**Hướng dẫn sử dụng mã hóa băm MD/ SHA với Java**

Tham khảo tên các phương pháp mã hóa trong Java Doc:

<https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html#AlgorithmParameters>

Tham khảo class mã hóa bằng kỹ thuật băm (MD5, SHA):

<https://docs.oracle.com/javase/7/docs/api/java/security/MessageDigest.html>

MD5 (Message-Digest Algorithms) và SHA(Secure Hash Algorithms) là các giải thuật mã hóa một chiều nhằm từ dữ liệu ban đầu các giải thuật này tạo ra một dữ liệu mới có độ dài cố định, gọi là ***digest***, giúp kiểm tra tính toàn vẹn của dữ liệu kèm theo dữ liệu ban đầu.

Bên Sender: Source – Encoding 🡪 Bit\_String\_1. Sender gửi cho receiver (Source + Bit\_String\_1).

Bên Receiver: Nhận được Source + Bit\_String\_1. Receiver mang Source đi mã hòa lại để được Bit\_String\_2. Nếu Bit\_String\_1 = Bit\_String\_2 thì kết luận Source này đáng tin cậy.

**Các cách dùng mã hóa băm**

1. Lưu user password dạng mã hóa băm an toàn hơn vì admin không thể biết được user password dù có mở database ra xem.
2. Phương tiện truyền file có kiểm tra. Xem lại thí dụ trên.

**Đánh giá MD5 và SHA**

* Người ta đã phát hiện trong một số rất ít tình huống 2 data nguồn khác nhau nhưng cho cùng kết quả MD5. Do vậy, MD5 chưa thực sự an toàn nhưng vẫn được dùng.
* SHA là giải thuật được giới thiệu sau MD và được ghi nhận là an toàn hơn MD5

**Mã hóa băm với Java: Package java.security**

Các lớp quan trọng: MessageDigest, NoSuchAlgorithmException (exception khi chỉ định tên giải thuật không đúng).

**Tên các giải thuật đã được định nghĩa trong Java**

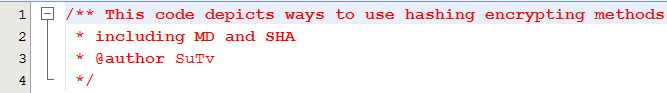
| Algorithm Name | Description |
| --- | --- |
| **MD2** | The MD2 message digest algorithm as defined in [RFC 1319](https://tools.ietf.org/html/rfc1319). |
| **MD5** | The MD5 message digest algorithm as defined in [RFC 1321](https://tools.ietf.org/html/rfc1321). |
| **SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 SHA-512/224 SHA-512/256** | Hash algorithms defined in the [FIPS PUB 180-4](https://csrc.nist.gov/publications/detail/fips/180/4/final).  Secure hash algorithms - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 - for computing a condensed representation of electronic data (message). When a message of any length less than 264 bits (for SHA-1, SHA-224, and SHA-256) or less than 2128 (for SHA-384 and SHA-512) is input to a hash algorithm, the result is an output called a message digest. A message digest ranges in length from 160 to 512 bits, depending on the algorithm. |

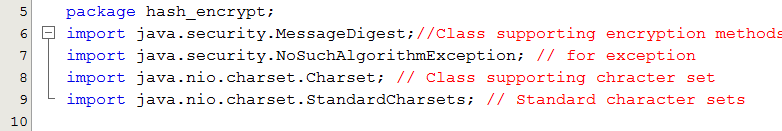
Các giải thuật dưới MD5 đang dần bị loại bỏ.

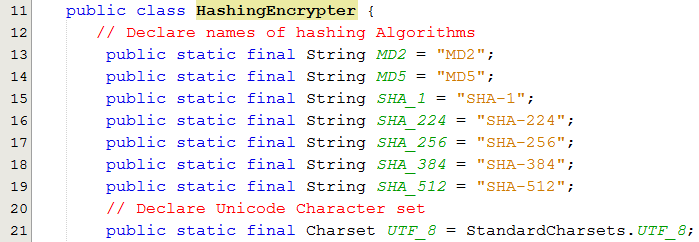
**Độ dài chuỗi mã hóa**

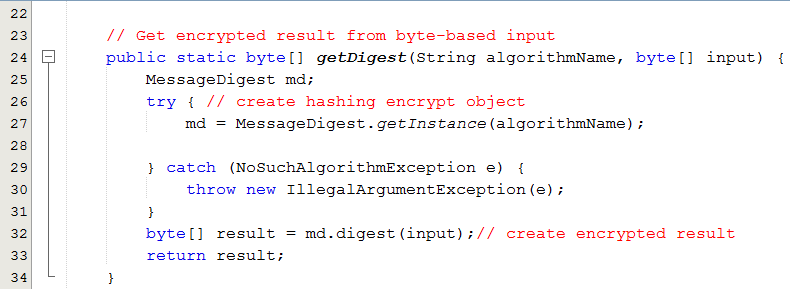
* MD5: 128 bit (16 bytes).
* SHA-1: kết quả là 160 bit (20 bytes), SHA-224: 224 bits (28 bytes), SHA-256: 256 bits (32 bytes), SHA-384: 384 bits, SHA-512: 512 bit (64 bytes)s

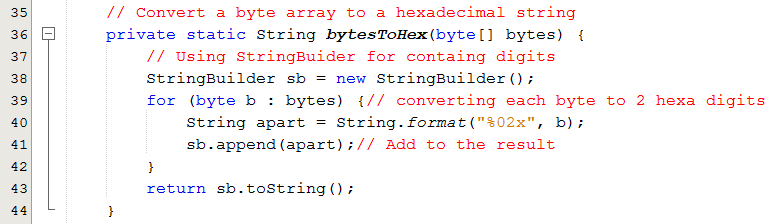
**Demo cách dùng mã hóa băm**

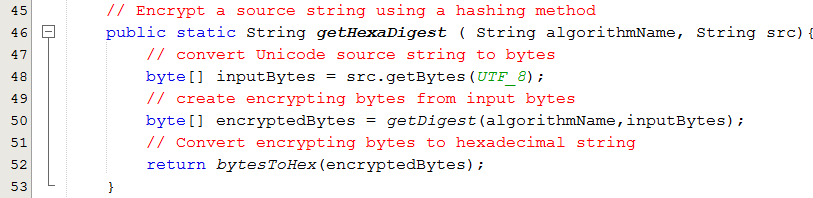


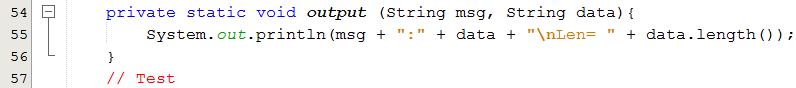


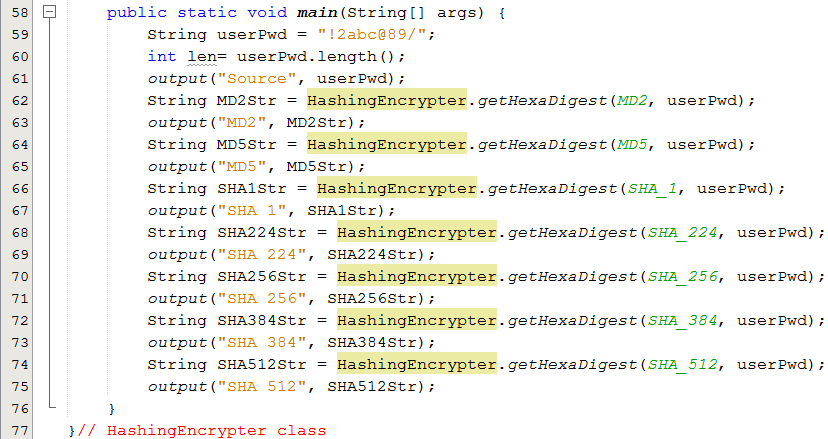












**Kết quả**

