ГБПОУ Колледж Автоматизации Информационных Технологий №20

ГОСТ Р 34.11-94 - Информационная технология. Криптографическая защита информации. Функция хеширования

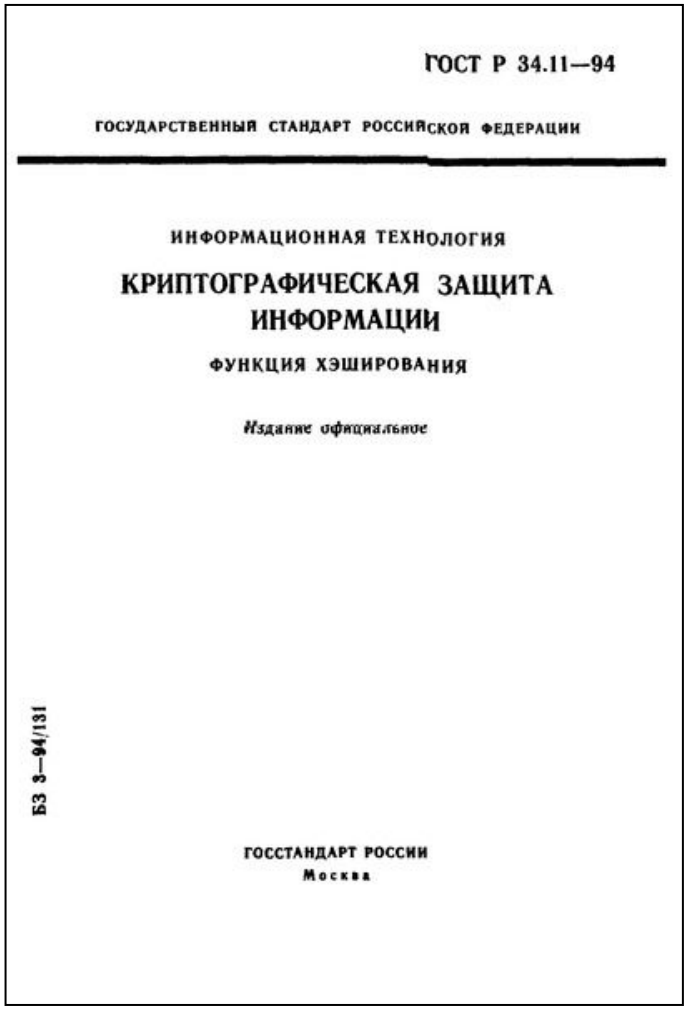
Выполнили:
Студенты группы 3ОТЗИ1
Абовян Владислав Евгеньевич
Мелихова Екатерина Григорьевна

Содержание

ГОСТ Р 34.11-94 - устаревший российский криптографический стандарт вычисления хеш-функции.

Дата отмены:	• 1 января 2013 года
Дата введения:	• 23 мая 1994 года
Размер хеша:	• 256 бит
Размер блока входных данных:	• 256 бит
Разработчик:	• ГУБС ФАПСИ и Всероссийский научно-исследовательский институт стандартизации

Стандарт определяет алгоритм и процедуру вычисления хеш-функции для последовательности символов. Этот стандарт является обязательным для применения в качестве алгоритма хеширования в государственных организациях РФ и ряде коммерческих организаций.



ГОСТ Р 34.11—94

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ФУНКЦИЯ ХЭШИРОВАНИЯ

Издание официальное

БЗ 3—94/131

ГОССТАНДАРТ РОССИИ
Москва

До 2013 г. ЦБ РФ требовал использовать ГОСТ Р 34.11-94 для электронной подписи предоставляемых ему документов.

С 1 января 2013 года заменён на ГОСТ Р 34.11-2012 «Стрибог».

Характеристика	ГОСТ Р 34.11-1994	ГОСТ Р 34.11-2012
Размер блока входных данных	256	512
Длина хэша	256	256, 512
Функции сжатия	симметричный блочный шифр ГОСТ Р 28147-89	нелинейное биективное преобразование (S); перестановка байт (P); линейное преобразование (L)
Значение инициализационного вектора	не определялось	значение фиксировано и определено в стандарте

ГОСТ Р 34.11-94 включает в себя:

1. Область применения
2. Нормативные ссылки
3. Обозначения
4. Общие положения
5. Шаговая функция хеширования
6. Процедура вычисления хеш-функции
7. Проверочные примеры

Особенности ГОСТ Р 34.11-94:

- При обработке блоков используются преобразования по алгоритму ГОСТ 28147—89;
- Обрабатывается блок длиной 256 бит, и выходное значение тоже имеет длину 256 бит.
- Определяет контрольную сумму, рассчитанную по всем блокам исходного сообщения, которая является частью финального вычисления хеша, что несколько затрудняет коллизионную атаку.
- Применены меры борьбы против поиска коллизий, основанном на неполноте последнего блока.
- Обработка блоков происходит по алгоритму шифрования ГОСТ 28147—89, который содержит преобразования на S-блоках, что существенно осложняет применение метода дифференциального криптоанализа к поиску коллизий.

Формат вывода

Согласно ГОСТ стандарту, результатом хеш-функции является 256-битное число. Стандарт не указывает, как оно должно выводиться. Разные реализации используют различные форматы вывода.

ГОСТ Р 34.11-94 в «приложении А» оперирует с Little-endian числами. Многие реализации выводят 32 байта результирующего хеша в шестнадцатеричном представлении, в порядке, в каком они располагаются в памяти — младшие байты первыми.

В приведённых в стандарте примерах результирующий хеш записывается как шестнадцатеричное представление 256-битного Little-endian числа. Тем самым, получается обратный порядок байт (старшие разряды первыми).

Оценка криптостойкости

В 2008 году командой экспертов из Австрии и Польши была обнаружена техническая уязвимость, сокращающая поиск коллизий в 2^{23} раз. Количество операций, необходимое для нахождения коллизии, таким образом, составляет 2^{105}, что, однако, на данный момент практически не реализуемо. Проведение коллизионной атаки на практике имеет смысл только в случае цифровой подписи документов, причём, если взломщик может изменять неподписанный оригинал.

Использование:

- В сертификатах открытых ключей.
- Для защиты сообщений в S/MIME (Cryptographic Message Syntax, PKCS#7).
- Для защиты соединений в TLS (SSL, HTTPS, WEB).
- Для защиты сообщений в XML Signature (XML Encryption).
- Защита целостности Интернет адресов и имён (DNSSEC).

Спасибо за внимание!