# ***«Стандарты современной криптографии в РФ»***

### ГОСТ Р 34.10-2012: Электронная цифровая подпись

### Стандарт ГОСТ Р 34.10-2012 регулирует процессы формирования и проверки электронной цифровой подписи (ЭЦП) с использованием асимметричного криптографического алгоритма, а также функции хэширования. ЭЦП играет ключевую роль в обеспечении аутентичности и целостности передаваемых данных в условиях незащищённых каналов связи.

**Принцип работы:**

1. **Формирование подписи:** Для создания подписи используется закрытый ключ подписанта, который применяется к хэш-сумме сообщения, полученной с помощью хэш-функции ГОСТ Р 34.11-2012.
2. **Проверка подписи:** Получатель сообщения использует открытый ключ отправителя для проверки подписанного хэш-кода и сопоставления его с хэш-суммой, вычисленной из принятого сообщения.

ЭЦП используется в различных системах, таких как электронный документооборот, для подтверждения подлинности электронных документов.

### ГОСТ Р 34.11-2012: Хеш-функция «Стрибог»

Стандарт ГОСТ Р 34.11-2012 описывает хеш-функцию «Стрибог», предназначенную для создания хеш-кодов с длиной 256 и 512 бит. Она обеспечивает целостность данных, позволяя выявлять любые изменения в передаваемом сообщении.

**Особенности алгоритма:**

1. **Стойкость к атакам:** «Стрибог» учитывает современные требования по стойкости хеш-функций, включая защиту от коллизий и обратных атак.
2. **Процесс хеширования:** Алгоритм обрабатывает данные блоками и использует операцию итерации для создания финального хэш-кода.

«Стрибог» широко используется в криптографических протоколах и системах защиты информации, включая сертификационные и банковские системы.

### ГОСТ Р 34.12-2015: Блочные шифры «Магма» и «Кузнечик»

ГОСТ Р 34.12-2015 регламентирует два блочных шифра — «Магма» и «Кузнечик», которые обеспечивают симметричное шифрование данных. Эти шифры используют различные размеры блоков и ключей, что позволяет выбирать оптимальные параметры в зависимости от задач и уровня требуемой безопасности.

**Магма:**

1. Работает с 64-битными блоками данных и 256-битным ключом.
2. Основные операции включают замены, перестановки и циклические сдвиги, обеспечивающие высокий уровень криптографической стойкости.

**Кузнечик:**

1. Использует 128-битные блоки и также 256-битный ключ, что значительно увеличивает уровень безопасности по сравнению с «Магмой».
2. Применяется для защиты данных, где требуется более высокая степень устойчивости к криптоанализу.

Эти шифры применяются для защиты как государственных, так и коммерческих данных, включая защиту информации в государственном и банковском секторах.

### ГОСТ Р 34.13-2015: Режимы работы блочных шифров

ГОСТ Р 34.13-2015 описывает различные режимы работы блочных шифров, которые определяют способ шифрования данных в зависимости от выбранного алгоритма. Среди наиболее известных режимов — режимы простой замены, гаммирования и другие.

**Основные режимы:**

1. **Режим простой замены:** Применяется для шифрования отдельных блоков данных, где каждый блок шифруется независимо.
2. **Режим гаммирования:** Включает использование ключевого потока (гаммы), который комбинируется с исходными данными для их шифрования, что позволяет обеспечить высокую скорость шифрования и безопасность при обработке больших объёмов данных.

Выбор режима работы оказывает влияние на общую безопасность системы, её устойчивость к атакам, а также на эффективность обработки данных. Эти режимы предоставляют гибкость при разработке криптографических систем и протоколо