Network Working Group
Request for Comments: 3874
Category: Informational

R. Housley
Vigil Security

September 2004

Необратимая 224-битовая хэш-функция SHA-224

A 224-bit One-way Hash Function: SHA-224

Статус документа

В этом документе содержится информация для сообщества Internet. Документ не содержит каких-либо стандартов Internet. Допускается свободное распространение документа.

Авторские права

Аннотация

В данном документе описывается 224-битовая необратимая хэш-функция SHA-224, основанная на SHA-256, но использующая другое начальное значение и размер 224 бита.

1. Введение

В этом документе содержится спецификация 224-битовой необратимой хэш-функции, носящей название SHA-224. Национальный институт стандартов и технологии США (NIST) в документе FIPS 180-2 Change Notice от 28 февраля 2004 подтвердил необратимость хэш-функции SHA-224. Необратимые хэш-функции называют также цифровыми подписями[1]. Функция SHA-224 основана на алгоритме SHA-256, обеспечивающем необратимое 256-битовое хэширование, подтверждённое NIST [SHA2]. Расчёт хэш-значения SHA-224 выполняется в два этапа. Сначала определяется значение SHA-256 (при этом используется иное стартовое значение) и затем полученный результат сокращается до 224 битов.

NIST занимается разработкой руководства по ключам шифрования и недавно этот институт опубликовал для комментариев черновой вариант документа [NISTGUIDE]. В руководстве обсуждаются пять уровней конфиденциальности с ключами размером 80, 112, 128, 192 и 256 битов. Для всех этих уровней, за исключением одного, доступны необратимые хэш-функции. SHA-224 предназначена для заполнения пустого места в этом списке. Необратимая хэш-функция SHA-224 обеспечивает ключи размером 112 битов, что совпадает с одним из общепринятых вариантов Triple-DES [3DES].

В этом документе приводится спецификация необратимой хэш-функции SHA-224 для сообщества Internet, а также идентификаторы объектов для использования в протоколах, основанных на ASN.1.

1.1. Вопросы применения

Поскольку функция SHA-224 основана на SHA-256, при её вычислении выполняется примерно такой же объем работ. Однако, несмотря на практически одинаковую сложность вычислений, SHA-224 хорошо подходит для использования в качестве необратимой хэш-функции, генерирующей ключи размером 112 битов. Использование другого стартового значения и последующее отсечение созданных сигнатур SHA-256 позволяет однозначно идентифицировать сигнатуры SHA-224, рассчитанные для тех же данных.

Для некоторых сред важен каждый передаваемый октет. В таких случаях сокращение сигнатуры на 4 октета по сравнению с SHA-256 имеет важное значение.

Исходя из сказанного выше можно предложить следующие рекомендации по использованию функции:

- при использовании с алгоритмами шифрования, основанными на ключах размером 112 битов SHA-224 обеспечивает подходящую необратимую хэш-функцию;
- когда компактность сигнатур не играет важной роли, следует использовать SHA-256, а не SHA-224.

1.2. Терминология

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с [STDWORDS].

2. Описание SHA-224

Алгоритм SHA-224 может использоваться при расчёте необратимых хэш-значений для сообщений размером до 2^{64} битов.

[1] Английский термин - message digest. *Прим. перев.*

SHA-224 использует алгоритм SHA-256 [SHA2]. Для расчёта необратимой хэш-функции SHA-256 использует опись[1] из шестидесяти четырёх 32-битовых слов, восемь 32-битовых рабочих переменных и создаёт хэш-значение из восьми 32-битовых слов.

Функция SHA-224 определяется также, как SHA-256, с двумя отличиями:

1) Для SHA-224 начальное хэш-значение представляет собой восемь 32-битовых рабочих переменных, совместно обозначаемых как H, которые должны быть равны:

```
H_0 = c1059ed8              H_4 = ffc00b31
H_1 = 367cd507              H_5 = 68581511
H_2 = 3070dd17              H_6 = 64f98fa7
H_3 = f70e5939              H_7 = befa4fa4
```

2) SHA-224 просто использует первые сеть 32-битовых слов результата SHA-256. Таким образом, окончательное значение H представляет собой конкатенацию (||) семи компонент:

```
H_0 || H_1 || H_2 || H_3 || H_4 || H_5 || H_6
```

3. Тестовые векторы

В этом параграфе описаны три тестовых вектора, которые могут использоваться для проверки реализации алгоритма SHA-224.

3.1. Вектор #1

Предположим, что хэшируемое сообщение содержит 24-битовую строку ASCII "abc", которая эквивалентна двоичной строке:

```
01100001 01100010 01100011
```

Функция SHA-224 в этом случае должна возвращать значение (в шестнадцатеричном представлении):

```
23097d22 3405d822 8642a477 bda255b3 2aadbce4 bda0b3f7 e36c9da7
```

3.2. Вектор #2

При хэшировании 448-битовой строки ASCII "abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq" функция SHA-224 должна возвращать значение (в шестнадцатеричном представлении):

```
75388b16 512776cc 5dba5da1 fd890150 b0c6455c b4f58b19 52522525
```

3.3. Вектор #3

При хэшировании сообщения, содержащего 1 000 000 символов "a", функция SHA-224 должна возвращать хэш-значение (в шестнадцатеричном представлении):

```
20794655 980c91d8 bbb4c1ea 97618a4b f03f4258 1948b2ee 4ee7ad67
```

4. Идентификатор объекта

NIST выделил идентификатор объекта ASN.1 [X.208-88, X.209-88] для SHA-224. Некоторые протоколы используют идентификатор объекта для именования необратимых хэш-функций. Примером такого протокола является CMS [CMS]. Разработчики такого типа протоколов, которые используют SHA-224, **должны** указывать идентификатор объекта.

```
id-sha224  OBJECT IDENTIFIER  ::=  { joint-iso-itu-t(2)
                country(16) us(840) organization(1) gov(101)
                csor(3) nistalgorithm(4) hashalgs(2) sha224(4) }
```

5. Вопросы безопасности

Необратимые хэш-функции обычно используются с другими криптографическими алгоритмами (такими, как алгоритмы создания цифровых подписей и кодов аутентификации сообщений) или при генерации случайных значений. При использовании необратимой хэш-функции вместе с другим алгоритмом могут присутствовать указанные где-либо требования по уровню безопасности (размер ключа). Например, если сообщение подписывается сигнатурой размером 128 битов, алгоритм создания такой сигнатуры может потребовать использования необратимой хэш-функции, возвращающей хэш-значение такого же размера. SHA-224 генерирует 112-битовые хэш-значения, в общем случае пригодные для Triple-DES [3DES].

Этот документ содержит спецификацию SHA-224 для сообщества Internet. Автор не даёт гарантий безопасности для того или иного использования алгоритма. Однако, поскольку применение SHA-256 обеспечивает ожидаемый уровень безопасности, SHA-224 также будет обеспечивать ожидаемый уровень.

6. Литература

6.1. Нормативные документы

[SHA2] Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, 1 August 2002.

[STDWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

6.2. Информационные ссылки

[3DES] American National Standards Institute. ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of Operation. 1998.

[CMS] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.

[1] В оригинале message schedule. *Прим. перев.*

[NISTGUIDE] National Institute of Standards and Technology. Second Draft: "Key Management Guideline, Part 1: General Guidance." June 2002. [http://csrc.nist.gov/encryption/kms/guideline-1.pdf]

[X.208-88] CCITT Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1). 1988.

[X.209-88] CCITT Recommendation X.209: Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1). 1988.

7. Благодарности

Большое спасибо Джиму Шааду (Jim Schaad) за генерацию тестовых векторов. Для подтверждения корректности этих векторов была использована реализация Брайана Глэдмана (Brian Gladman).

8. Адреса авторов

Russell Housley

Vigil Security, LLC

918 Spring Knoll Drive

Herndon, VA 20170

USA

EMail: housley@vigilsec.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

9. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.