

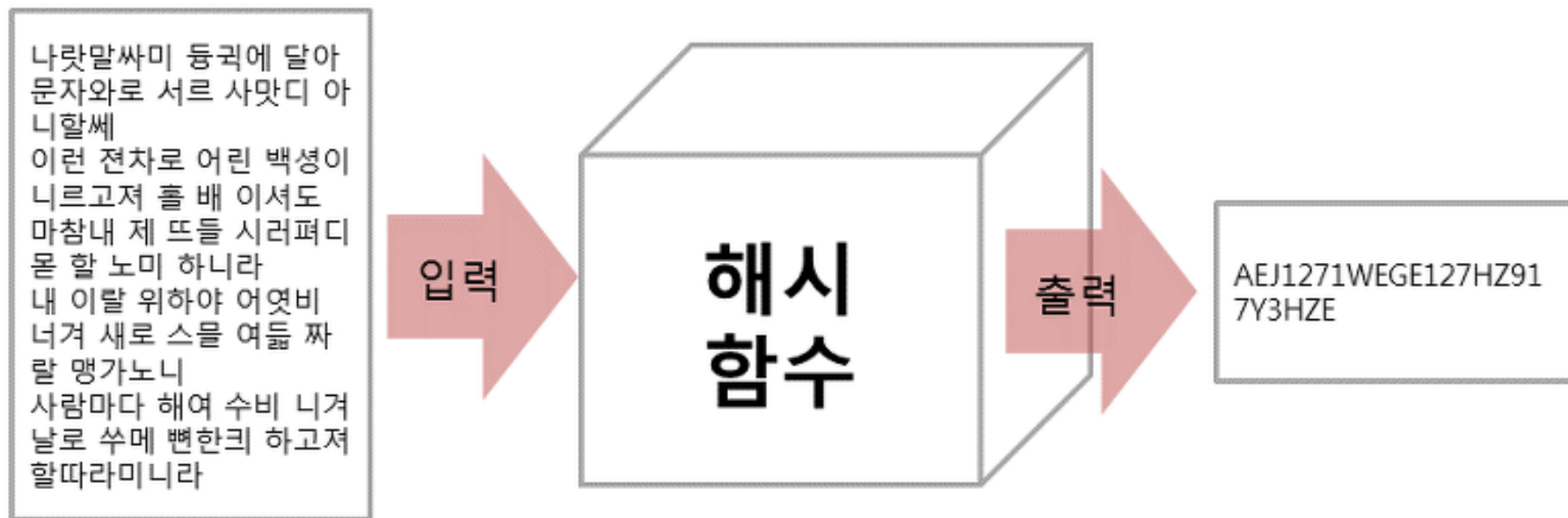
해시함수 MD5

송민호

유튜브 주소: <https://youtu.be/nTt99dRGnWk>

해시함수

입력 데이터를 고정된 길이의 키로 변환
데이터 암호화, 무결성 검증



종류

해시 함수	블록 크기	키 길이
SHA 시리즈(SHA-256)	512	256
MD5	512	128
N-NASH	128	128
SNEFRU	512	128,256

MD5

128비트 암호화 해시 함수

주로 무결성 검사에 이용

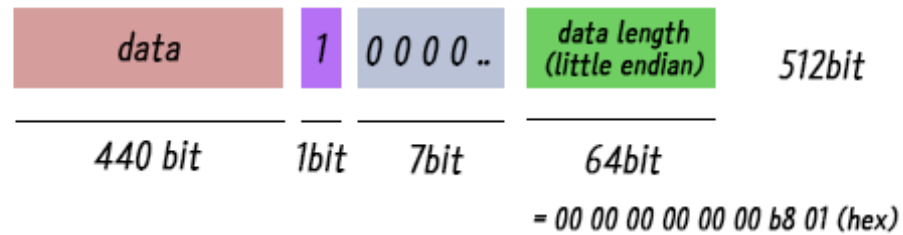
패딩을 사용하여 입력 메시지를 512비트 블록으로 나눔

MD5

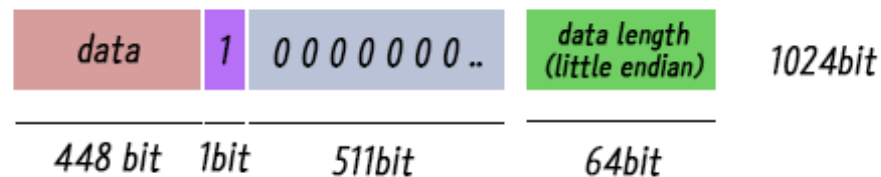
패딩

input	bit1	bit2 ~	나머지 64bit
data	1	0	data length(little endian)

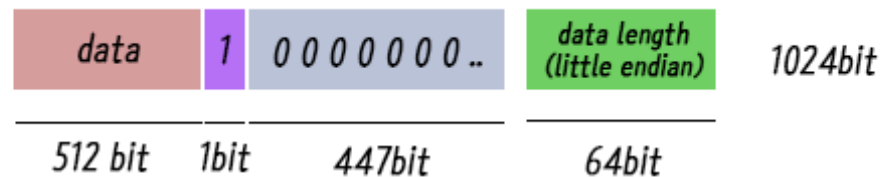
ex) input data 440bit



ex2) input data 448 bit



ex3) input data 512 bit



MD5

알고리즘

128비트 스테이트에 대해 동작

4라운드로 구성

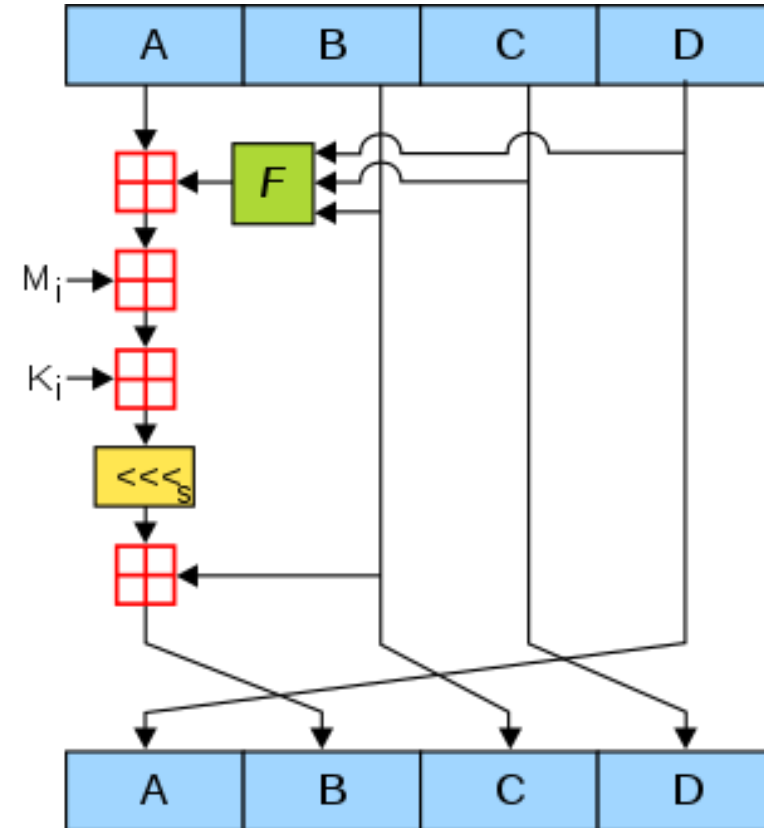
각 라운드마다 다른 F함수 사용

$$F(X, Y, Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$

$$G(X, Y, Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$

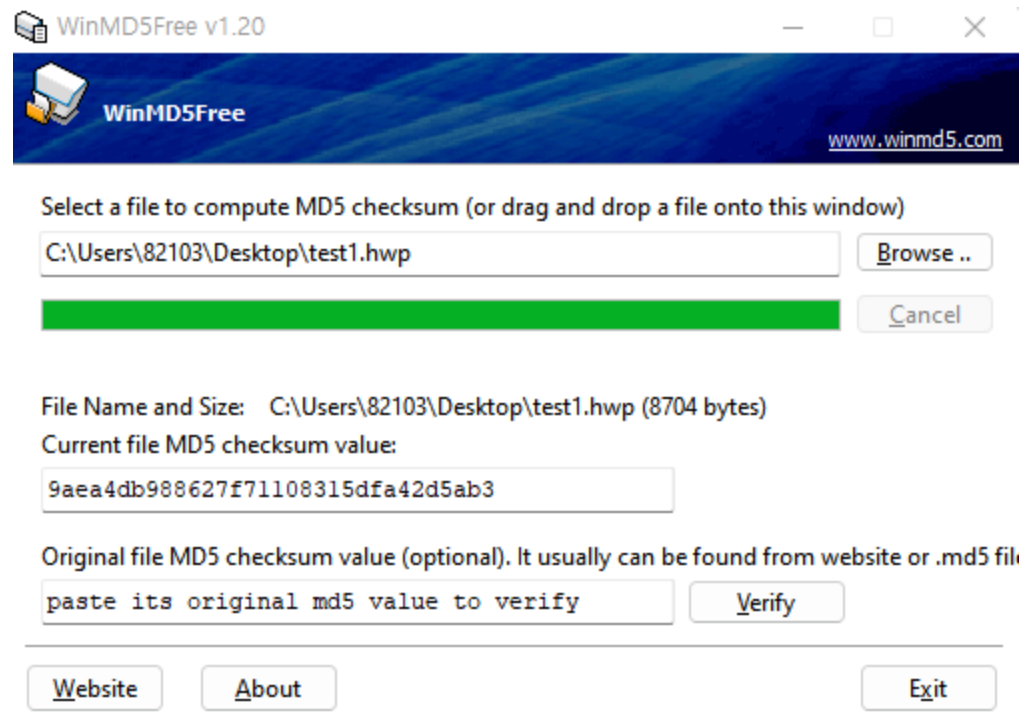
$$H(X, Y, Z) = X \oplus Y \oplus Z$$

$$I(X, Y, Z) = Y \oplus (X \vee \neg Z)$$



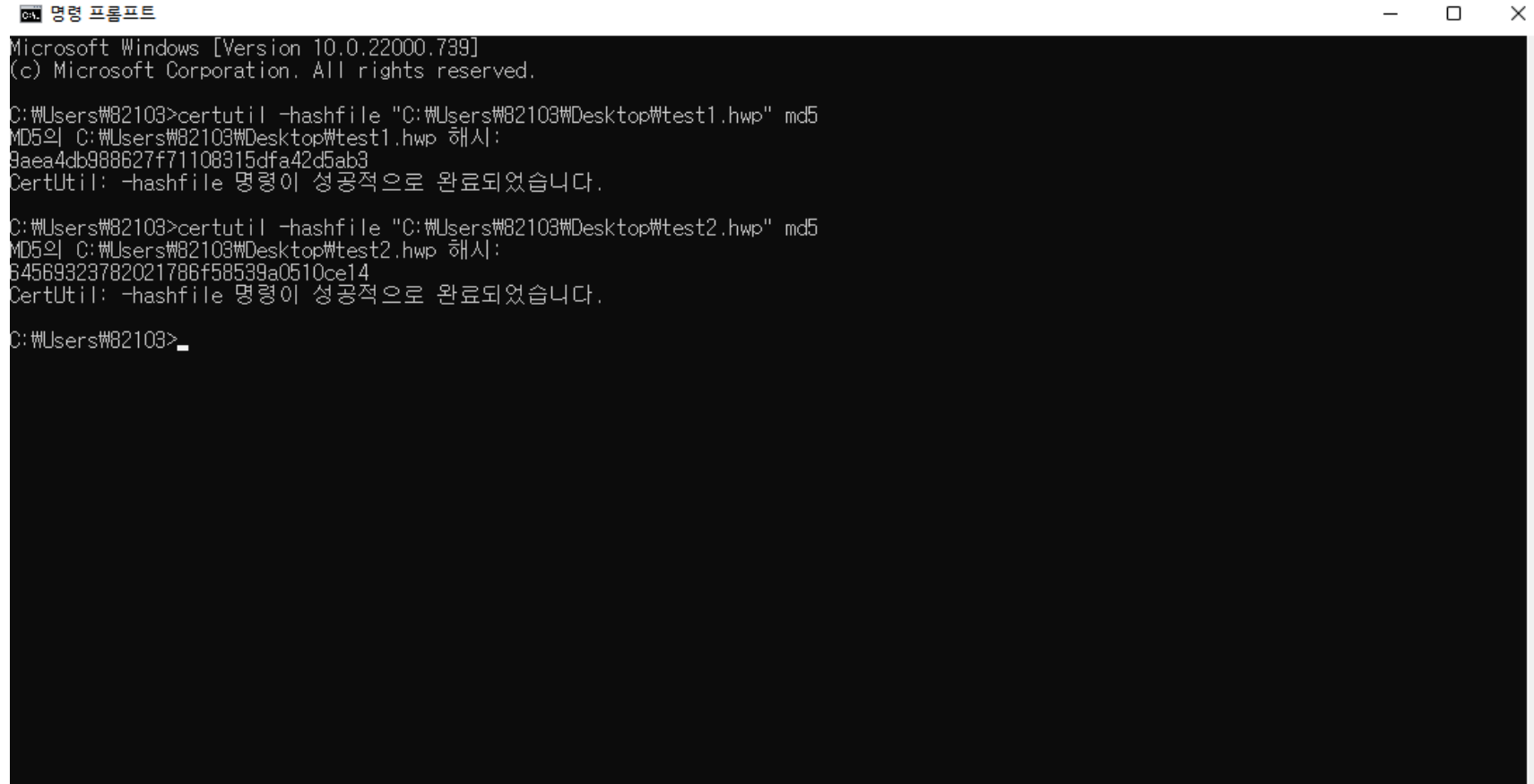
MD5

프로그램 통해 해시 확인



MD5

Certutil -hashfile <경로명> md5



```
CA> 명령 프롬프트
Microsoft Windows [Version 10.0.22000.739]
(c) Microsoft Corporation. All rights reserved.

C:\Users\82103>certutil -hashfile "C:\Users\82103\Desktop\test1.hwp" md5
MD5의 C:\Users\82103\Desktop\test1.hwp 해시:
9aea4db988627f71108315dfa42d5ab3
CertUtil: -hashfile 명령이 성공적으로 완료되었습니다.

C:\Users\82103>certutil -hashfile "C:\Users\82103\Desktop\test2.hwp" md5
MD5의 C:\Users\82103\Desktop\test2.hwp 해시:
64569323782021786f58539a0510ce14
CertUtil: -hashfile 명령이 성공적으로 완료되었습니다.

C:\Users\82103>
```


MD5

암호화

MD5 암호화 온라인 도구

1

abc123

UpperCase

Hash Result in UpperCase

 빈

MD5 암호화

 결과 복사

1

E99A18C428CB38D5F260853678922E03

MD5

문제점

복호화 가능

날짜	취약점
1996년	설계상 결함이 발견. 해시 용도로 SHA-1와 같이 다른 안전한 알고리즘을 사용할 것을 권장
2004년 8월	알고리즘 결함(해시 충돌) 발견
2006년 3월	컴퓨터 한 대의 계산 능력으로 1분 내에 해시 충돌 발견
2008년 12월	MD5의 결함을 이용한 SSL 인증서 변조 가능성 발표

MD5

복호화

Enter 32 character MD5 hash to decode or decrypt

Enter 32 digit MD5 hash:

e99a18c428cb38d5f260853678922e03

Enter 4 digit security code:

9348

9348

MD5 HASH DECODE

MD5 hash decryption results

[Re-encode result](#)

The hash `md5:e99a18c428cb38d5f260853678922e03` decodes to:

String: `abc123`

Hex: `61 62 63 31 32 33`

Q & A