# How MD5 Works

2014-10-14

Yiwang ZHENG (12330423)

MD5 means Message Digest Algorithm – 5, it's an algorithm to generate an unique identification string, just like our fingerprints identify who we are. So this algorithm is widely applied to help one checking whether the message he received is exactly the original message he wants.

The working flow of MD5 contains three basic steps:

- Data Provider
    1. generate the “fingerprints” for data
    2. release their data
    3. put the “fingerprints” to someplace for user to check, usually the officail website of their products
- Customer
    1. get the data by any ways
    2. use software to calculate the MD5 value of the data he got
    3. visit some reliable place and get the correct MD5 value
    4. compare these two MD5 value, if they are just the same, then the customer can draw a conclusion that the data he got is the original data

If the data has been modified by someone or some errors occur when downloading or any possible issues that may change the content of the data happens, it's impossible for the user to generate the correct MD5 value since even little changes in the data will leads to great differences to the MD5 value.