GLOBAL 2007

Обучение Java

Тема **Безопасность в JAVA**

Часть **Дайджесты сообщений**

Автор **ASKIL (omendba@gmail.com)**

1.03.2007

За последние 50 лет специалисты в области математики и информатики разработали много сложных алгоритмов поддержки целостности данных и цифровых подписей. Многие из них реализованы в пакете java.security. Для использования таких алгоритмов совсем не обязательно понимать математические принципы, на которых основаны. Существует механизм, с помощью которого *дайджест сообщения* позволяет обнаружить факт изменения данного документа, а также способы, посредством которых цифровая подпись подтверждает личность пользователя.

Дайджест сообщения – это цифровой "отпечаток" блока данных. Например, хэш-алгоритм обеспечения безопасности SHA1 ставит в соответствие блоку данных произвольного размера – 160 бит (20 байт). По аналогии с отпечатками пальцев, считается, что не существует двух одинаковых отпечатков SHA1. На самом деле это не так, поскольку алгоритм SHA1 поддерживает 2^{160} отпечатков, поэтому теоретически они могут совпадать. Но число 2^{160} настолько велико, что вероятность дублирования очень мала.

Дайджест сообщения имеет два важных свойства.

1. Если изменяется один или несколько битов данных, то дайджест сообщения тоже будет изменен.

2. Нельзя изменить оригинальное сообщение таким образом, чтобы полученное поддельное сообщение имело такой же дайджест, что и у оригинального сообщения.

Второе свойство, конечно, соблюдается с определенной степенью вероятности.

Существует несколько алгоритмов определения дайджеста сообщения. Наиболее известными из них являются SHA1, разработанный национальным институтом стандартов и технологий (NIST), и MD5, изобретенный Рональдом Райвестом (Ronald Rivest) из Массачуссетского технологического института (MIT). Оба алгоритма зашифровывают сообщение разными оригинальными способами. В алгоритме MD5 совсем недавно были обнаружены изъяны, поэтому многие ведущие специалисты-шифровальщики рекомендуют использовать алгоритм SHA1.

В языке Java реализованы оба эти алгоритма. Класс MessageDigest представляет собой фабрику (factory) объектов, которые реализуют алгоритмы создания цифровых отпечатков. Данный класс содержит статический метод getInstance(), который возвращает экземпляр подкласса класса MessageDigest. Поэтому класс MessageDigest может выступать в роли класса-фабрики, или суперкласса, для всех алгоритмов создания профиля сообщения.

Рассмотрим процедуру, вычисляющую дайджест сообщения.

```
/**
 * Получить цифровой отпечаток сообщения.
 * @param alg <B>Алгоритм отпечатка</B>
 * @param message <B>Сообщение</B>
 * @return Строка из hex-значений
*/
public String GetMessageDigest(String alg, String message)
{
 try
 {
   MessageDigest md = MessageDigest.getInstance(alg);
   md.update(message.getBytes());
   byte [] hash = md.digest();
   return GetHexString(hash);
 }
 catch(NoSuchAlgorithmException e){GetError(e.getMessage()); return null;}
}
```

При выполнении кода:

```
String s = "Hello Java";
System.out.println(GetMessageDigest("SHA1",s));
System.out.println(GetMessageDigest("MD5",s));
```

Мы получим следующее:

```
63 52 24 46 BA A1 F6 5E DB 79 D5 EF 8A B6 84 C5 CF D0 88 15
3A 79 FB 63 BB 4A 36 EB 64 21 83 6A 59 E2 AF 10
```