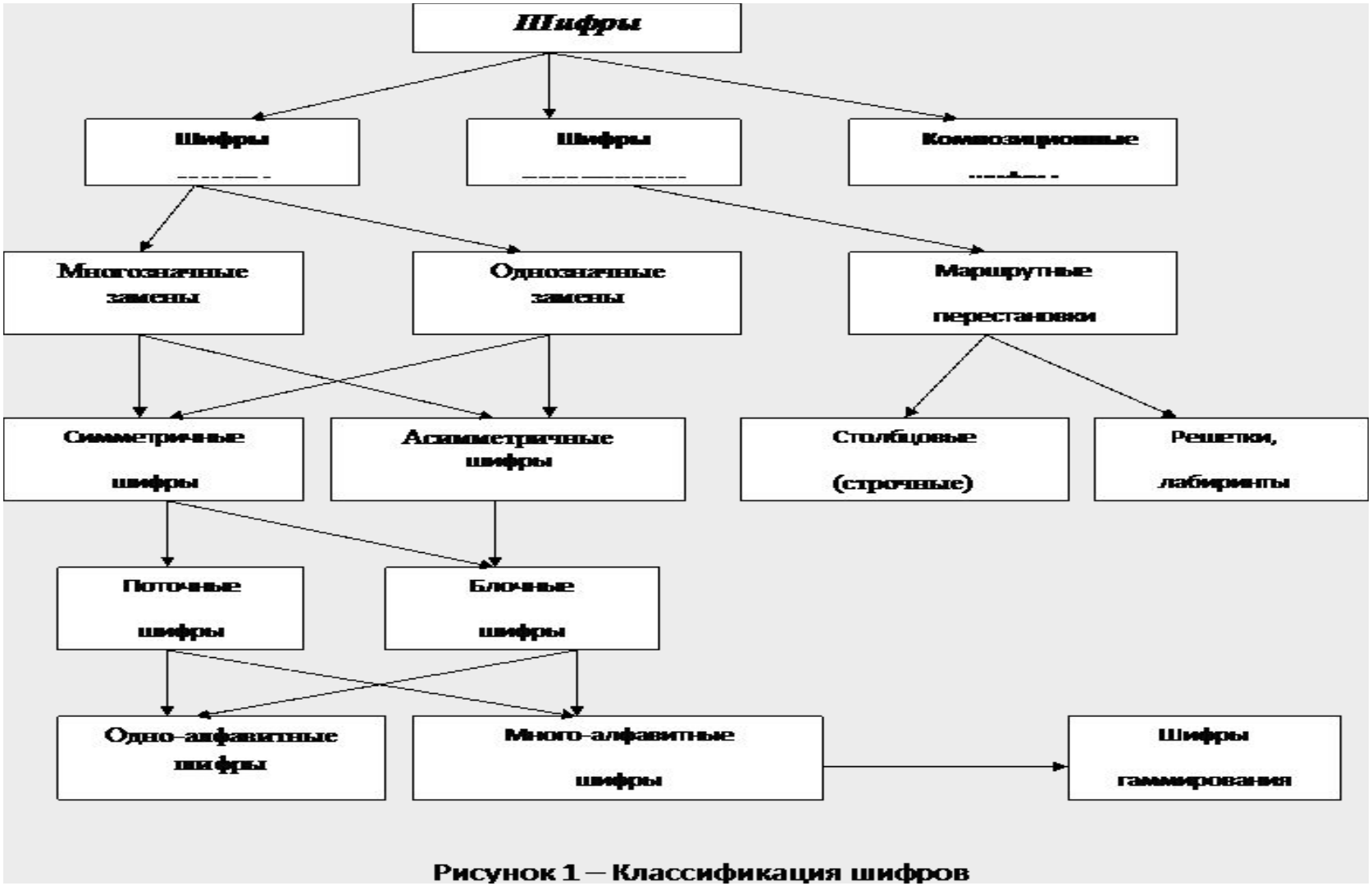
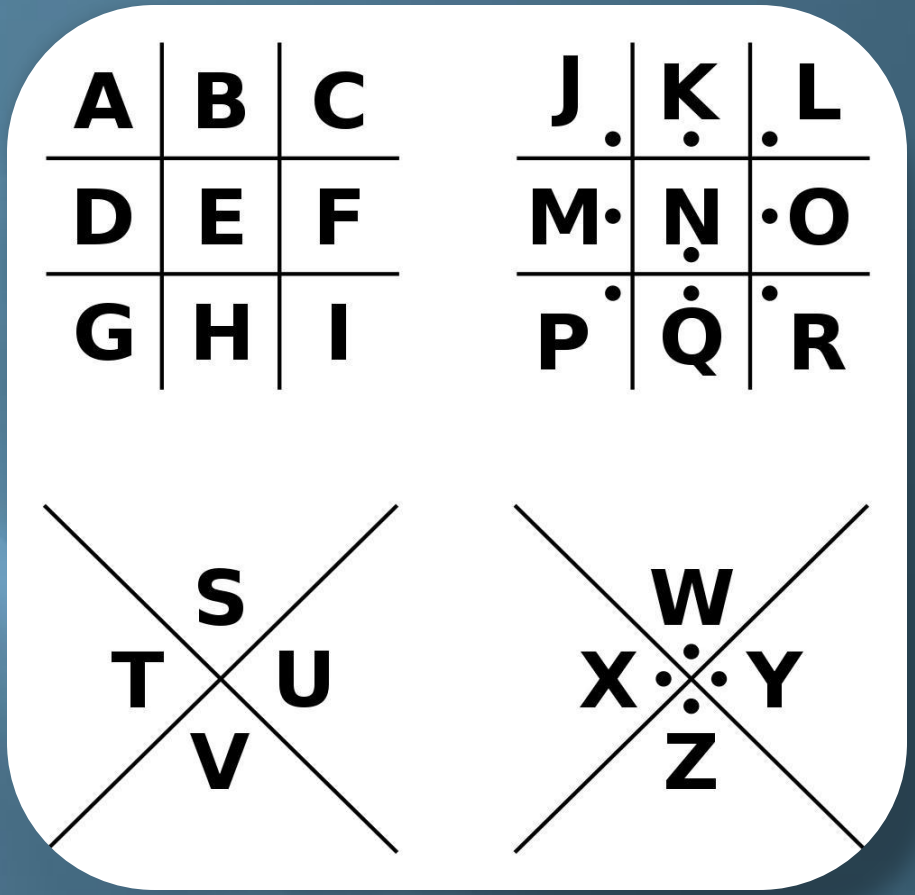


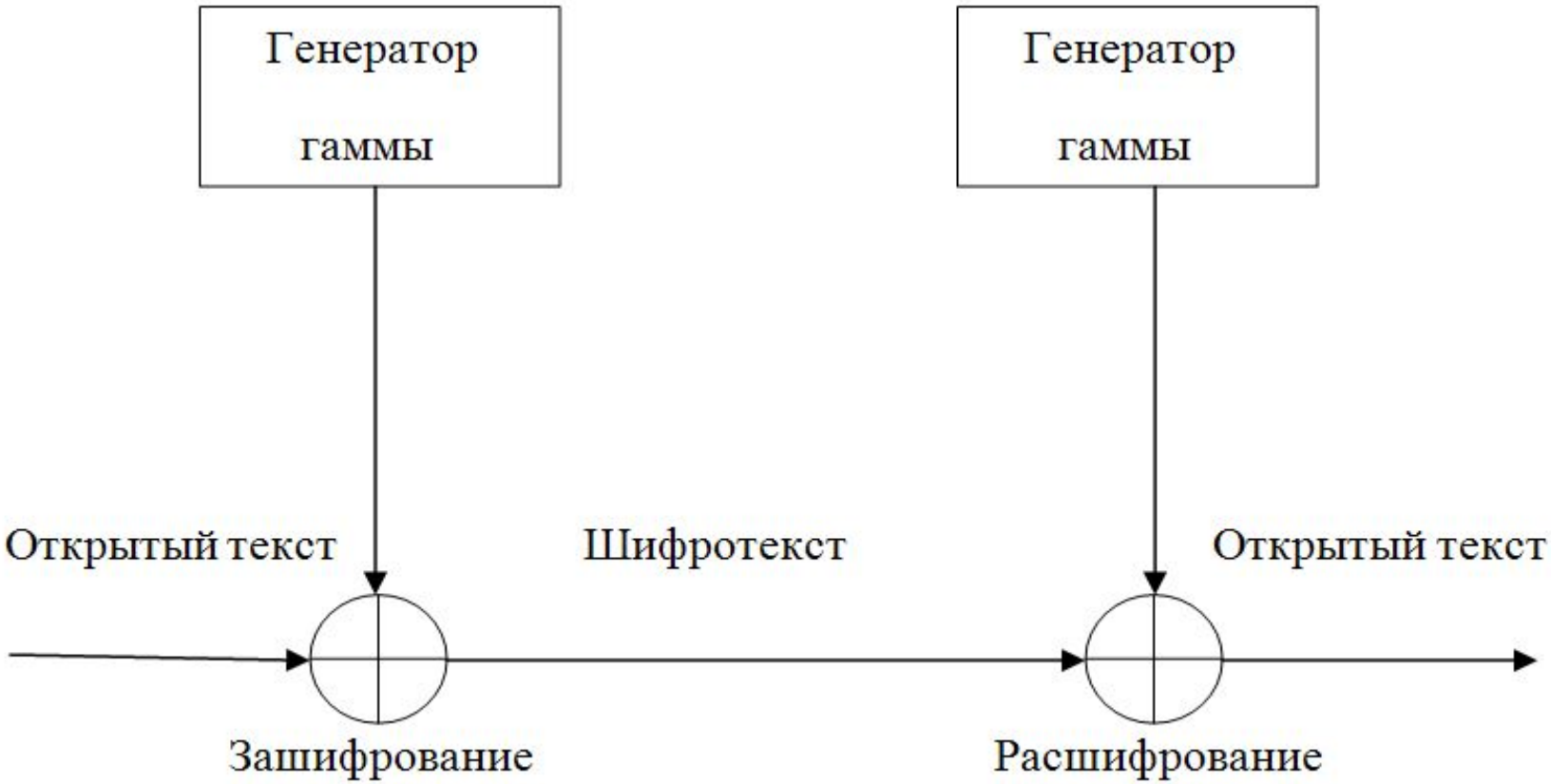
Рисунок 1 – Классификация шифров

Шифр замены – это шифр, в котором фрагменты открытого текста заменяются некоторыми их эквивалентами в шифротексте.

Если ключ шифрования совпадает с ключом расшифровывания, то такие шифры называют симметричными, если же ключи различны, то такие шифры называют асимметричными.



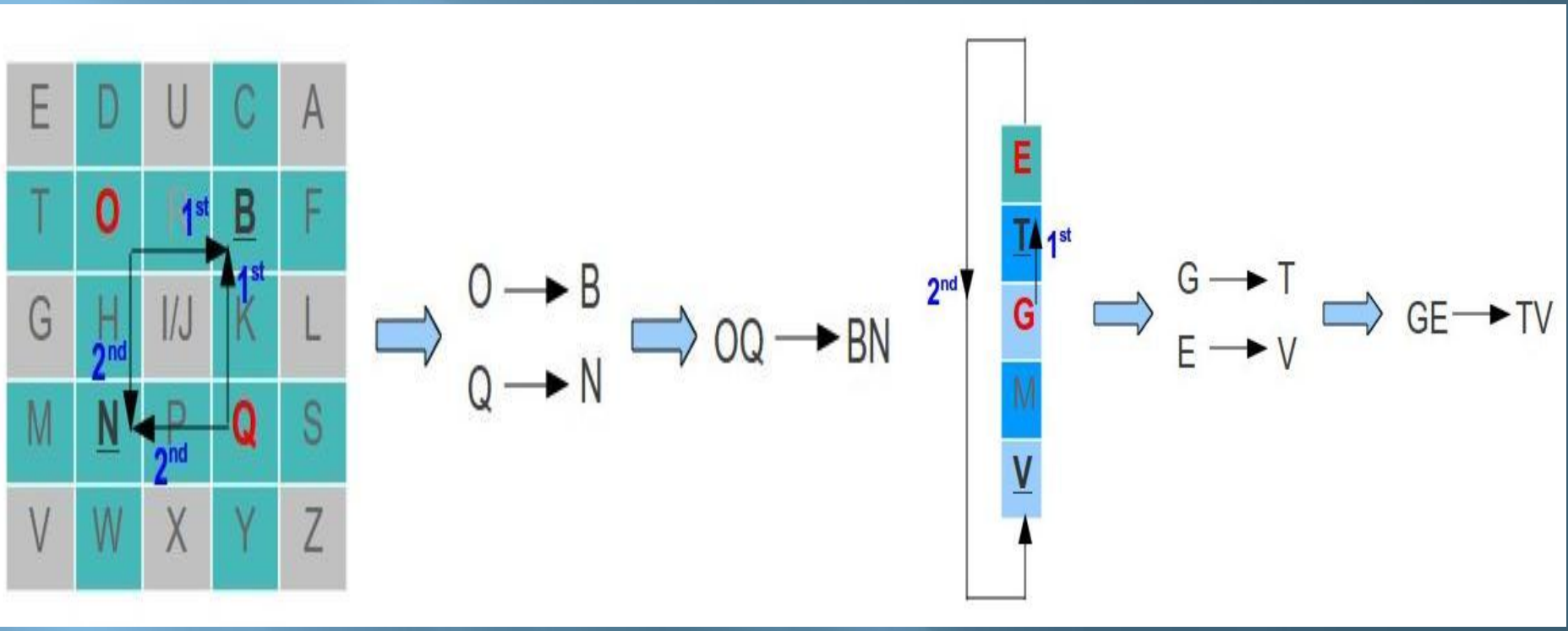
Метод шифрования масонов



Шифр гаммирования - пример шифра однозначной замены со случайной равновероятной гаммой (гаммой принято называть последовательность чисел $k_1 \ldots k_n$, складываемую по модулю с шифруемым сообщением).

Шифр перестановки – это шифр преобразования из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих (буквы открытого текста при шифровании лишь меняются местами друг с другом). Ключом шифра является перестановка номеров букв открытого текста.

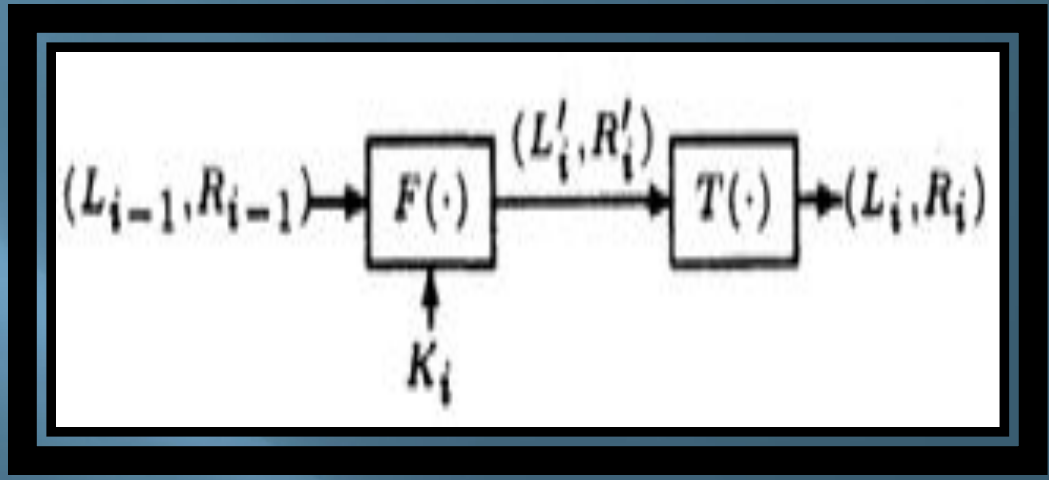
Шифр перестановки "скитала"



Шифр Плейфера

Одной из разновидностей шифров простой замены являются *блочные шифры*. Простейший блочный шифр оперирует с биграммными шифровеличинами. Одним из первых таких шифров был биграммный шифр Порта и Плейфера.

Композиционный шифр – это всевозможные композиции различных шифров. То есть, с целью повышения надежности шифрования шифрованный текст, полученный применением некоторого шифра, может быть еще раз зашифрован с помощью другого шифра.



Основные требования к криптографическим системам

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений)
- знание алгоритма шифрования не должно влиять на надежность защиты
- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при шифровании одного и того же исходного текста
- незначительное изменение исходного текста должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа
- структурные элементы алгоритма шифрования должны быть неизменными
- дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте
- длина шифрованного текста должна быть равной длине исходного текста
- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования
- любой ключ из множества возможных должен обеспечивать надежную защиту информации
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования

Заключение

Широкое применение компьютерных технологий и постоянное увеличение объема информационных потоков вызывает постоянный рост интереса к криптографии. Криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности. Например, для портативных компьютеров, физически защитить которые крайне трудно, только криптография позволяет гарантировать конфиденциальность информации даже в случае кражи.