

TUTORIAL

CRYPTOGRAPH

Y

Hash function

1. Hashing algorithm with certutil

- Estimated duration: 10 mins

CertUtil is a pre-installed Windows utility that can be used to generate hash checksums:

```
certUtil -hashfile pathToFileToCheck  
[HashAlgorithm]
```

HashAlgorithm choices: MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512

Download the Unikey software from FIT

portal. Save it to Desktop, rename it as

unikey.exe

Open CMD, change working directory to Desktop

Use *certutil* command to see hash value of the file.

```
C:\Users\ADMIN>cd Desktop  
  
C:\Users\ADMIN\Desktop>certutil -hashfile unikey.exe  
SHA1 hash of unikey.exe:  
c698a001358459252c089bfe55f591f80d141e17  
CertUtil: -hashfile command completed successfully.
```

Go to this website: <http://unikey.vn/vietnam/#nav4> to view checksum of original file.

Tell me the file downloaded from FIT portal is modified or not, compared to the original file from its official site.

2. Online generator

<https://www.md5hashgenerator.com>

<http://www.sha1-online.com>

3. Practice with Hash functions in Java

Download code here: (MD5, SHA, Bcrypt)

[https://drive.google.com/drive/folders/118fb-paTaZfriWr2-3T2cLC39q9bYp9h?usp=share link](https://drive.google.com/drive/folders/118fb-paTaZfriWr2-3T2cLC39q9bYp9h?usp=share_link)