

SHA-3 해시함수 알고리즘에 대한 소스코드 활용 매뉴얼

2020. 02.

제·개정 이력

순번	제·개정일	제·개정 내역
1	2020.02	"SHA-3 해시함수 알고리즘에 대한 소스코드 활용 매뉴얼" 발간

Contents

1. 개요	1
2. 해시함수 SHA-3	1
3. 소스코드	7
4. 응용 프로그램	8
5. 웹 프로그램	19
6. 참조구현값	25
7. C/C++ 소스코드	71

1. 개요

SHA-3는 데이터의 무결성을 제공하기 위한 해시함수으로써, 안전성에 문제가 제기된 SHA-1과 SHA-2를 대체하기 위하여 NIST에서 SHA-3 해시함수 공모를 통해 선정한 해시함수이다.

본 매뉴얼은 SHA-3의 다양한 출력비트 별 소스코드를 다양한 언어 및 플랫폼에서 쉽게 활용할 수 있도록 C/C++, Java, ASP, PHP, JSP용으로 개발된 소스코드의 설명과 함께 사용 시 주의사항을 다룬다.

2. 해시함수 SHA-3

가. 해시함수

해시함수는 정보에 대한 무결성 확인, 인증, 전자서명 등의 정보보안 기능을 제공하기 위해 사용되는 함수이다. 해시함수는 임의의 길이를 갖는 메시지를 입력받아 해시함수에서 제공하는 고정된 길이의 해시값을 출력해 주는 함수이다. 해시함수의 출력값, 즉, 해시값을 사용하여 본래의 메시지 또는 정보에 대한 무결성을 확인할 수 있는 기능을 담고 있다. 암호학에서 말하는 해시함수는 역상 저항성, 제 2 역상 저항성, 충돌 저항성을 만족해야 하며, 수학적으로 증명가능한 안전성이 보장되는 알고리즘을 말한다.

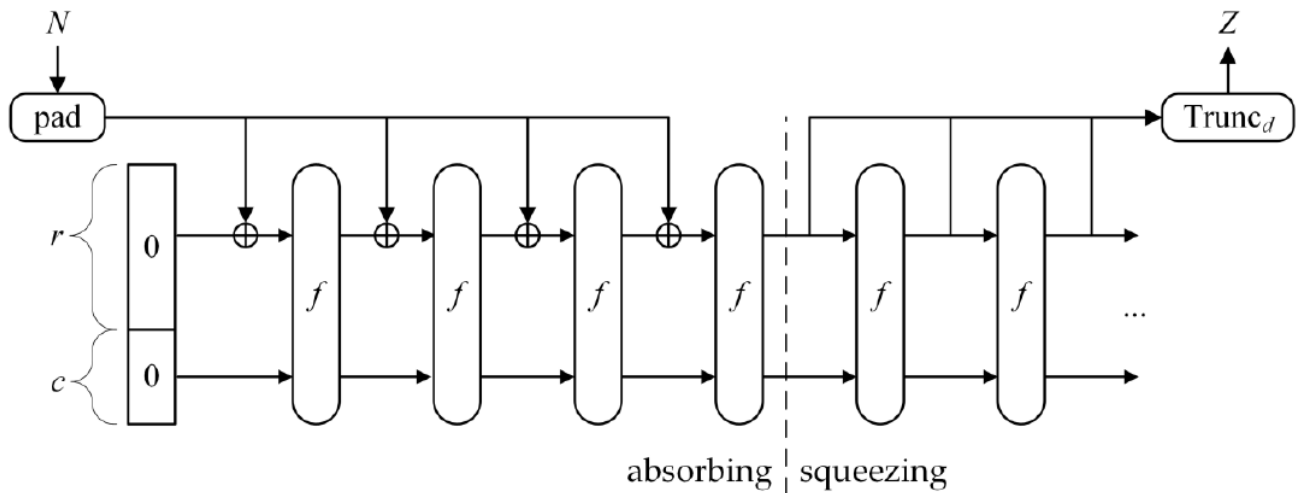
SHA(Secure Hash Algorithm) 해시함수는 미국에서 처음으로 제안되었으며, SHA-1, SHA-2를 표준화가 진행되었다. 그러나, 2005년 SHA-1에 대한 충돌쌍 공격이 발표되면서 SHA-1의 안전성에 대한 문제가 거론되고 이어 SHA-2의 안전성에 대한 의문이 제기된다. 이에 2007년 SHA-3 공모를 통해, 2012년 KECCAK 알고리즘이 SHA-3로 선정되었다.

나. SHA-3

SHA-3는 SHA3-224, SHA3-256, SHA3-384, SHA3-512 4개의 해시함수와 SHAKE128, SHAKE256 2개의 확장 가능한 출력함수(Extendable-output functions, XOF)로 구성되어 있다.

1) SHA-3 스펀지 구조

SHA-3는 스펀지 구조를 갖고 있다. SHA-3에서는 b 비트 순열을 갖는 f 함수와 메시지를 패딩하는 패딩함수를 이용하여 메시지 압축과정을 진행한다. 입력된 메시지는 정해진 bitrate에 따라 f 함수 출력과 XOR 연산 과정을 통해 흡수(absorbing)과정을 거치게 되고 마지막 압착(squeezing)과정을 통해 최종 해시값을 출력한다.



< SHA3 스펀지 구조 >

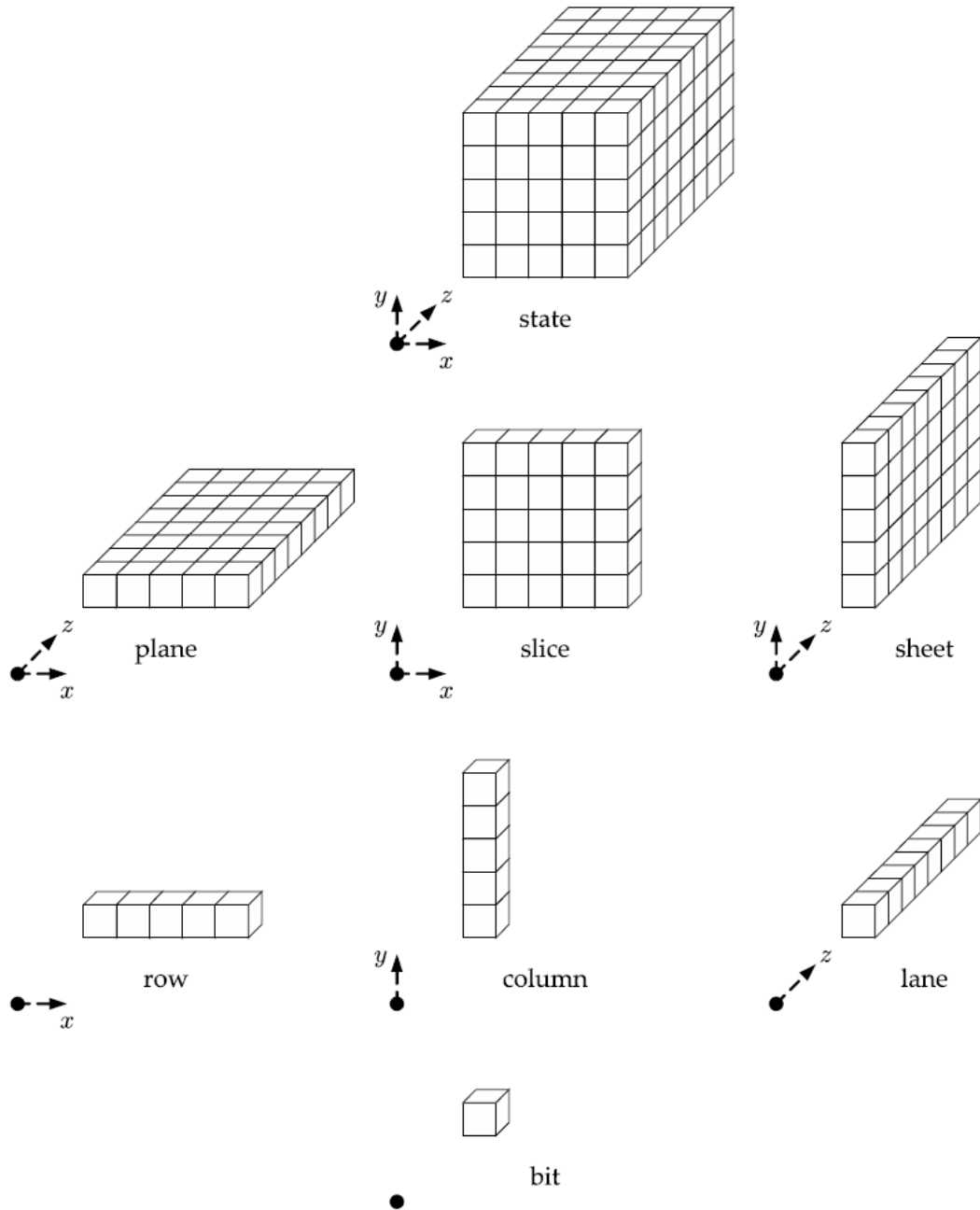
SHA-3의 b 순열은 $state$ 의 크기를 말하며 $b \in 25, 50, 100, 200, 400, 800, 1600$ 으로 정해져 있다. b 는 bitrate인 r 과 capacity인 c 로 나누어지며 $b = r + c$ 만족해야 한다, 다음은 $b = 1600$ 일 때, 각 해시함수의 r 과 c 값이다.

	bitrate(r)	capacity(c)
SHA3-224	448	1152
SHA3-256	512	1088
SHA3-384	768	832
SHA3-512	1024	576
SHAKE128	256	1344
SHAKE256	512	1088

< 입력 b 비트별 bitrate(r)과 capacity(c) 값 >

2) SHA-3 f 함수

SHA-3 f 함수는 3차원 행렬 $state$ 로 이뤄져 있다. 다음은 3차원 행렬 $state$ 의 각 구조와 3차원 행렬을 이루는 부분들의 명칭이다.



< SHA-3 3차원 행렬 *state*와 각 부분 명칭 >

SHA-3 해시함수의 *state*는 $x \times y \times z$ 3차원 행렬로써 $\text{row}(x)$ 와 $\text{column}(y)$ 는 각각 5로 고정이며 b 비트에 따라 $5 \times 5 \times w$ 로 구성된다. 다음은 각 b 에 따른 w 와 l 값이다.

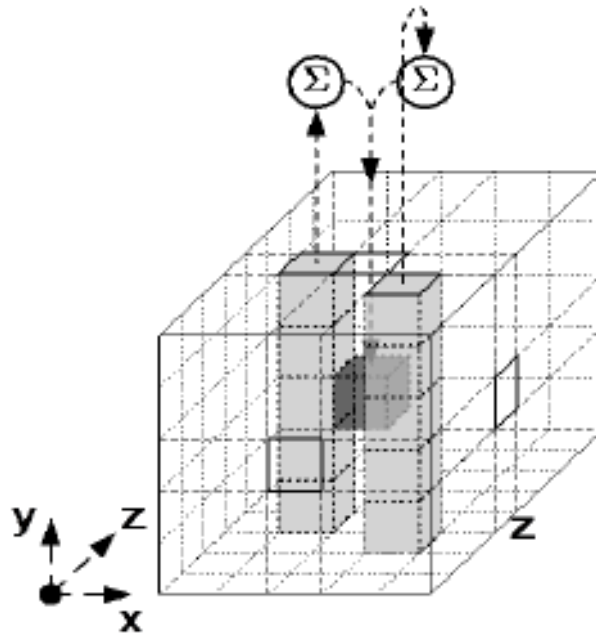
$b(\text{bit})$	25	50	100	200	400	800	1600
w	1	2	4	8	16	32	64
l	0	1	2	3	4	5	6

< b 비트에 따른 w 와 l 값 >

SHA-3는 b 에 따라 라운드 값이 결정된다. b 가 1600인 경우 라운드는 24이다. 각 라운드는 5개의 부분함수로 구성되어 있으며 각 부분함수는 다음과 같으며 $state$ 는 A 로 표시한다.

$[\theta(A)$ (Theta)]

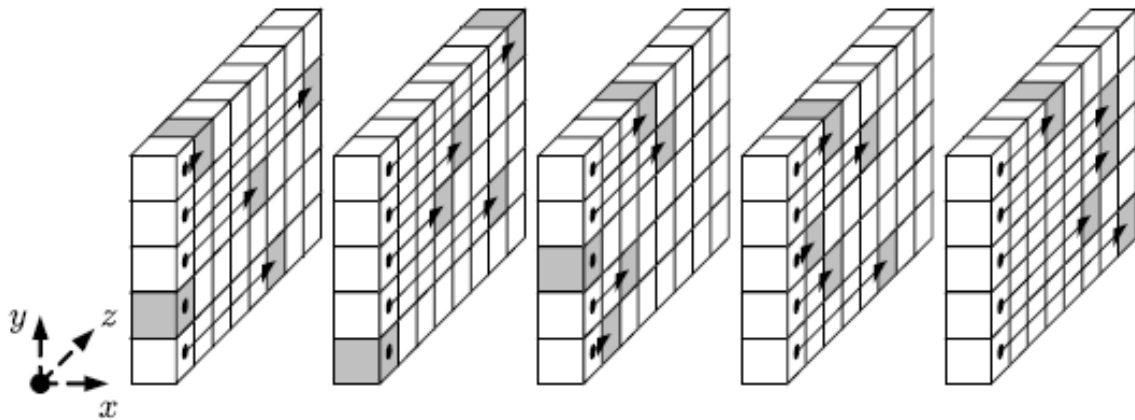
$((x-1), z)$ column 비트 합과 $((x+1), (z-1))$ column 비트 합을 XOR 한 뒤 (x, y, z) 의 비트 값과 XOR 하여 (x, y, z) 에 저장하는 과정이다.



< $\theta(A)$ 함수의 구조 >

$[\rho(A)$ (Rho)]

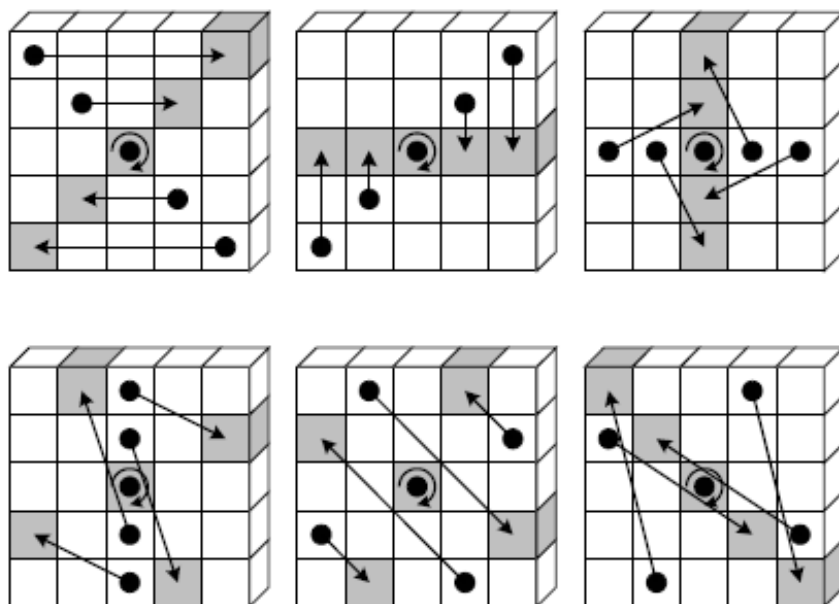
각 $lane$ 에서 정해진 offset 만큼 Rotate하는 과정이다.



< $\rho(A)$ 함수의 구조 >

$[\pi(A)(Pi)]$

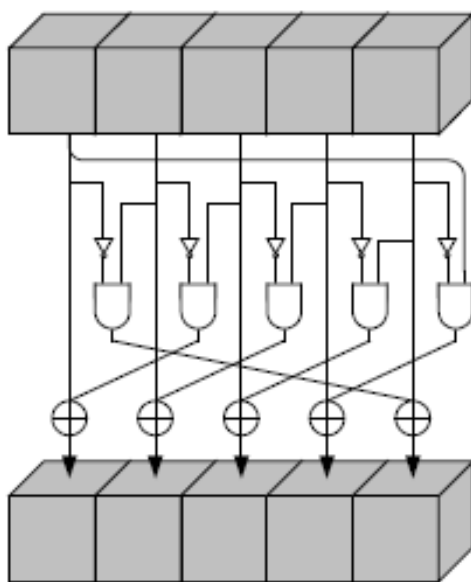
$state$ 내에서 $lane$ 의 자리를 재배열하는 과정이다.



< $\pi(A)$ 함수의 구조 >

$[\chi(A)(Chi)]$

오른쪽 2개 비트를 곱셈 연산한 결과와 XOR 연산하는 과정이다.



< $\chi(A)$ 함수의 구조 >

$[\iota(A)(Iota)]$

$Lane(0,0)$ 이 라운드 상수와 XOR 연산을 수행하는 과정이다.

SHA-3 f 함수는 위 5개의 부분함수를 하나의 라운드 함수로 동작하며, 입력 b 비트에 따라 $12 + 2l$ 만큼의 라운드로 f 함수가 구성된다.

3) SHA-3 패딩함수

SHA-3 해시함수에 입력된 메시지는 bitrate 단위로 f 함수의 출력과 XOR 연산이 수행되어야 한다. 따라서 입력된 메시지는 패딩과정을 통해 메시지 길이값을 bitrate의 배수로 보정해야 한다. 메시지 패딩은 $\text{bitrate}(r)$ 과 메시지 길이 M 에 대하여 다음 연산을 통해 패딩이 이뤄진다.

$$1||0^j||1, (j = (-M-2) \bmod r)$$

3. 소스코드

본 문서에서는 SHA3의 SHA3-224, SHA3-256, SHA3-384, SHA3-512 4개의 해시함수와 SHAKE128, SHAKE256 2개의 확장 가능한 출력함수 소스코드 구현에 대해 설명한다. 총 6개의 함수는 C/C++, Java, JSP, ASP, PHP로 구현되었으며, 각 함수 API에 대한 설명 및 동작 방법에 대하여 설명한다.

SHA3 소스코드는 다음과 같이 구성되어 있다.

- SHA3의 C/C++ 소스코드
- SHA3의 Java 소스코드
- SHA3의 JSP 소스코드
- SHA3의 ASP 소스코드
- SHA3의 PHP 소스코드

	동작환경
C/C++	Windows
	Linux
Java	Windows
	Linux
JSP	Apache Tomcat 9.0.19
ASP	Windows10/IIS(Version 10.0.17763.1) .NET v4.5
PHP	PHP Version 7.3.5

< 소스코드 별 동작환경 >

모든 소스코드는 32비트/64비트 운영체제에서 모두 동작한다.

4. 응용 프로그램

Windows, Linux 등 다양한 운영체제 환경에서 응용 프로그램을 개발과 함께 암호화를 적용할 수 있도록 기본적으로 많이 사용하는 C/C++ 및 Java를 기반으로 SHA-3 해시함수 소스코드를 개발하였다.

가. C/C++

프로젝트 생성 및 소스 추가, 빌드 등 배포되는 소스코드를 이용하여 암호화를 실행하는 방법에 대해서는 Microsoft 社の Visual studio 2019를 활용하여 설명하도록 한다.

1) Windows SHA-3 테스트 소스 실행

Windows 운영체제 환경에서 C/C++ 소스코드를 개발할 경우 다양한 IDE를 활용하여 개발할 수 있다. 본 절에서는 Microsoft 社에서 배포하고 있는 Visual Studio 2019를 활용하여 소스코드를 사용하는 방법을 설명한다. Visual Studio 2019가 아닌 다른 IDE를 활용하여 개발하는 내용은 생략하나, 이와 유사한 방법을 활용하여 개발할 수 있다.



Visual Studio를 실행하여 [파일]에서 [새로만들기]->[프로젝트]를 클릭하여 "콘솔 앱"을 선택한다. 이름에는 프로젝트명을 입력하고 위치에는 생성시키고자 하는 곳의 위치를 지정한다.

새 프로젝트 만들기

최근 프로젝트 템플릿(R)

최근에 액세스한 템플릿 목록이 여기에 표시됩니다.

템플릿 검색(Alt+S) 🔍

언어(L) ▾

플랫폼(P) ▾

프로젝트 형식(T) ▾

필터링 기준: Windows

필터 지우기

콘솔 앱
Windows 터미널에서 코드를 실행합니다. 기본적으로 "Hello World"를 출력합니다.
C++ Windows 콘솔

Windows 데스크톱 마법사
마법사를 사용하여 고유한 Windows 앱을 만드세요.
C++ Windows 데스크톱 콘솔 라이브러리

Windows 데스크톱 애플리케이션
Windows에서 실행되는 그래픽 사용자 인터페이스를 사용하는 애플리케이션용 프로젝트입니다.
C++ Windows 데스크톱

공유 항목 프로젝트
공유 항목 프로젝트는 여러 프로젝트 간에 파일을 공유하는 데 사용됩니다.
C++ Windows Android iOS Linux 데스크톱 콘솔 라이브러리 UWP 게임 모바일

콘솔 앱(.NET Framework)
명령줄 애플리케이션을 만드는 프로젝트입니다.
C# Windows 콘솔

뒤로(B)

다음(N)

생성된 프로젝트는 미리 컴파일된 헤더를 사용하도록 구성된 기본 파일들도 함께 생성된다. 개발환경에 따라 미리 컴파일된 헤더를 사용할 경우와 그렇지 않은 경우는 상이하므로 적절한 환경 설정을 해야 한다.

새 프로젝트 구성

콘솔 앱 C++ Windows 콘솔

프로젝트 이름(N)

ConsoleApplication1

위치(L)

C:\Users\KISA\source\repos

솔루션 이름(M) ?

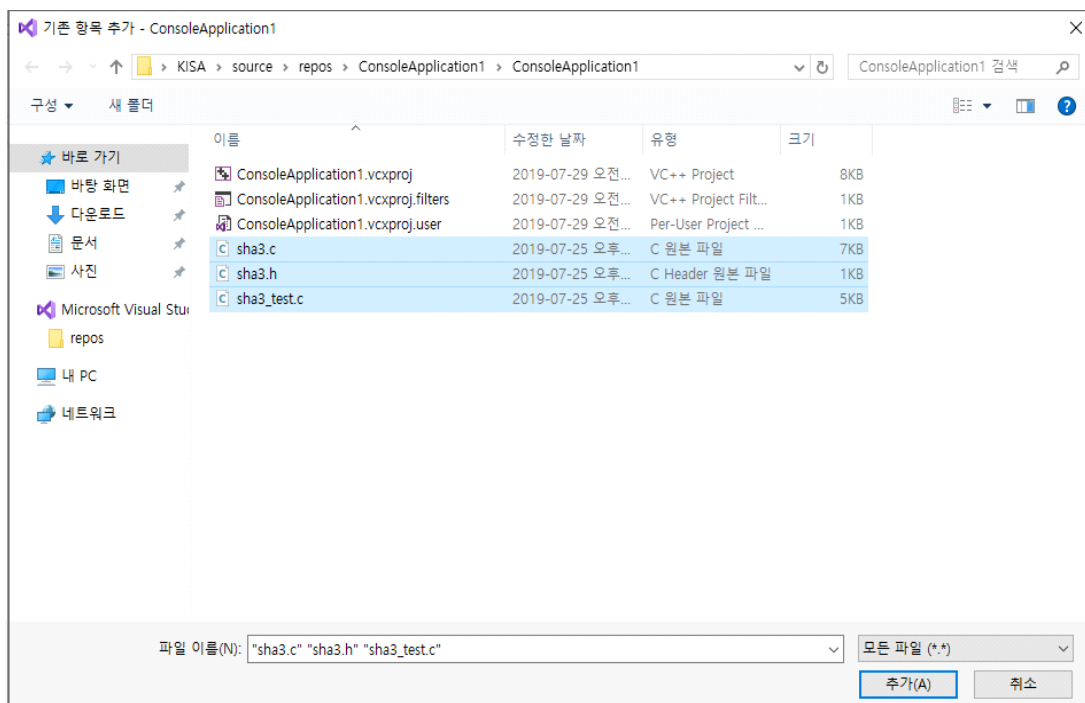
ConsoleApplication1

☐ 솔루션 및 프로젝트를 같은 디렉터리에 배치(D)

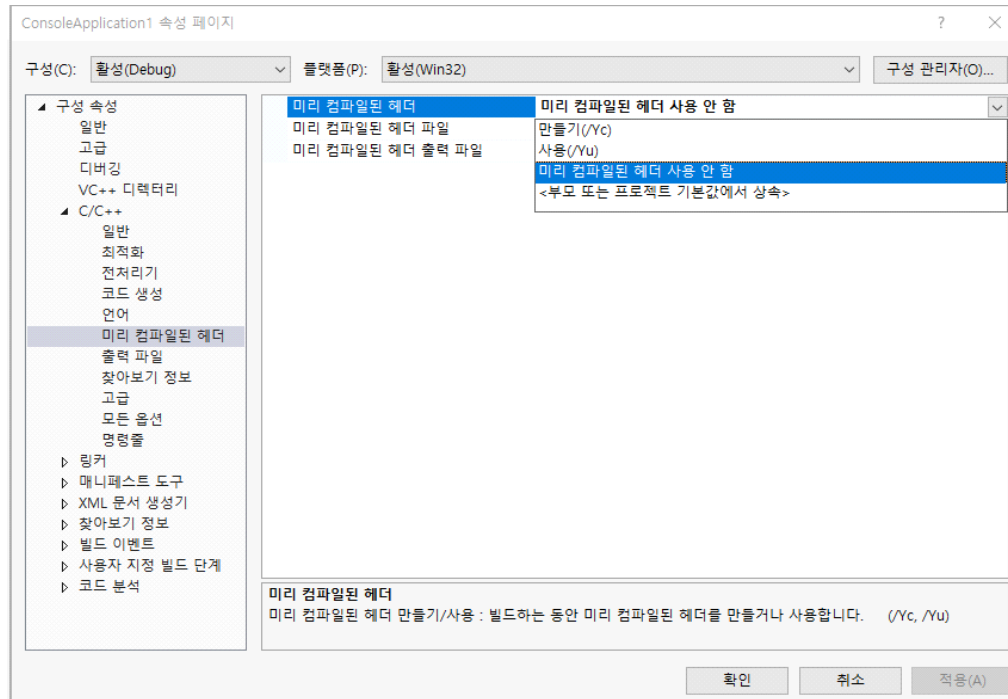
뒤로(B)

만들기(C)

본 설명에서는 기본 생성된 파일을 사용하지 않고 배포된 파일을 사용하는 것을 기준으로 설명한다. 배포된 파일을 추가하기 위해서는 "솔루션 탐색기"에서 프로젝트를 우클릭한 뒤 [추가]->[기준 항목]을 선택한 후, 배포된 소스코드와 헤더파일을 추가한다.



프로젝트 속성 창이 열리면 좌측 트리에서 [C/C++]->[미리 컴파일된 헤더]을 클릭한다. [미리 컴파일된 헤더]에서 "미리 컴파일된 헤더 사용 안 함"을 선택한다.



위와 같이 설정이 완료된 이후, 프로젝트를 빌드 한 뒤 테스트 소스를 실행한다.

```

Microsoft Visual Studio 디버그 콘솔

SHA3 ObIt Message Test!
sha3-224 :
6B 4E 03 42 36 67 DB B7 3B 6E 15 45 4F 0E B1 AB
04 59 7F 9A 1B 07 8E 3F 5B 5A 6B C7

sha3-256 :
A7 FF 06 F8 BF 1E D7 66 51 C1 47 56 A0 61 D6 62
F5 80 FF 4D E4 3B 49 FA 82 D8 0A 4B 80 F8 43 4A

sha3-384 :
0C 63 A7 5B 84 5E 4F 7D 01 10 7D 85 2E 4C 24 85
C5 1A 50 AA AA 94 FC 61 99 5E 71 B8 EE 98 3A 2A
C3 71 38 31 26 4A DB 47 FB 6B D1 E0 58 D5 F0 04

sha3-512 :
A6 9F 73 0C A2 3A 9A C5 C8 B5 67 DC 18 5A 75 6E
97 C9 82 16 4F E2 58 59 E0 D1 DC C1 47 5C 80 A6
15 B2 12 3A F1 F5 F9 4C 11 E3 E9 40 2C 3A C5 58
F5 00 19 9D 95 B6 D3 E3 01 75 85 86 28 1D CD 26

shake128 :
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 8E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C 80 FC A9 76 7B E1 FD A6 94 19 DF
69 27 E9 DF 07 34 8B 19 66 91 AB AE B5 80 B3 2D
EF 58 53 8B 8D 23 F8 77 32 EA 63 B0 2B 4F A0 F4
87 33 60 E2 84 19 28 CD 60 DD 4C EE 8C CD D4 C8
22 A9 61 88 D0 32 67 5C 8A C8 50 93 3C 7A FF 15
33 B9 4C 83 4A DB B6 9C 61 15 BA D4 B9 2D B6 19
F9 0B 0C DF 8A 7B 9C 26 40 29 AC 18 56 70 B8 3F
28 01 F2 F4 E3 F7 0C 59 3E A3 AE EB 61 3A 7F 1B
1D E3 3F D7 50 81 F5 92 30 5F 2E 45 26 ED 00 96
31 B1 09 58 F4 64 DB 89 F3 1B A0 10 25 0F DA 7F
13 68 EC 29 67 FC 84 EF 2A E9 AF F2 68 E0 B1 70
0A FF 06 82 0B 32 3A 3D 91 71 35 F2 DF F2 EE 06
8F E7 2B 31 24 72 1D 4A 26 00 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 DB 03 55 D4 85 E9 F5 1D D0 B5 E9
08 3C D0 5F 8C E8 03 AA 62 B8 D8 54 D8 53 D0 C2
8D 0F F2 73 09 FE B6 73 FA D8 B2 D4 55 76 D0 C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C 9E 27 5D A8
5E E2 14 3F 1A F1 8D 47 EF DD C4 C7 B7 06 5E 34
5D B9 3C 39 36 8E A3 23 49 1C C8 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B8 B2 15 3D 20 41 D2 06 B4
43 E4 1B 45 A6 53 F2 A5 C4 A9 2C 1A D0 54 46 12
DD A2 52 98 33 46 2B 71 A4 1A 45 BE 97 29 0B 6F
  
```

2) Linux SHA-3 테스트 소스 실행

Linux 운영체제 환경에서 C/C++ 소스코드를 개발하는 방법 역시 다양하다. Windows와 달리 Linux에서는 운영체제에 기본 개발환경이 갖춰진 경우가 일반적이다. 따라서 각 Linux 운영체제의 터미널 또는 콘솔에서 간단한 명령어로도 C/C++ 소스코드를 활용할 수 있다. 본 절에서는 Linux 배포판 중 하나인 Ubuntu 18.04 환경에서 소스코드를 활용하는 방법을 설명한다.

Download Ubuntu Desktop

Ubuntu 18.04.1 LTS

Download the latest LTS version of Ubuntu, for desktop PCs and laptops. LTS stands for long-term support — which means five years, until April 2023, of free security and maintenance updates, guaranteed.

[Ubuntu 18.04 LTS release notes](#)

Recommended system requirements:

- ✓ 2 GHz dual core processor or better
- ✓ 2 GB system memory
- ✓ 25 GB of free hard drive space
- ✓ Either a DVD drive or a USB port for the installer media
- ✓ Internet access is helpful

Download

For other versions of Ubuntu Desktop including torrents, the network installer, a list of local mirrors, and past releases [see our alternative downloads](#).

Ubuntu 18.04 버전을 내려받은 후 설치하면 아래와 같이 환경 정보를 확인할 수 있다.

```
kisa@ubuntu: ~/KISA/SHA3/[01] C-C++
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
kisa@ubuntu:[01] C-C++$ uname -a
Linux ubuntu 5.0.0-23-generic #24~18.04.1-Ubuntu SMP Mon Jul 29 16:12:28 UTC 201
9 x86_64 x86_64 x86_64 GNU/Linux
kisa@ubuntu:[01] C-C++$ gcc --version
gcc (Ubuntu 7.4.0-1ubuntu1~18.04.1) 7.4.0
Copyright (C) 2017 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

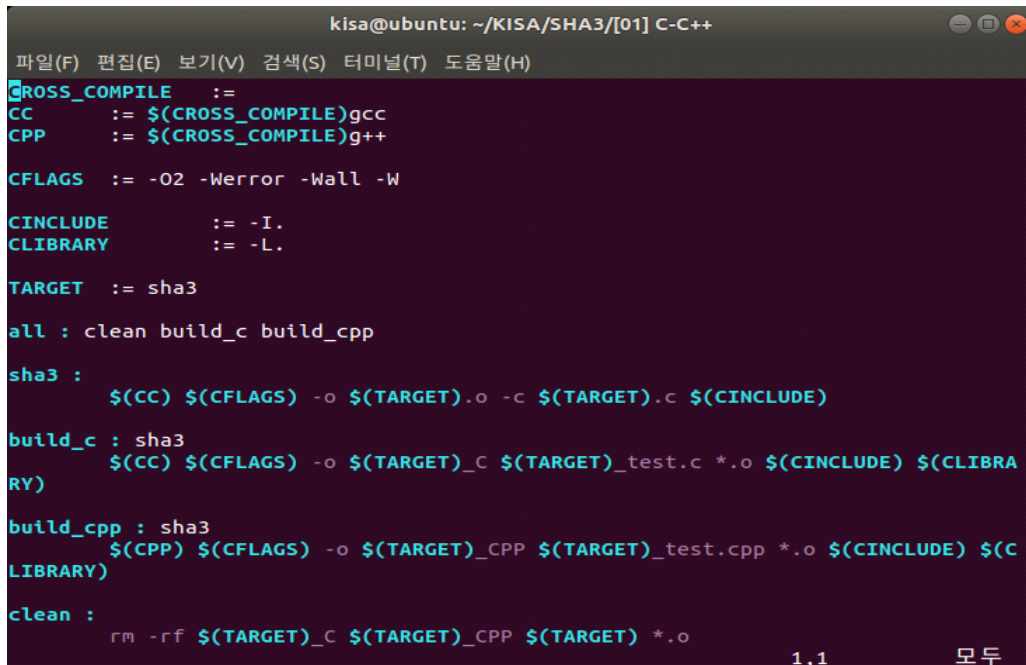
kisa@ubuntu:[01] C-C++$ g++ --version
g++ (Ubuntu 7.4.0-1ubuntu1~18.04.1) 7.4.0
Copyright (C) 2017 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

kisa@ubuntu:[01] C-C++$ make --version
GNU Make 4.1
x86_64-pc-linux-gnu 빌드
Copyright (C) 1988-2014 Free Software Foundation, Inc.
라이선스 GPLv3+: GNU GPL 버전 3 또는 이후 <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
kisa@ubuntu:[01] C-C++$
```

간혹, minimal version을 설치한 경우 위와 같은 정보를 확인할 수 없다. 그런 경우 아래 명령어를 통해 개발환경을 구축할 수 있다.

```
: $ sudo apt install build-essential -y
```

위 명령어를 통해 위 개발환경이 구축된 뒤 "gcc" 또는 "g++" 명령어를 활용하여 배포된 소스코드를 활용할 수 있다. Makefile을 작성하여 "make" 명령어로 손쉽게 개발할 수 있다. 아래는 Makefile의 예이다.



```
kisa@ubuntu: ~/KISA/SHA3/[01] C-C++
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
CROSS_COMPILE :=
CC := $(CROSS_COMPILE)gcc
CPP := $(CROSS_COMPILE)g++

CFLAGS := -O2 -Werror -Wall -W

CINCLUDE := -I.
CLIBRARY := -L.

TARGET := sha3

all : clean build_c build_cpp

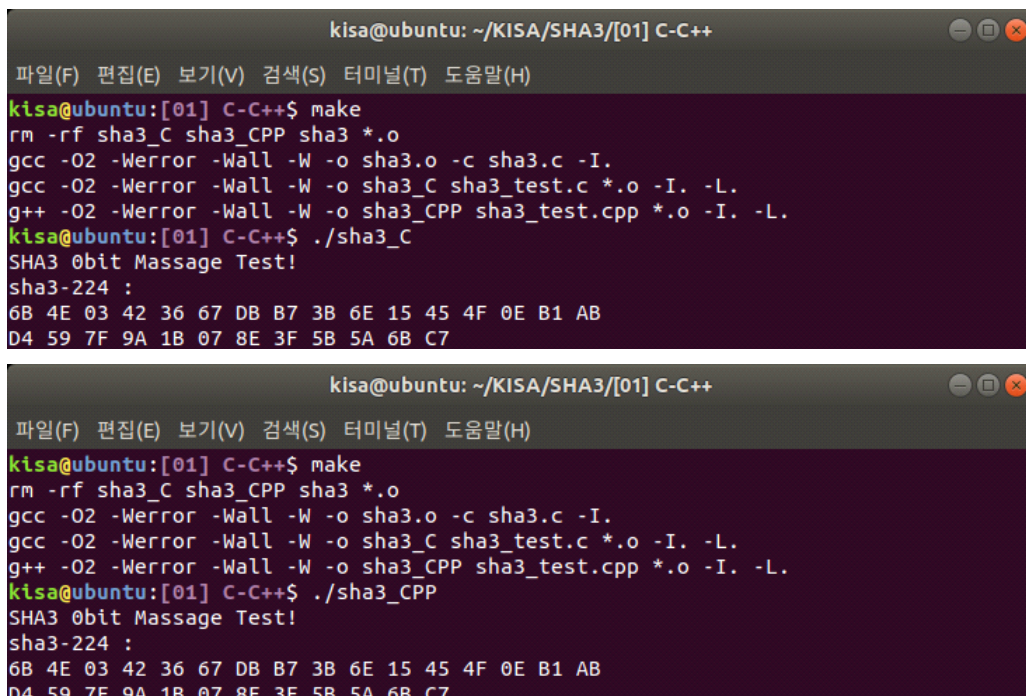
sha3 :
    $(CC) $(CFLAGS) -o $(TARGET).o -c $(TARGET).c $(CINCLUDE)

build_c : sha3
    $(CC) $(CFLAGS) -o $(TARGET)_C $(TARGET)_test.c *.o $(CINCLUDE) $(CLIBRARY)

build_cpp : sha3
    $(CPP) $(CFLAGS) -o $(TARGET)_CPP $(TARGET)_test.cpp *.o $(CINCLUDE) $(CLIBRARY)

clean :
    rm -rf $(TARGET)_C $(TARGET)_CPP $(TARGET) *.o
1,1 모두
```

"make" 명령어를 통해 C와 C++로 컴파일된 결과물을 얻을 수 있다. "sha3_C", "sha3_CPP" 각각 C와 C++로 컴파일된 결과물이다.



```
kisa@ubuntu: ~/KISA/SHA3/[01] C-C++
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
kisa@ubuntu:[01] C-C++$ make
rm -rf sha3_C sha3_CPP sha3 *.o
gcc -O2 -Werror -Wall -W -o sha3.o -c sha3.c -I.
gcc -O2 -Werror -Wall -W -o sha3_C sha3_test.c *.o -I. -L.
g++ -O2 -Werror -Wall -W -o sha3_CPP sha3_test.cpp *.o -I. -L.
kisa@ubuntu:[01] C-C++$ ./sha3_C
SHA3 0bit Message Test!
sha3-224 :
6B 4E 03 42 36 67 DB B7 3B 6E 15 45 4F 0E B1 AB
D4 59 7F 9A 1B 07 8E 3F 5B 5A 6B C7

kisa@ubuntu: ~/KISA/SHA3/[01] C-C++
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
kisa@ubuntu:[01] C-C++$ make
rm -rf sha3_C sha3_CPP sha3 *.o
gcc -O2 -Werror -Wall -W -o sha3.o -c sha3.c -I.
gcc -O2 -Werror -Wall -W -o sha3_C sha3_test.c *.o -I. -L.
g++ -O2 -Werror -Wall -W -o sha3_CPP sha3_test.cpp *.o -I. -L.
kisa@ubuntu:[01] C-C++$ ./sha3_CPP
SHA3 0bit Message Test!
sha3-224 :
6B 4E 03 42 36 67 DB B7 3B 6E 15 45 4F 0E B1 AB
D4 59 7F 9A 1B 07 8E 3F 5B 5A 6B C7
```

3) C/C++ 코드 구성

파일명	내용
sha3.h	SHA-3 함수 정의
sha3.c	SHA-3 함수 구현
sha3_test.c	SHA-3 테스트 함수 구현(C언어)
sha3_test.cpp	SHA-3 테스트 함수 구현(C++언어)

SHA-3 소스코드는 C와 C++ 모두 사용 가능하다. 개발시 sha3.c와 sha3.h를 발췌하여 편리하게 SHA-3를 호출하여 사용할 수 있는 구조이며, 사용방법은 sha3_test.c 또는 sha3_test.cpp를 참고하면 된다.

4) SHA-3 소스코드 인터페이스

SHA-3 소스코드는 최상위 API sha3_hash 함수를 통해 해시값을 생성하며, sha3_hash함수는 init, update, final 단계를 거친다. init 단계에서는 SHA-3의 보안 매개변수를 설정하고 내부 state를 초기화하는 단계를 수행하며 update에서는 SHA-3의 Sponge 구조의 Absorbing(흡수과정)이 수행된다. 마지막 final 과정에서 Squeezing(압착과정)을 통해 최종 해시값을 얻을 수 있다.

```
int sha3_hash(uint8_t* output, int outLen, uint8_t* input, int inLen, int bitSize, int useSHAKE);
```

매개변수 :

- output SHA3 해시값을 출력할 버퍼
- outLen 해시값 출력 길이(바이트 단위)
- input SHA3 해시값을 계산할 메시지
- inLen 메시지의 길이(바이트 단위)
- bitSize SHA3 보안매개변수 설정
 - SHA3-224 = 224
 - SHA3-256 = 256
 - SHA3-384 = 384
 - SHA3-512 = 512
 - SHAKE128 = 128
 - SHAKE256 = 256
- useSHAKE
 - SHAKE를 사용할 경우 SHA3_SHAKE_USE(=1)을 설정
 - SHAKE를 사용하지 않을 경우 SHA3_SHAKE_NONE(=0)을 설정

반환값 :

- SHA3_OK 정상적으로 수행한 경우 SHA3_OK(=0)을 반환

참 고 :

SHA3 통합함수로서 SHA3-224,256,384,512와 SHAKE128,256에 따라 입력값과 매개변수를 설정하여 최종 해시값을 얻을 수 있다. SHA3-224,256,384,512와 SHAKE128,256에 따라 출력길이가 다르므로 적절한 출력 길이값을 입력해야 한다.

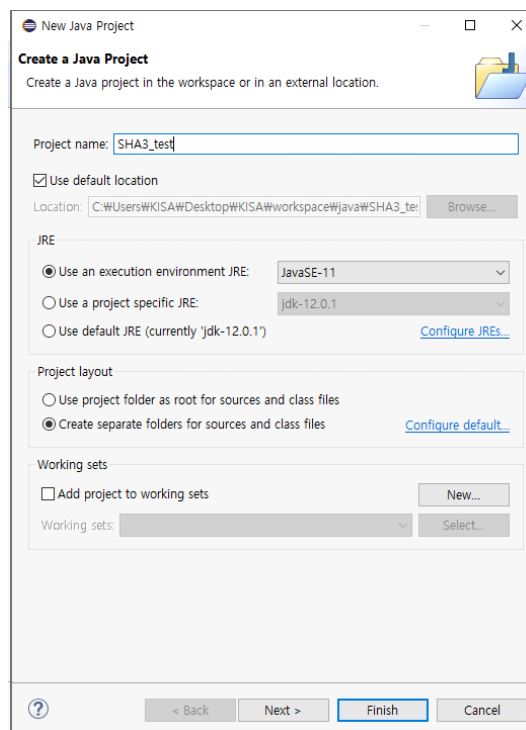
나. Java

1) Windows SHA-3 테스트 소스 실행

Windows 운영체제 환경에서 Java 소스코드를 개발하는데에는 다양한 IDE를 활용하여 개발할 수 있다. 본 절에서는 Eclipse PHOTON 무료 배포버전을 활용하여 소스코드를 사용하는 방법을 설명한다. Java는 기본적으로 개발환경에 Java JDK를 설치하여 개발환경을 구축해야 하나, 이에 대한 방법은 생략한다.

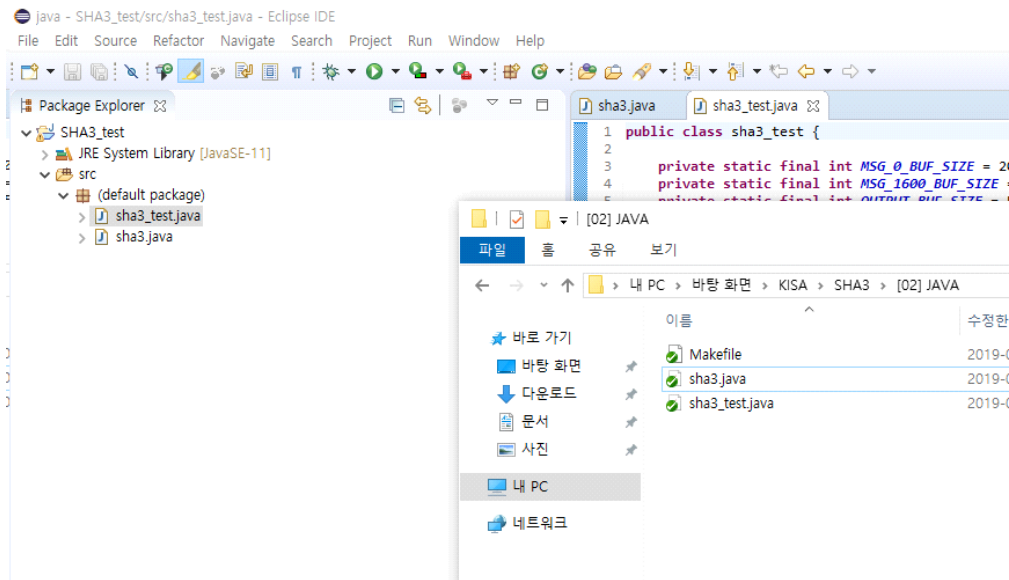


Eclipse Photon을 실행하여 [File]에서 [New]->[Java Project]를 클릭하여 프로젝트명을 기입하고 개발환경에 적절한 Java JRE를 선택하여 프로젝트를 생성한다.

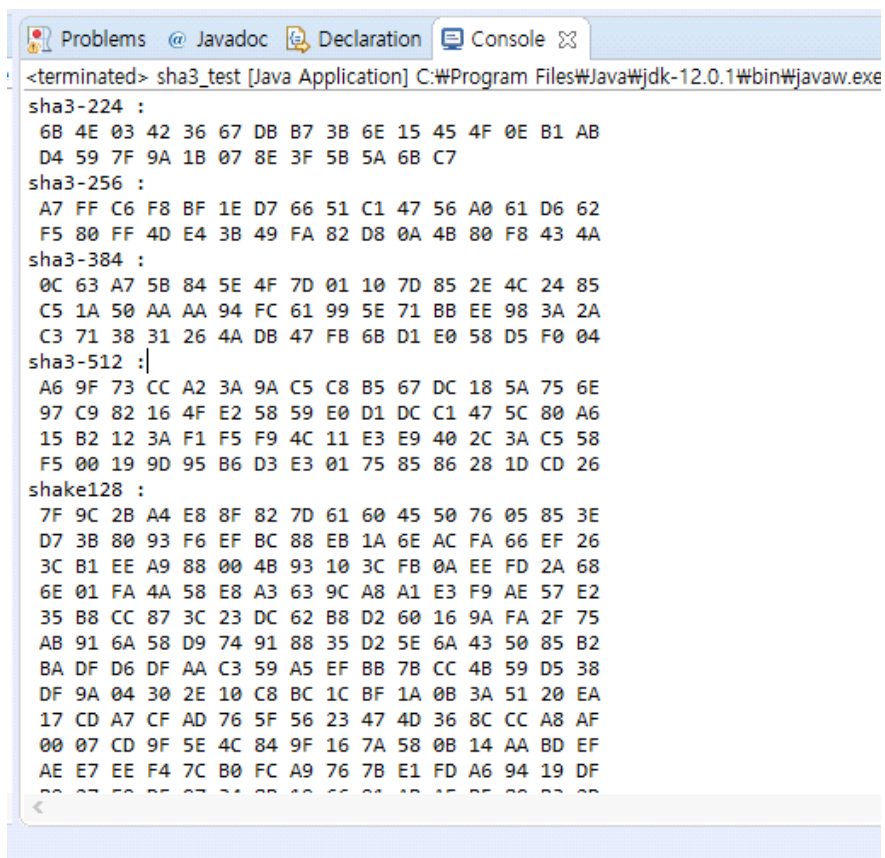


생성된 프로젝트는 기본 파일을 함께 생성된다. 개발환경에 따라 필요한 파일을 사용하도록 설정한다.

본 설명에서는 기본 생성된 파일을 생성하지 않고 배포된 파일을 사용하는 것을 기준으로 설명한다. Eclipse에서 "Package Explorer"의 src에 배포된 소스코드를 추가한다. 이후 개발환경에 맞춰서 개발을 진행한다.



이클립스에서 추가한 소스코드를 빌드한 후 실행한다.



2) Linux SHA-3 테스트 소스 실행

Linux 운영체제 환경에서 C/C++ 소스코드를 개발하는 방법 역시 다양하다. Windows와 달리 Linux에서는 운영체제에 기본 개발환경이 갖춰진 경우가 일반적이다. 따라서 각 Linux 운영체제의 터미널 또는 콘솔에서 간단한 명령어로도 C/C++ 소스코드를 활용할 수 있다. 본 절에서는 Linux 배포판 중 하나인 Ubuntu 18.04 환경에서 소스코드를 활용하는 방법을 설명한다.

Download Ubuntu Desktop

Ubuntu 18.04.1 LTS

Download the latest [LTS](#) version of Ubuntu, for desktop PCs and laptops. LTS stands for long-term support — which means five years, until April 2023, of free security and maintenance updates, guaranteed.

[Ubuntu 18.04 LTS release notes](#)

Recommended system requirements:

- ✓ 2 GHz dual core processor or better
- ✓ 2 GB system memory
- ✓ 25 GB of free hard drive space
- ✓ Either a DVD drive or a USB port for the installer media
- ✓ Internet access is helpful

[Download](#)

For other versions of Ubuntu Desktop including torrents, the network installer, a list of local mirrors, and past releases [see our alternative downloads](#).

Ubuntu 18.04 버전을 내려받은 후 설치하면 아래와 같이 환경 정보를 확인할 수 있다.

```
kisa@ubuntu: ~/KISA/SHA3/[02] JAVA
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
kisa@ubuntu:[02] JAVA$ uname -a
Linux ubuntu 5.0.0-23-generic #24~18.04.1-Ubuntu SMP Mon Jul 29 16:12:28 UTC 201
9 x86_64 x86_64 x86_64 GNU/Linux
kisa@ubuntu:[02] JAVA$ java --version
openjdk 11.0.4 2019-07-16
OpenJDK Runtime Environment (build 11.0.4+11-post-Ubuntu-1ubuntu218.04.3)
OpenJDK 64-Bit Server VM (build 11.0.4+11-post-Ubuntu-1ubuntu218.04.3, mixed mod
e, sharing)
kisa@ubuntu:[02] JAVA$ javac --version
javac 11.0.4
kisa@ubuntu:[02] JAVA$ make --version
GNU Make 4.1
x86_64-pc-linux-gnu 빌드
Copyright (C) 1988-2014 Free Software Foundation, Inc.
라이선스 GPLv3+: GNU GPL 버전 3 또는 이후 <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
kisa@ubuntu:[02] JAVA$
```

Ubuntu 18.04에서는 기본적으로 Java 개발환경이 구축되어 있지 않다. 하지만 openJDK는 Ubuntu의 패키지 설치로 간편하게 설치 가능하다.

SHA-3 소스코드는 개발시 sha3.java를 발췌하여 편리하게 sha3를 호출하여 사용할 수 있는 구조이며, 사용방법은 sha3_test.java를 참고하면 된다.

1) SHA-3 소스코드 인터페이스

SHA-3 소스코드는 최상위 API sha3_hash 함수를 통해 해시값을 생성하며, sha3_hash함수는 init, update, final 단계를 거친다. init 단계에서는 SHA-3의 보안 매개변수를 설정하고 내부 state를 초기화하는 단계를 수행하며 update에서는 SHA-3의 Sponge 구조의 Absorbing(흡수과정)이 수행된다. 마지막 final 과정에서 Squeezing(압착과정)을 통해 최종 해시값을 얻을 수 있다.

```
public final int sha3_hash(uint8_t* output, int outLen, uint8_t* input, int inLen,
                           int bitSize, int useSHAKE);
```

매개변수 :

- output SHA3 해시값을 출력할 버퍼
- outLen 해시값 출력 길이(바이트 단위)
- input SHA3 해시값을 계산할 메시지
- inLen 메시지의 길이(바이트 단위)
- bitSize SHA3 보안매개변수 설정
 - SHA3-224 = 224
 - SHA3-256 = 256
 - SHA3-384 = 384
 - SHA3-512 = 512
 - SHAKE128 = 128
 - SHAKE256 = 256
- useSHAKE
 - SHAKE를 사용할 경우 SHA3_SHAKE_USE(=1)을 설정
 - SHAKE를 사용하지 않을 경우 SHA3_SHAKE_NONE(=0)을 설정

반환값 :

- SHA3_OK
 - 정상적으로 수행한 경우 SHA3_OK(=0)을 반환

참 고 :

SHA3 통합함수로서 SHA3-224,256,384,512와 SHAKE128,256에 따라 입력값과 매개변수를 설정하여 최종 해시값을 얻을 수 있다. SHA3-224,256,384,512와 SHAKE128,256에 따라 출력길이가 다르므로 적절한 출력 길이값을 입력해야 한다.

5. 웹 프로그램

Data Base, Homepage 등 다양한 Web Service 환경에서 전송·저장되는 구간의 암호화를 적용할 수 있도록 국산암호 소스코드를 개발하였다. 기본적으로 많이 사용하는 ASP, JSP, PHP를 기반으로 한다.

가. ASP

소스 활용 등 배포되는 소스코드를 이용하여 암호화를 실행하는 방법에 대해서는 간단한 에디터 상태에서 설명하도록 한다. 단, 웹 개발환경 구축에 대한 설명은 생략하기로 한다.

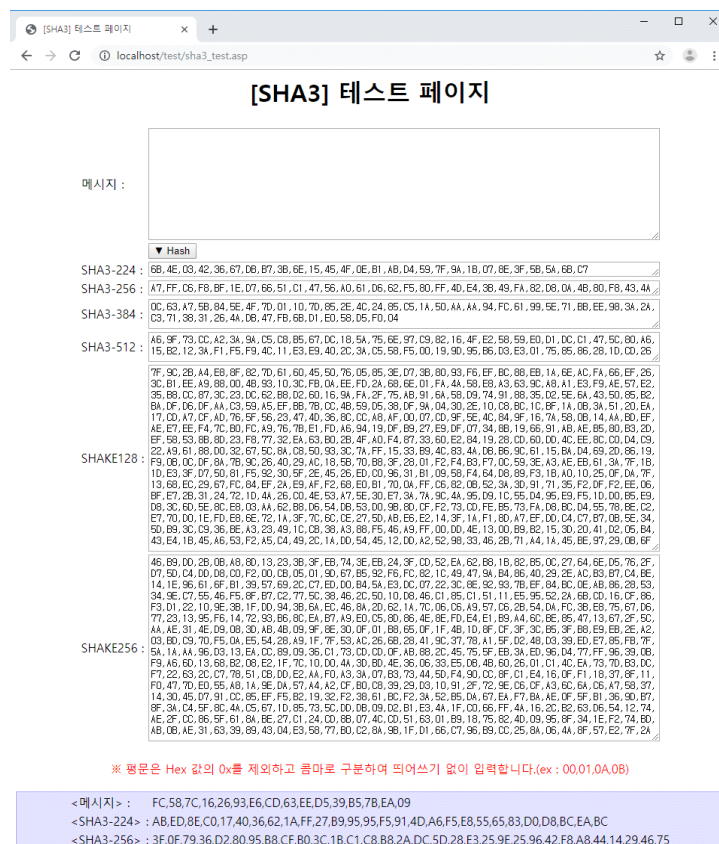
ASP로 개발된 웹 프로그램 소스코드에 배포된 파일을 포함시킨다.

```

sha3_test.asp
[03] ASP > sha3_test.asp
1 <!--#include file="sha3.asp"-->
2 <%
3   dim msg
4   dim sha3_224
5   dim sha3_256
6   dim sha3_384
7   dim sha3_512

```

sha3.asp를 포함시킨 페이지를 브라우저에서 로드하면 다음과 같이 실행된다.



1) ASP 코드 구성

파일명	내용
sha3.asp	SHA3 함수 구현(ASP)

SHA-3 소스코드는 개발시 sha3.asp를 발췌하여 편리하게 sha3를 호출하여 사용할 수 있는 구조이며, 사용방법은 sha3_test.asp를 참고하면 된다.

2) SHA-3 소스코드 인터페이스

SHA-3 소스코드는 최상위 API sha3_hash 함수를 통해 해시값을 생성하며, sha3_hash함수는 init, update, final 단계를 거친다. init 단계에서는 SHA-3의 보안 매개변수를 설정하고 내부 state를 초기화하는 단계를 수행하며 update에서는 SHA-3의 Sponge 구조의 Absorbing(흡수과정)이 수행된다. 마지막 final 과정에서 Squeezing(압착과정)을 통해 최종 해시값을 얻을 수 있다.

```
public function sha3_hash(byref output, outLen, input, inLen, bitSize, useSHAKE);
```

매개변수 :

- output SHA3 해시값을 출력할 버퍼
- outLen 해시값 출력 길이(바이트 단위)
- input SHA3 해시값을 계산할 메시지
- inLen 메시지의 길이(바이트 단위)
- bitSize SHA3 보안매개변수 설정
 - SHA3-224 = 224
 - SHA3-256 = 256
 - SHA3-384 = 384
 - SHA3-512 = 512
 - SHAKE128 = 128
 - SHAKE256 = 256
- useSHAKE
 - SHAKE를 사용할 경우 SHA3_SHAKE_USE(=1)을 설정
 - SHAKE를 사용하지 않을 경우 SHA3_SHAKE_NONE(=0)을 설정

반환값 :

- SHA3_OK
 - 정상적으로 수행한 경우 SHA3_OK(=0)을 반환

참 고 :

SHA3 통합함수로서 SHA3-224,256,384,512와 SHAKE128,256에 따라 입력값과 매개변수를 설정하여 최종 해시값을 얻을 수 있다. SHA3-224,256,384,512와 SHAKE128,256에 따라 출력길이가 다르므로 적절한 출력 길이값을 입력해야 한다.

1) PHP 코드 구성

파일명	내용
sha3.php	SHA3 함수 구현(PHP)

SHA-3 소스코드는 개발시 sha3.php를 발췌하여 편리하게 sha3를 호출하여 사용할 수 있는 구조이며, 사용방법은 sha3_test.php를 참고하면 된다.

2) SHA-3 소스코드 인터페이스

SHA-3 소스코드는 최상위 API sha3_hash 함수를 통해 해시값을 생성하며, sha3_hash함수는 init, update, final 단계를 거친다. init 단계에서는 SHA-3의 보안 매개변수를 설정하고 내부 state를 초기화하는 단계를 수행하며 update에서는 SHA-3의 Sponge 구조의 Absorbing(흡수과정)이 수행된다. 마지막 final 과정에서 Squeezing(압착과정)을 통해 최종 해시값을 얻을 수 있다.

```
static function sha3_hash(&$output, $outLen, $input, $inLen, $bitSize, $useSHAKE);
```

매개변수 :

- output SHA3 해시값을 출력할 버퍼
- outLen 해시값 출력 길이(바이트 단위)
- input SHA3 해시값을 계산할 메시지
- inLen 메시지의 길이(바이트 단위)
- bitSize SHA3 보안매개변수 설정
 - SHA3-224 = 224
 - SHA3-256 = 256
 - SHA3-384 = 384
 - SHA3-512 = 512
 - SHAKE128 = 128
 - SHAKE256 = 256
- useSHAKE
 - SHAKE를 사용할 경우 SHA3_SHAKE_USE(=1)을 설정
 - SHAKE를 사용하지 않을 경우 SHA3_SHAKE_NONE(=0)을 설정

반환값 :

- SHA3_OK
 - 정상적으로 수행한 경우 SHA3_OK(=0)을 반환

참 고 :

SHA3 통합함수로서 SHA3-224,256,384,512와 SHAKE128,256에 따라 입력값과 매개변수를 설정하여 최종 해시값을 얻을 수 있다. SHA3-224,256,384,512와 SHAKE128,256에 따라 출력길이가 다르므로 적절한 출력 길이값을 입력해야 한다.

1) JSP 코드 구성

파일명	내용
sha3.jsp	SHA3 함수 구현(JSP)

SHA3 소스코드는 개발시 sha3.jsp를 발췌하여 편리하게 sha3를 호출하여 사용할 수 있는 구조이며, 사용방법은 sha3_test.jsp를 참고하면 된다.

2) SHA-3 소스코드 인터페이스

SHA-3 소스코드는 최상위 API sha3_hash 함수를 통해 해시값을 생성하며, sha3_hash함수는 init, update, final 단계를 거친다. init 단계에서는 SHA-3의 보안 매개변수를 설정하고 내부 state를 초기화하는 단계를 수행하며 update에서는 SHA-3의 Sponge 구조의 Absorbing(흡수과정)이 수행된다. 마지막 final 과정에서 Squeezing(압착과정)을 통해 최종 해시값을 얻을 수 있다.

```
public static function int sha3_hash(byte[] output, int outLen, byte[] input, int inLen,
                                     int bitSize, int useSHAKE);
```

매개변수 :

- output SHA3 해시값을 출력할 버퍼
- outLen 해시값 출력 길이(바이트 단위)
- input SHA3 해시값을 계산할 메시지
- inLen 메시지의 길이(바이트 단위)
- bitSize SHA3 보안매개변수 설정
 - SHA3-224 = 224
 - SHA3-256 = 256
 - SHA3-384 = 384
 - SHA3-512 = 512
 - SHAKE128 = 128
 - SHAKE256 = 256
- useSHAKE
 - SHAKE를 사용할 경우 SHA3_SHAKE_USE(=1)을 설정
 - SHAKE를 사용하지 않을 경우 SHA3_SHAKE_NONE(=0)을 설정

반환값 :

- SHA3_OK
 - 정상적으로 수행한 경우 SHA3_OK(=0)을 반환

참 고 :

SHA3 통합함수로서 SHA3-224,256,384,512와 SHAKE128,256에 따라 입력값과 매개변수를 설정하여 최종 해시값을 얻을 수 있다. SHA3-224,256,384,512와 SHAKE128,256에 따라 출력길이가 다르므로 적절한 출력 길이값을 입력해야 한다.

	68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0
해시값(H)	14,08,78,8C,06,6F,D9,7A,90,82,0B,47,D4,B0,EA,BF, E1,6B,BB,56,DF,27,77,C1,F6,B3,F8,17

< 데이터 4 - 3,200비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A
해시값(H)	40,4F,6B,0D,87,D3,81,05,23,B5,F1,67,F5,A6,48,85, 59,38,30,19,C3,25,0F,F4,85,E6,59,40

< 데이터 5 - 4,800비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59
해시값(H)	05,1B,D1,C0,4C,D6,E8,7A,66,2A,F1,7B,55,86,05,62, 1F,65,7B,07,72,1E,A3,F8,3D,5F,3B,CF

< 데이터 6 - 6,400비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59,63,3B,57,09,C5,59,81,F3, 21,DB,8D,62,DD,8C,B1,38,FE,22,D9,4F,D7,98,FF,E6, B9,72,23,4B,FC,24,B0,22,D5,71,33,C9,E2,7B,0F,43, 9E,13,45,2B,17,FC,DC,5F,55,DB,BE,FF,3D,25,49,C8, E4,D6,D3,D6,8A,4F,28,C3,CD,77,D4,B6,73,4F,E3,BB,
--------	--

	31,79,EE,11,30,94,1A,D1,AF,F3,84,AD,EC,71,C1,FC, 3B,75,9D,AC,50,57,F6,DA,69,0B,3A,4B,4B,AB,9F,23, 32,C4,3F,5B,E5,BB,C7,53,2B,35,64,E6,DF,CE,26,95, 65,F5,99,70,9A,59,0C,71,4F,E6,32,36,70,71,51,FB, B7,0B,32,07,78,BA,70,5C,6C,04,A4,D9,9E,FB,D8,D4, BE,88,7F,1B,1D,E0,6D,6E,FE,FE,E9,22,DD,23,79,10, F5,DA,F1,AC,08,E8,58,23,03,40,B6,1D,C0,57,DC,84, C8,F9,C8,43,78,81,48,76,40,64,8C,AA,09,CA,33,08
해시값(H)	C5,E3,8D,CC,59,59,B9,BB,81,69,D6,38,DF,94,D8,F7, C1,74,48,AE,9B,5E,E9,50,A7,EF,FB,95

< 데이터 7 - 8,000비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C,
--------	--

	82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59,63,3B,57,09,C5,59,81,F3, 21,DB,8D,62,DD,8C,B1,38,FE,22,D9,4F,D7,98,FF,E6, B9,72,23,4B,FC,24,B0,22,D5,71,33,C9,E2,7B,0F,43, 9E,13,45,2B,17,FC,DC,5F,55,DB,BE,FF,3D,25,49,C8, E4,D6,D3,D6,8A,4F,28,C3,CD,77,D4,B6,73,4F,E3,BB, 31,79,EE,11,30,94,1A,D1,AF,F3,84,AD,EC,71,C1,FC, 3B,75,9D,AC,50,57,F6,DA,69,0B,3A,4B,4B,AB,9F,23, 32,C4,3F,5B,E5,BB,C7,53,2B,35,64,E6,DF,CE,26,95, 65,F5,99,70,9A,59,0C,71,4F,E6,32,36,70,71,51,FB, B7,0B,32,07,78,BA,70,5C,6C,04,A4,D9,9E,FB,D8,D4, BE,88,7F,1B,1D,E0,6D,6E,FE,FE,E9,22,DD,23,79,10, F5,DA,F1,AC,08,E8,58,23,03,40,B6,1D,C0,57,DC,84, C8,F9,C8,43,78,81,48,76,40,64,8C,AA,09,CA,33,08, E7,AE,3A,27,1F,40,4A,6D,33,BE,DE,EA,98,6C,3A,FD, CD,1C,B3,37,4B,93,AA,23,59,D7,37,6E,CD,F3,29,BD, 63,C6,0B,88,19,CA,3E,50,7B,92,0E,B0,6A,DA,AC,AD, BB,A1,4A,9A,AF,62,BB,24,D1,B2,D7,0F,94,08,91,AB, 3D,4E,7C,D6,C7,BD,DF,0D,EC,98,CC,AE,C2,D1,00,4B, 43,24,50,BC,F7,96,E7,35,A1,C3,2E,A2,D9,D5,CA,AE, 42,41,EA,70,28,D3,56,C1,78,36,3F,2A,F9,21,76,CA, 3C,A4,2F,AF,73,47,18,A9,D2,CE,D1,84,FD,3F,27,C1, 82,2D,FB,7C,DC,8F,DE,16,23,08,8F,DB,7E,0A,A4,F5, DB,03,2B,3C,E7,9E,67,58,88,8E,2C,76,28,E9,49,39, 3A,8B,F5,5D,C4,89,F8,9F,A6,5B,8B,84,B0,41,62,DE, BA,E2,0D,EA,78,EA,56,A4,4B,0D,CE,48,08,01,67,34, 21,C3,FB,FD,9E,A9,01,01
해시값(H)	91,2A,DC,DB,53,12,2D,0E,DB,16,A3,AB,EA,44,D4,1F, BC,16,80,DB,62,E0,39,AC,EF,5D,AB,79

< 데이터 4 - 3,200비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A
해시값(H)	A6,5F,67,6B,03,A9,AF,3C,00,33,C6,19,B8,7D,BC,D0, 79,6F,B6,39,C3,E6,64,AB,22,24,99,07,96,7B,F0,CD

< 데이터 5 - 4,800비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73,
--------	--

	85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59
해시값(H)	D4,34,EE,AD,25,7B,A0,49,8D,C9,A6,A6,50,C9,AC,B9, F6,9B,37,D1,37,81,A8,87,53,89,67,51,33,E9,80,C1

< 데이터 6 - 6,400비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73,
--------	--

	85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59,63,3B,57,09,C5,59,81,F3, 21,DB,8D,62,DD,8C,B1,38,FE,22,D9,4F,D7,98,FF,E6, B9,72,23,4B,FC,24,B0,22,D5,71,33,C9,E2,7B,0F,43, 9E,13,45,2B,17,FC,DC,5F,55,DB,BE,FF,3D,25,49,C8, E4,D6,D3,D6,8A,4F,28,C3,CD,77,D4,B6,73,4F,E3,BB, 31,79,EE,11,30,94,1A,D1,AF,F3,84,AD,EC,71,C1,FC, 3B,75,9D,AC,50,57,F6,DA,69,0B,3A,4B,4B,AB,9F,23, 32,C4,3F,5B,E5,BB,C7,53,2B,35,64,E6,DF,CE,26,95, 65,F5,99,70,9A,59,0C,71,4F,E6,32,36,70,71,51,FB, B7,0B,32,07,78,BA,70,5C,6C,04,A4,D9,9E,FB,D8,D4, BE,88,7F,1B,1D,E0,6D,6E,FE,FE,E9,22,DD,23,79,10, F5,DA,F1,AC,08,E8,58,23,03,40,B6,1D,C0,57,DC,84, C8,F9,C8,43,78,81,48,76,40,64,8C,AA,09,CA,33,08
해시값(H)	A2,CF,67,76,FD,69,78,DE,EA,3E,6F,DB,06,05,B7,BA, AE,E2,C1,4D,C3,D0,9A,CA,77,14,5A,71,5C,64,20,76

< 데이터 7 - 8,000비트 >

메시지(M)	<p> B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59,63,3B,57,09,C5,59,81,F3, 21,DB,8D,62,DD,8C,B1,38,FE,22,D9,4F,D7,98,FF,E6, B9,72,23,4B,FC,24,B0,22,D5,71,33,C9,E2,7B,0F,43, 9E,13,45,2B,17,FC,DC,5F,55,DB,BE,FF,3D,25,49,C8, E4,D6,D3,D6,8A,4F,28,C3,CD,77,D4,B6,73,4F,E3,BB, 31,79,EE,11,30,94,1A,D1,AF,F3,84,AD,EC,71,C1,FC, </p>
--------	---

	3B,75,9D,AC,50,57,F6,DA,69,0B,3A,4B,4B,AB,9F,23, 32,C4,3F,5B,E5,BB,C7,53,2B,35,64,E6,DF,CE,26,95, 65,F5,99,70,9A,59,0C,71,4F,E6,32,36,70,71,51,FB, B7,0B,32,07,78,BA,70,5C,6C,04,A4,D9,9E,FB,D8,D4, BE,88,7F,1B,1D,E0,6D,6E,FE,FE,E9,22,DD,23,79,10, F5,DA,F1,AC,08,E8,58,23,03,40,B6,1D,C0,57,DC,84, C8,F9,C8,43,78,81,48,76,40,64,8C,AA,09,CA,33,08, E7,AE,3A,27,1F,40,4A,6D,33,BE,DE,EA,98,6C,3A,FD, CD,1C,B3,37,4B,93,AA,23,59,D7,37,6E,CD,F3,29,BD, 63,C6,0B,88,19,CA,3E,50,7B,92,0E,B0,6A,DA,AC,AD, BB,A1,4A,9A,AF,62,BB,24,D1,B2,D7,0F,94,08,91,AB, 3D,4E,7C,D6,C7,BD,DF,0D,EC,98,CC,AE,C2,D1,00,4B, 43,24,50,BC,F7,96,E7,35,A1,C3,2E,A2,D9,D5,CA,AE, 42,41,EA,70,28,D3,56,C1,78,36,3F,2A,F9,21,76,CA, 3C,A4,2F,AF,73,47,18,A9,D2,CE,D1,84,FD,3F,27,C1, 82,2D,FB,7C,DC,8F,DE,16,23,08,8F,DB,7E,0A,A4,F5, DB,03,2B,3C,E7,9E,67,58,88,8E,2C,76,28,E9,49,39, 3A,8B,F5,5D,C4,89,F8,9F,A6,5B,8B,84,B0,41,62,DE, BA,E2,0D,EA,78,EA,56,A4,4B,0D,CE,48,08,01,67,34, 21,C3,FB,FD,9E,A9,01,01
해시값(H)	72,19,22,28,A5,77,45,69,A8,F2,0D,32,C8,0D,39,70, 52,8F,03,19,90,53,CC,D1,1E,DA,0F,AD,16,6A,30,09

해시값(H)	1A,84,FB,CD,39,AD,31,B1,BF,A5,5D,5F,41,39,FE,1C, 01,C5,89,31,64,51,26,BF,B6,E9,7F,99,8E,F6,78,0C, 4C,4F,03,BA,DC,21,B7,42,5E,F1,0F,4D,F7,72,C7,33
--------	---

< 데이터 4 - 3,200비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A
해시값(H)	CB,EA,7E,19,67,E0,64,E1,E5,67,A1,DE,19,2B,C5,29, 12,83,66,86,71,A9,57,EF,84,D3,EF,EB,0E,42,E8,63, 53,2C,38,3B,E9,56,10,33,A2,8D,5A,A8,B2,4D,C1,83

< 데이터 5 - 4,800비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B,
--------	--

	F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59
해시값(H)	88,F1,A8,CF,2C,EA,AE,E9,43,1D,DB,77,7D,E7,90,32, 6E,13,25,5D,E4,84,EC,FC,77,2C,46,7F,70,95,EB,D9, 94,A2,29,86,45,F5,AC,21,90,06,8E,BF,AD,5D,F8,CD

< 데이터 6 - 6,400비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F,
--------	--

15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B,
 F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E,
 AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59,
 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD,
 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90,
 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68,
 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73,
 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89,
 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85,
 BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B,
 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B,
 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB,
 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7,
 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B,
 D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA,
 ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43,
 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A,
 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9,
 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF,
 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90,
 CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A,
 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8,
 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11,
 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08,
 BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45,
 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C,
 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80,
 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74,
 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9,
 EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C,
 F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7,
 E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4,
 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF,
 80,B7,AF,BA,6E,95,5E,59,63,3B,57,09,C5,59,81,F3,
 21,DB,8D,62,DD,8C,B1,38,FE,22,D9,4F,D7,98,FF,E6,
 B9,72,23,4B,FC,24,B0,22,D5,71,33,C9,E2,7B,0F,43,
 9E,13,45,2B,17,FC,DC,5F,55,DB,BE,FF,3D,25,49,C8,
 E4,D6,D3,D6,8A,4F,28,C3,CD,77,D4,B6,73,4F,E3,BB,
 31,79,EE,11,30,94,1A,D1,AF,F3,84,AD,EC,71,C1,FC,
 3B,75,9D,AC,50,57,F6,DA,69,0B,3A,4B,4B,AB,9F,23,
 32,C4,3F,5B,E5,BB,C7,53,2B,35,64,E6,DF,CE,26,95,
 65,F5,99,70,9A,59,0C,71,4F,E6,32,36,70,71,51,FB,
 B7,0B,32,07,78,BA,70,5C,6C,04,A4,D9,9E,FB,D8,D4,

	BE,88,7F,1B,1D,E0,6D,6E,FE,FE,E9,22,DD,23,79,10, F5,DA,F1,AC,08,E8,58,23,03,40,B6,1D,C0,57,DC,84, C8,F9,C8,43,78,81,48,76,40,64,8C,AA,09,CA,33,08
해시값(H)	62,09,01,6D,1B,3C,68,0C,20,4D,27,91,E2,8B,23,F3, FD,0C,73,98,0D,B9,3A,83,D6,88,48,23,50,2F,1B,ED, 31,0C,D3,CB,52,0D,71,B2,91,21,D5,67,CE,7E,7E,64

< 데이터 7 - 8,000비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C,
--------	--

	F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59,63,3B,57,09,C5,59,81,F3, 21,DB,8D,62,DD,8C,B1,38,FE,22,D9,4F,D7,98,FF,E6, B9,72,23,4B,FC,24,B0,22,D5,71,33,C9,E2,7B,0F,43, 9E,13,45,2B,17,FC,DC,5F,55,DB,BE,FF,3D,25,49,C8, E4,D6,D3,D6,8A,4F,28,C3,CD,77,D4,B6,73,4F,E3,BB, 31,79,EE,11,30,94,1A,D1,AF,F3,84,AD,EC,71,C1,FC, 3B,75,9D,AC,50,57,F6,DA,69,0B,3A,4B,4B,AB,9F,23, 32,C4,3F,5B,E5,BB,C7,53,2B,35,64,E6,DF,CE,26,95, 65,F5,99,70,9A,59,0C,71,4F,E6,32,36,70,71,51,FB, B7,0B,32,07,78,BA,70,5C,6C,04,A4,D9,9E,FB,D8,D4, BE,88,7F,1B,1D,E0,6D,6E,FE,FE,E9,22,DD,23,79,10, F5,DA,F1,AC,08,E8,58,23,03,40,B6,1D,C0,57,DC,84, C8,F9,C8,43,78,81,48,76,40,64,8C,AA,09,CA,33,08, E7,AE,3A,27,1F,40,4A,6D,33,BE,DE,EA,98,6C,3A,FD, CD,1C,B3,37,4B,93,AA,23,59,D7,37,6E,CD,F3,29,BD, 63,C6,0B,88,19,CA,3E,50,7B,92,0E,B0,6A,DA,AC,AD, BB,A1,4A,9A,AF,62,BB,24,D1,B2,D7,0F,94,08,91,AB, 3D,4E,7C,D6,C7,BD,DF,0D,EC,98,CC,AE,C2,D1,00,4B, 43,24,50,BC,F7,96,E7,35,A1,C3,2E,A2,D9,D5,CA,AE, 42,41,EA,70,28,D3,56,C1,78,36,3F,2A,F9,21,76,CA, 3C,A4,2F,AF,73,47,18,A9,D2,CE,D1,84,FD,3F,27,C1, 82,2D,FB,7C,DC,8F,DE,16,23,08,8F,DB,7E,0A,A4,F5, DB,03,2B,3C,E7,9E,67,58,88,8E,2C,76,28,E9,49,39, 3A,8B,F5,5D,C4,89,F8,9F,A6,5B,8B,84,B0,41,62,DE, BA,E2,0D,EA,78,EA,56,A4,4B,0D,CE,48,08,01,67,34, 21,C3,FB,FD,9E,A9,01,01
해시값(H)	5D,B4,4A,F9,E7,25,30,11,78,86,D8,20,B9,7A,F5,68, C9,51,7B,EE,3D,CF,0D,1E,E6,8F,2C,7A,B6,F8,BA,73, 30,23,22,00,29,E2,BA,9C,AE,ED,DD,88,E3,48,5F,C4

	85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0
해시값(H)	9C,DA,24,DD,45,C4,C1,A3,BC,F5,C3,18,03,4D,DF,F9, 20,37,78,EB,43,20,08,0A,A6,18,4C,36,AA,62,65,46, 4F,AC,FB,3A,55,F2,28,E6,18,48,EE,24,F8,66,04,5A, A1,B7,3E,05,BB,31,F8,13,50,95,69,F1,5A,04,42,84

< 데이터 4 - 3,200비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A
해시값(H)	4F,D4,B3,76,F3,98,AD,7E,4F,6B,1D,4F,A4,59,78,60, 35,D8,C0,17,50,C3,45,4D,A3,6D,DE,9A,A0,6A,8F,52, 25,4B,8F,78,FD,91,72,82,CB,8A,23,55,85,E3,12,8E, EC,C3,FC,B2,32,7C,FB,F3,3D,90,B0,B5,63,FD,66,34

< 데이터 5 - 4,800비트 >

메시지(M)	<p> B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59 </p>
해시값(H)	<p> 1A,B1,FB,0A,7C,CE,68,FA,73,37,C6,94,97,60,23,CA, 01,BD,A8,C7,43,23,D1,C5,4D,76,45,B8,08,8E,12,5C, FE,B2,63,55,55,79,CD,74,43,16,76,2B,AA,E6,DD,B4, DE,A8,0A,2D,E1,C2,AB,3A,27,E6,98,7F,E3,90,97,F8 </p>

< 데이터 6 - 6,400비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59,63,3B,57,09,C5,59,81,F3, 21,DB,8D,62,DD,8C,B1,38,FE,22,D9,4F,D7,98,FF,E6, B9,72,23,4B,FC,24,B0,22,D5,71,33,C9,E2,7B,0F,43, 9E,13,45,2B,17,FC,DC,5F,55,DB,BE,FF,3D,25,49,C8, E4,D6,D3,D6,8A,4F,28,C3,CD,77,D4,B6,73,4F,E3,BB, 31,79,EE,11,30,94,1A,D1,AF,F3,84,AD,EC,71,C1,FC,
--------	--

	3B,75,9D,AC,50,57,F6,DA,69,0B,3A,4B,4B,AB,9F,23, 32,C4,3F,5B,E5,BB,C7,53,2B,35,64,E6,DF,CE,26,95, 65,F5,99,70,9A,59,0C,71,4F,E6,32,36,70,71,51,FB, B7,0B,32,07,78,BA,70,5C,6C,04,A4,D9,9E,FB,D8,D4, BE,88,7F,1B,1D,E0,6D,6E,FE,FE,E9,22,DD,23,79,10, F5,DA,F1,AC,08,E8,58,23,03,40,B6,1D,C0,57,DC,84, C8,F9,C8,43,78,81,48,76,40,64,8C,AA,09,CA,33,08
해시값(H)	7C,0D,5C,84,78,B6,8D,B6,97,2B,07,94,60,39,92,B2, A3,9E,69,E0,F5,94,1B,C0,1E,70,50,06,2E,D3,16,24, 56,0A,A0,6D,BF,DB,90,83,9C,2D,C6,2E,A3,B9,B4,64, 9E,C8,64,0D,49,11,F4,7D,C6,04,70,7B,A7,AD,5A,69

< 데이터 7 - 8,000비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45,
--------	--

	0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59,63,3B,57,09,C5,59,81,F3, 21,DB,8D,62,DD,8C,B1,38,FE,22,D9,4F,D7,98,FF,E6, B9,72,23,4B,FC,24,B0,22,D5,71,33,C9,E2,7B,0F,43, 9E,13,45,2B,17,FC,DC,5F,55,DB,BE,FF,3D,25,49,C8, E4,D6,D3,D6,8A,4F,28,C3,CD,77,D4,B6,73,4F,E3,BB, 31,79,EE,11,30,94,1A,D1,AF,F3,84,AD,EC,71,C1,FC, 3B,75,9D,AC,50,57,F6,DA,69,0B,3A,4B,4B,AB,9F,23, 32,C4,3F,5B,E5,BB,C7,53,2B,35,64,E6,DF,CE,26,95, 65,F5,99,70,9A,59,0C,71,4F,E6,32,36,70,71,51,FB, B7,0B,32,07,78,BA,70,5C,6C,04,A4,D9,9E,FB,D8,D4, BE,88,7F,1B,1D,E0,6D,6E,FE,FE,E9,22,DD,23,79,10, F5,DA,F1,AC,08,E8,58,23,03,40,B6,1D,C0,57,DC,84, C8,F9,C8,43,78,81,48,76,40,64,8C,AA,09,CA,33,08, E7,AE,3A,27,1F,40,4A,6D,33,BE,DE,EA,98,6C,3A,FD, CD,1C,B3,37,4B,93,AA,23,59,D7,37,6E,CD,F3,29,BD, 63,C6,0B,88,19,CA,3E,50,7B,92,0E,B0,6A,DA,AC,AD, BB,A1,4A,9A,AF,62,BB,24,D1,B2,D7,0F,94,08,91,AB, 3D,4E,7C,D6,C7,BD,DF,0D,EC,98,CC,AE,C2,D1,00,4B, 43,24,50,BC,F7,96,E7,35,A1,C3,2E,A2,D9,D5,CA,AE, 42,41,EA,70,28,D3,56,C1,78,36,3F,2A,F9,21,76,CA, 3C,A4,2F,AF,73,47,18,A9,D2,CE,D1,84,FD,3F,27,C1, 82,2D,FB,7C,DC,8F,DE,16,23,08,8F,DB,7E,0A,A4,F5, DB,03,2B,3C,E7,9E,67,58,88,8E,2C,76,28,E9,49,39, 3A,8B,F5,5D,C4,89,F8,9F,A6,5B,8B,84,B0,41,62,DE, BA,E2,0D,EA,78,EA,56,A4,4B,0D,CE,48,08,01,67,34, 21,C3,FB,FD,9E,A9,01,01
해시값(H)	E1,F3,AD,92,1E,AF,C1,40,B1,20,FB,84,A3,94,01,61, 51,DA,2E,B4,A1,55,2B,FB,95,60,26,53,38,FB,26,BF, 13,0D,1A,72,55,F0,35,09,91,67,BA,14,A8,E8,D7,29, 70,D7,71,4A,51,4B,55,E7,9E,AC,B7,BB,49,BB,4B,B3

마. SHAKE128 참조구현값

< 출력길이 - 4096비트(512바이트) >

< 데이터 1 - 0비트 >

메시지(M)	(Null String)
해시값(H)	7F,9C,2B,A4,E8,8F,82,7D,61,60,45,50,76,05,85,3E, D7,3B,80,93,F6,EF,BC,88,EB,1A,6E,AC,FA,66,EF,26, 3C,B1,EE,A9,88,00,4B,93,10,3C,FB,0A,EE,FD,2A,68, 6E,01,FA,4A,58,E8,A3,63,9C,A8,A1,E3,F9,AE,57,E2, 35,B8,CC,87,3C,23,DC,62,B8,D2,60,16,9A,FA,2F,75, AB,91,6A,58,D9,74,91,88,35,D2,5E,6A,43,50,85,B2, BA,DF,D6,DF,AA,C3,59,A5,EF,BB,7B,CC,4B,59,D5,38, DF,9A,04,30,2E,10,C8,BC,1C,BF,1A,0B,3A,51,20,EA, 17,CD,A7,CF,AD,76,5F,56,23,47,4D,36,8C,CC,A8,AF, 00,07,CD,9F,5E,4C,84,9F,16,7A,58,0B,14,AA,BD,EF, AE,E7,EE,F4,7C,B0,FC,A9,76,7B,E1,FD,A6,94,19,DF, B9,27,E9,DF,07,34,8B,19,66,91,AB,AE,B5,80,B3,2D, EF,58,53,8B,8D,23,F8,77,32,EA,63,B0,2B,4F,A0,F4, 87,33,60,E2,84,19,28,CD,60,DD,4C,EE,8C,C0,D4,C9, 22,A9,61,88,D0,32,67,5C,8A,C8,50,93,3C,7A,FF,15, 33,B9,4C,83,4A,DB,B6,9C,61,15,BA,D4,69,2D,86,19, F9,0B,0C,DF,8A,7B,9C,26,40,29,AC,18,5B,70,B8,3F, 28,01,F2,F4,B3,F7,0C,59,3E,A3,AE,EB,61,3A,7F,1B, 1D,E3,3F,D7,50,81,F5,92,30,5F,2E,45,26,ED,C0,96, 31,B1,09,58,F4,64,D8,89,F3,1B,A0,10,25,0F,DA,7F, 13,68,EC,29,67,FC,84,EF,2A,E9,AF,F2,68,E0,B1,70, 0A,FF,C6,82,0B,52,3A,3D,91,71,35,F2,DF,F2,EE,06, BF,E7,2B,31,24,72,1D,4A,26,C0,4E,53,A7,5E,30,E7, 3A,7A,9C,4A,95,D9,1C,55,D4,95,E9,F5,1D,D0,B5,E9, D8,3C,6D,5E,8C,E8,03,AA,62,B8,D6,54,DB,53,D0,9B, 8D,CF,F2,73,CD,FE,B5,73,FA,D8,BC,D4,55,78,BE,C2, E7,70,D0,1E,FD,E8,6E,72,1A,3F,7C,6C,CE,27,5D,AB, E6,E2,14,3F,1A,F1,8D,A7,EF,DD,C4,C7,B7,0B,5E,34, 5D,B9,3C,C9,36,BE,A3,23,49,1C,CB,38,A3,88,F5,46, A9,FF,00,DD,4E,13,00,B9,B2,15,3D,20,41,D2,05,B4, 43,E4,1B,45,A6,53,F2,A5,C4,49,2C,1A,DD,54,45,12, DD,A2,52,98,33,46,2B,71,A4,1A,45,BE,97,29,0B,6F

< 데이터 2 - 1,600비트 >

메시지(M)	A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,
--------	--

	A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3
해시값(H)	13,1A,B8,D2,B5,94,94,6B,9C,81,33,3F,9B,B6,E0,CE, 75,C3,B9,31,04,FA,34,69,D3,91,74,57,38,5D,A0,37, CF,23,2E,F7,16,4A,6D,1E,B4,48,C8,90,81,86,AD,85, 2D,3F,85,A5,CF,28,DA,1A,B6,FE,34,38,17,19,78,46, 7F,1C,05,D5,8C,7E,F3,8C,28,4C,41,F6,C2,22,1A,76, F1,2A,B1,C0,40,82,66,02,50,80,22,94,FB,87,18,02, 13,FD,EF,5B,0E,CB,7D,F5,0C,A1,F8,55,5B,E1,4D,32, E1,0F,6E,DC,DE,89,2C,09,42,4B,29,F5,97,AF,C2,70, C9,04,55,6B,FC,B4,7A,7D,40,77,8D,39,09,23,64,2B, 3C,BD,05,79,E6,09,08,D5,A0,00,C1,D0,8B,98,EF,93, 3F,80,64,45,BF,87,F8,B0,09,BA,9E,94,F7,26,61,22, ED,7A,C2,4E,5E,26,6C,42,A8,2F,A1,BB,EF,B7,B8,DB, 00,66,E1,6A,85,E0,49,3F,07,DF,48,09,AE,C0,84,A5, 93,74,8A,C3,DD,E5,A6,D7,AA,E1,E8,B6,E5,35,2B,2D, 71,EF,BB,47,D4,CA,EE,D5,E6,D6,33,80,5D,2D,32,3E, 6F,D8,1B,46,84,B9,3A,26,77,D4,5E,74,21,C2,C6,AE, A2,59,B8,55,A6,98,FD,7D,13,47,7A,1F,E5,3E,5A,4A, 61,97,DB,EC,5C,E9,5F,50,5B,52,0B,CD,95,70,C4,A8, 26,5A,7E,01,F8,9C,0C,00,2C,59,BF,EC,6C,D4,A5,C1, 09,25,89,53,EE,5E,E7,0C,D5,77,EE,21,7A,F2,1F,A7, 01,78,F0,94,6C,9B,F6,CA,87,51,79,34,79,F6,B5,37, 73,7E,40,B6,ED,28,51,1D,8A,2D,7E,73,EB,75,F8,DA, AC,91,2F,F9,06,E0,AB,95,5B,08,3B,AC,45,A8,E5,E9, B7,44,C8,50,6F,37,E9,B4,E7,49,A1,84,B3,0F,43,EB, 18,8D,85,5F,1B,70,D7,1F,F3,E5,0C,53,7A,C1,B0,F8, 97,4F,0F,E1,A6,AD,29,5B,A4,2F,6A,EC,74,D1,23,A7, AB,ED,DE,6E,2C,07,11,CA,B3,6B,E5,AC,B1,A5,A1,1A, 4B,1D,B0,8B,A6,98,2E,FC,CD,71,69,29,A7,74,1C,FC, 63,AA,44,35,E0,B6,9A,90,63,E8,80,79,5C,3D,C5,EF, 32,72,E1,1C,49,7A,91,AC,F6,99,FE,FE,E2,06,22,7A, 44,C9,FB,35,9F,D5,6A,C0,A9,A7,5A,74,3C,FF,68,62, F1,7D,72,59,AB,07,52,16,C0,69,95,11,64,3B,64,39

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0
해시값(H)	5D,7A,5B,8B,91,A5,8B,3B,E5,C3,C7,7A,3E,6C,38,BC, 55,09,71,9B,DB,6F,CA,B4,D7,C9,95,79,BD,AA,4F,55, 0A,F4,34,11,9D,33,B4,93,85,51,F1,18,56,FD,D9,65, CB,F4,0E,DF,A7,22,92,79,D0,5B,14,5A,47,84,DC,11, 6D,D0,20,7D,A9,6A,44,FE,FE,0B,F2,B5,58,8E,17,F4, D7,83,ED,C7,B8,BF,1F,B1,12,68,6D,12,F6,EF,57,5C, 07,4E,0B,24,4C,DB,44,01,C6,14,7E,25,3B,D9,98,32, 47,FB,57,F2,86,92,F1,33,42,10,55,4A,5F,04,2F,5D, FE,EB,3A,2E,CA,F0,2C,23,32,EF,A4,EF,72,C0,47,99, 08,8C,46,4B,FC,4B,86,4C,0F,68,1E,79,D2,A7,9E,41, EC,6A,46,3C,ED,7B,E2,9F,78,3C,B0,33,BC,1D,4A,49, E3,93,1F,42,0E,B3,45,99,37,EB,D1,2D,35,76,64,D7, 46,1F,EE,54,FF,A6,55,CC,AA,6D,E1,17,C8,25,52,88, 90,2F,71,43,53,CF,1E,50,32,B0,D4,42,4D,E2,56,70, 22,3F,DF,44,DC,F9,3A,01,35,EE,F1,2F,C3,8D,B2,B3, AE,10,84,B2,8E,A6,08,6B,5D,D0,94,C9,72,59,68,FB, 44,9E,4D,78,68,F5,01,E5,70,52,55,BF,8B,62,AA,C4, 68,47,E2,E8,A8,59,CA,71,75,F0,7E,60,18,12,2C,BD, EE,5D,11,27,BD,CD,E7,C2,E3,B4,C5,4A,60,CB,EB,58, DE,9B,04,3A,FE,F3,21,1C,A0,B8,CA,18,0F,BD,85,BA, 02,9A,38,07,AC,1E,C2,34,45,5F,06,FE,1D,83,05,F9, 08,14,0E,15,9B,CB,86,50,CA,84,3A,6F,29,00,55,6B, 5A,CB,89,7F,F7,AB,65,05,15,97,86,68,85,EE,C1,DA, E7,E2,4B,2C,B7,79,26,93,01,2B,B5,70,49,A0,94,22, 05,B7,CC,14,98,57,DC,60,BB,4F,A8,C3,53,86,FF,6C, 3D,78,F5,B1,92,26,79,F4,CB,60,81,17,BE,76,80,07, CA,5C,01,52,F6,4A,54,38,96,27,4C,0E,D4,64,AD,A1, 71,69,CF,7D,73,7E,31,9C,94,FC,90,16,2A,74,56,24, 04,4C,F2,95,E2,D9,ED,82,5C,EC,80,DD,7D,4F,C7,72, 1B,D2,79,A4,8D,26,66,7B,F1,CF,AA,53,50,32,92,09,

	86,CD,AC,22,98,ED,78,F4,90,4C,D1,91,36,2D,DF,C3, 2C,D1,DE,BD,87,4D,D6,2C,CD,FA,0A,D6,94,1D,F2,6B
--	---

< 데이터 4 - 3,200비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A
해시값(H)	5C,07,C4,06,13,D4,7A,E2,19,0F,14,30,D9,DF,42,FF, 49,21,1A,61,90,DB,3D,E8,EA,67,2F,78,3D,05,CD,38, C8,69,4E,34,BF,EF,C5,61,87,A0,E1,5B,B6,94,16,94, 60,1E,62,9A,5A,58,72,F9,87,38,54,90,BD,0D,BF,C5, 0E,46,69,56,CE,63,44,09,27,28,7F,8D,50,A3,5E,CF, EB,EE,52,24,11,62,EC,4A,ED,4F,74,6D,1A,05,6E,4A, 7B,E2,2C,35,F8,96,20,BF,CC,58,EB,59,46,3F,5C,EA, C8,FC,CC,56,53,C0,20,E4,01,95,BE,5E,B3,72,17,C2, B4,FE,8E,A1,73,9D,AE,33,56,18,EF,6A,9F,DF,F6,CA, EF,F6,FD,1D,8D,BF,8E,C2,66,C0,46,F9,D3,5F,2E,C5, 5B,ED,7D,E3,5B,2F,E7,FB,40,DB,59,B9,60,47,F1,13, 4A,B4,72,BF,64,5A,EC,4C,A0,5E,A7,81,D1,2C,49,77,

	7D,B8,42,D7,A2,1F,0F,71,36,8A,10,D2,76,A1,3B,D8, F0,FD,6C,F4,25,43,20,43,D6,86,E6,D5,CA,E9,E8,EF, D8,C9,31,D8,16,F1,80,1A,90,74,9C,D5,F5,F4,D1,9E, 9B,D7,D0,BF,18,E2,70,36,FF,CE,92,23,14,52,FE,49, C6,9E,54,D6,EF,D7,1B,E4,79,AD,F0,5F,0D,20,2A,92, 38,4B,82,DF,BB,AD,61,54,16,D6,69,3C,EC,D8,E9,71, 5A,13,4A,9F,BA,4C,5B,7F,0F,15,00,3E,49,8E,1F,0E, D0,01,D5,7F,27,A6,68,D3,AD,D9,A9,80,FB,3B,7F,0E, 72,BD,08,9B,1A,25,3C,EF,CC,28,82,0F,DB,0D,8C,65, E8,49,1E,E3,64,24,DD,27,A3,8D,5E,11,EB,D9,8A,85, A4,8F,AE,4F,B5,A3,53,33,1A,7C,5B,C5,30,F3,31,AC, 94,4B,89,87,75,D9,CB,E3,AC,28,99,9C,56,CC,F8,B7, 0D,F7,71,5C,00,62,C3,EF,0D,06,75,7D,CD,BC,28,EC, B6,16,FF,AF,68,89,C7,04,9A,B8,E0,4A,5E,51,86,8E, 97,EE,F2,B6,8F,2C,09,7A,BD,2A,7E,22,54,AD,39,FF, 80,0B,4E,48,FE,6E,33,8B,BA,36,6F,66,EF,A3,76,88, AC,AD,2F,39,D1,77,4F,5E,1F,5F,42,0E,58,A7,46,7C, 94,5D,53,35,BF,5D,C6,F7,45,D1,CE,34,23,18,4B,86, A9,6D,F2,0D,8D,5B,8C,8C,4B,77,12,A6,15,45,06,C5, 02,F9,5C,C5,0B,A9,F0,CF,42,57,1B,18,7B,AE,71,F2,
--	--

< 데이터 5 - 4,800비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA,
--------	--

	ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59
해시값(H)	34,D6,D8,8C,D7,77,F3,DC,A5,92,23,81,C8,70,4C,79, 77,CD,23,F1,78,7F,A2,B6,38,63,1E,BD,B1,98,1C,31, 52,D0,D1,25,30,46,F4,BF,A7,99,CE,84,DF,F7,97,EE, 98,69,2B,E4,A3,09,B1,69,6F,6D,13,A0,DA,6D,0C,5F, 2A,13,0C,52,01,AE,B5,C6,D6,06,39,B1,E2,35,62,AD, 8A,80,92,6E,FB,63,52,54,BC,00,D2,38,C4,A7,BF,4C, 47,CD,30,F9,59,ED,F2,54,DE,32,BE,49,22,05,D0,54, A7,92,9C,3D,0F,DC,2C,38,3D,6E,68,11,A2,32,AE,71, 6E,0B,84,40,CA,07,F8,B2,2F,BD,3A,7C,FF,E8,CC,B0, D2,61,BA,22,58,F1,FB,B2,67,C0,F5,45,01,4D,14,3D, FB,B7,D4,62,7A,A9,E5,C4,E1,29,E8,20,B5,EF,CB,08, EB,60,6C,D2,FE,CF,73,B4,D2,68,20,F9,DE,AC,12,58, 77,B1,A2,09,88,4F,66,72,8A,2D,8B,03,94,0D,3A,02, 0C,F4,54,30,17,F9,51,FF,30,E8,78,36,2A,96,D3,AA, 6A,71,CD,97,C5,28,C8,E3,1B,CD,02,EE,18,E4,A8,2C, CB,CF,93,B3,93,73,36,20,36,7D,4A,EA,11,4B,05,E5, 2B,A5,52,C5,03,0E,73,5A,FC,A5,C8,35,26,47,98,D2, 2F,6A,A9,76,C5,92,DC,11,16,23,5D,86,E4,D5,EE,F0, 1F,81,01,33,D8,01,0F,98,5B,99,08,DF,67,8C,52,9D, A6,95,FB,B6,11,F3,01,55,0C,83,60,9A,EF,75,4D,05, E5,CD,25,DF,3C,61,D7,8E,68,7F,72,CF,AA,00,02,70, FC,ED,81,78,74,63,48,70,F7,1F,0C,66,B1,D8,A9,E5, DF,BA,97,3D,A8,26,E8,8E,E3,C9,27,CF,FA,1F,B1,C3, B0,90,8E,2F,07,BC,14,45,7F,06,F6,49,0E,59,EC,79,

	23,0D,70,13,09,FC,DC,65,65,9C,04,BC,26,2C,67,DC, 3E,22,AB,C7,79,37,15,8B,9C,AB,33,99,84,95,14,51, AA,14,34,E6,87,A5,16,EA,0C,D3,6C,FD,97,05,54,66, 06,1A,BF,E8,F2,ED,DE,B2,D1,79,46,D7,70,04,87,87, DF,F6,82,7A,D3,48,F2,42,EA,A0,DC,05,7F,48,34,83, 3F,CA,9C,C3,8A,F4,D1,6B,62,23,C4,9D,3E,41,22,07, 47,7F,7A,8A,73,2A,D8,3F,46,EE,B2,42,D5,05,87,A9, 3E,1E,24,B3,E7,26,BB,59,6D,D6,F1,C8,BA,85,C6,70
--	---

< 데이터 6 - 6,400비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74,
--------	--

	8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59,63,3B,57,09,C5,59,81,F3, 21,DB,8D,62,DD,8C,B1,38,FE,22,D9,4F,D7,98,FF,E6, B9,72,23,4B,FC,24,B0,22,D5,71,33,C9,E2,7B,0F,43, 9E,13,45,2B,17,FC,DC,5F,55,DB,BE,FF,3D,25,49,C8, E4,D6,D3,D6,8A,4F,28,C3,CD,77,D4,B6,73,4F,E3,BB, 31,79,EE,11,30,94,1A,D1,AF,F3,84,AD,EC,71,C1,FC, 3B,75,9D,AC,50,57,F6,DA,69,0B,3A,4B,4B,AB,9F,23, 32,C4,3F,5B,E5,BB,C7,53,2B,35,64,E6,DF,CE,26,95, 65,F5,99,70,9A,59,0C,71,4F,E6,32,36,70,71,51,FB, B7,0B,32,07,78,BA,70,5C,6C,04,A4,D9,9E,FB,D8,D4, BE,88,7F,1B,1D,E0,6D,6E,FE,FE,E9,22,DD,23,79,10, F5,DA,F1,AC,08,E8,58,23,03,40,B6,1D,C0,57,DC,84, C8,F9,C8,43,78,81,48,76,40,64,8C,AA,09,CA,33,08
해시값(H)	12,D2,71,95,96,28,8F,57,39,1E,A2,86,84,04,9A,57, 1F,C6,FC,CA,1E,0D,9A,FC,81,79,DF,8E,CC,1B,98,27, 7D,35,DD,39,D4,03,A9,BF,82,49,37,A0,FB,F0,24,40, 8D,B0,D8,FE,35,16,F0,25,B1,E3,78,B8,22,A6,ED,68, 34,A8,D1,5E,DF,C5,15,F7,1F,25,C1,77,13,7D,26,E9, 0C,F3,5F,FC,85,47,28,5E,36,16,89,53,B7,C5,50,ED, F6,59,81,D1,B7,E5,70,B7,BD,AB,81,62,5E,36,65,4B, 2D,74,28,5E,DF,4F,87,6A,0D,7B,94,F5,F4,9F,26,17, 8A,1B,4C,25,36,9E,F1,14,CF,A9,E8,64,DE,5A,64,91, F1,64,CA,6D,1C,FA,3E,CA,F5,71,8D,83,D8,B1,37,5B, 17,73,8C,5C,14,A1,C7,89,F6,EB,95,09,2A,21,D7,5E, EF,51,14,14,A5,5F,42,E8,A8,E6,E3,09,63,4C,0E,E7, AC,19,35,A3,A0,BA,A1,DF,F7,1F,C8,C6,38,D2,0D,AA, 70,69,48,81,5F,D6,1F,F5,97,AC,ED,A7,65,99,4B,11, EE,C4,CF,38,09,14,1F,D8,8D,89,D7,DE,30,E4,47,18, 29,28,04,EE,10,B1,47,AA,E8,27,9F,AD,8A,46,CE,1A, AE,DA,F7,F6,7C,C7,A4,A2,B9,98,27,2D,57,7B,11,7A, C7,5D,BF,CF,DF,78,FE,39,2C,26,98,AF,05,13,4F,C5, A2,B9,82,20,8B,A3,3B,F5,26,1A,BC,43,3D,29,1E,67, 6A,6D,9E,5D,74,93,3C,06,42,39,3D,77,95,00,AD,8E, AE,2B,81,B2,AC,25,1D,A7,15,99,B3,F8,79,8B,0E,E2, 7E,A0,73,0E,72,2A,CB,02,7C,27,73,97,53,10,ED,BA, FB,D8,B0,49,AF,33,D2,F5,24,FE,08,E4,7C,E0,43,28, 23,46,2C,EF,58,42,C3,2E,B0,04,83,AA,17,EF,13,8F, 05,24,D8,9C,33,F1,52,81,0F,E7,20,46,F6,EF,ED,51,

	DE,43,11,7D,56,A5,40,FA,FB,10,FC,EE,FA,3F,77,A1, 35,B1,E6,F8,6D,CA,65,1A,29,FF,CE,D9,64,13,F3,9F, C7,BF,FE,4B,58,91,0C,FE,CD,B2,98,EA,D4,D1,35,12, 2D,F2,AC,04,2D,91,69,04,FA,EE,31,36,31,E1,45,7C, 70,CA,4D,07,5B,CA,32,CA,62,E9,60,44,77,46,B8,A6, 6E,EE,FD,0C,04,44,B0,08,24,16,B8,F2,A9,40,74,B2, E2,D1,B8,FE,D1,2C,FC,BC,0E,AD,AE,C2,E9,46,12,D9
--	---

< 데이터 7 - 8,000비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9,
--------	--

	EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59,63,3B,57,09,C5,59,81,F3, 21,DB,8D,62,DD,8C,B1,38,FE,22,D9,4F,D7,98,FF,E6, B9,72,23,4B,FC,24,B0,22,D5,71,33,C9,E2,7B,0F,43, 9E,13,45,2B,17,FC,DC,5F,55,DB,BE,FF,3D,25,49,C8, E4,D6,D3,D6,8A,4F,28,C3,CD,77,D4,B6,73,4F,E3,BB, 31,79,EE,11,30,94,1A,D1,AF,F3,84,AD,EC,71,C1,FC, 3B,75,9D,AC,50,57,F6,DA,69,0B,3A,4B,4B,AB,9F,23, 32,C4,3F,5B,E5,BB,C7,53,2B,35,64,E6,DF,CE,26,95, 65,F5,99,70,9A,59,0C,71,4F,E6,32,36,70,71,51,FB, B7,0B,32,07,78,BA,70,5C,6C,04,A4,D9,9E,FB,D8,D4, BE,88,7F,1B,1D,E0,6D,6E,FE,FE,E9,22,DD,23,79,10, F5,DA,F1,AC,08,E8,58,23,03,40,B6,1D,C0,57,DC,84, C8,F9,C8,43,78,81,48,76,40,64,8C,AA,09,CA,33,08, E7,AE,3A,27,1F,40,4A,6D,33,BE,DE,EA,98,6C,3A,FD, CD,1C,B3,37,4B,93,AA,23,59,D7,37,6E,CD,F3,29,BD, 63,C6,0B,88,19,CA,3E,50,7B,92,0E,B0,6A,DA,AC,AD, BB,A1,4A,9A,AF,62,BB,24,D1,B2,D7,0F,94,08,91,AB, 3D,4E,7C,D6,C7,BD,DF,0D,EC,98,CC,AE,C2,D1,00,4B, 43,24,50,BC,F7,96,E7,35,A1,C3,2E,A2,D9,D5,CA,AE, 42,41,EA,70,28,D3,56,C1,78,36,3F,2A,F9,21,76,CA, 3C,A4,2F,AF,73,47,18,A9,D2,CE,D1,84,FD,3F,27,C1, 82,2D,FB,7C,DC,8F,DE,16,23,08,8F,DB,7E,0A,A4,F5, DB,03,2B,3C,E7,9E,67,58,88,8E,2C,76,28,E9,49,39, 3A,8B,F5,5D,C4,89,F8,9F,A6,5B,8B,84,B0,41,62,DE, BA,E2,0D,EA,78,EA,56,A4,4B,0D,CE,48,08,01,67,34, 21,C3,FB,FD,9E,A9,01,01
해시값(H)	1C,75,41,29,44,CE,EC,96,7D,9E,6C,F2,F3,D3,CD,4B, AC,70,B8,2D,D6,4C,9D,42,18,E0,C2,83,09,30,D7,AD, 45,C3,BA,E7,4C,2D,B7,67,13,45,D1,9A,BB,6E,9D,17, 8B,72,D2,BC,71,81,21,F3,A3,E3,9C,6D,85,56,93,55, 1D,8A,AD,1F,9C,DF,A2,3B,C3,DC,7D,58,BA,A1,54,F2, DE,D2,64,92,5D,ED,31,B1,32,C7,0C,9F,17,D4,88,9F, 83,1B,92,13,F8,9D,36,A0,CD,B5,6B,ED,6C,B2,8E,3E, F3,F3,BF,D5,BF,0D,1F,78,EC,5E,53,F4,C7,0C,83,85, 44,45,FF,AC,DB,46,D1,70,3A,6A,95,39,47,7B,A2,4C, 40,B1,6B,50,E2,13,A1,9F,82,30,09,6B,A4,D1,4B,53, 3B,CF,4A,A3,00,C7,12,B5,F4,45,EE,62,D7,A9,63,74, A8,24,FD,31,8C,B2,56,F4,AF,74,7C,1A,5E,6A,66,28, 6E,19,26,43,1A,83,53,36,B3,57,0A,8D,AE,29,67,B6,

	<p>58,7D,90,F1,AE,AF,62,ED,47,28,A3,0B,ED,E6,B9,34, 9A,59,10,FA,AF,36,62,CC,37,C1,7A,E6,2D,FD,2D,CF, 5D,E3,DD,02,2E,21,4A,8C,04,91,41,FC,63,AB,5D,67, 47,51,D6,C2,81,39,35,AF,D4,83,10,90,70,4B,65,EB, 62,73,B2,F6,69,1C,20,3A,02,9F,E9,10,22,48,88,AE, B9,F6,B9,11,0C,10,3D,1C,61,89,B6,1F,FD,2D,D8,F1, 89,2A,36,86,CF,04,0F,D9,2A,A4,FF,E0,AF,A7,2D,14, 31,F0,0F,0D,8A,D8,1B,FA,80,FC,0A,07,1A,59,50,70, 05,08,2C,9E,4A,54,60,3B,FE,B5,F9,8F,57,C0,05,B1, 52,48,F2,74,D5,74,C3,75,54,64,30,4C,EF,92,71,AA, 3A,B7,7C,1B,64,37,DD,18,8D,59,4E,71,41,E9,75,A2, C1,DF,4B,1E,12,BE,3E,5C,B5,B4,DC,D3,08,D3,24,DA, BE,05,70,65,3B,A9,31,93,4C,58,6D,E5,66,BF,FC,EF, 27,89,FB,C2,B5,FC,59,48,6F,A3,35,9C,AD,35,38,C1, D0,F4,BB,06,B3,70,61,59,4D,C6,00,01,C4,A7,D1,5A, DF,99,7E,50,17,DD,B9,CF,EF,B4,BC,31,44,42,64,32, 8A,DD,56,97,9A,AD,49,C7,F4,1F,CB,5B,37,E4,50,2E, B2,E2,07,13,B6,F9,47,3E,3A,61,B6,63,1F,64,46,0E, 54,5C,DF,63,84,9B,71,4C,F1,C7,EE,6F,16,0A,9E,65</p>
--	--

바. SHAKE256 참조구현값

< 출력길이 - 4096비트(512바이트) >

< 데이터 1 - 0비트 >

메시지(M)	(Null String)
해시값(H)	46,B9,DD,2B,0B,A8,8D,13,23,3B,3F,EB,74,3E,EB,24, 3F,CD,52,EA,62,B8,1B,82,B5,0C,27,64,6E,D5,76,2F, D7,5D,C4,DD,D8,C0,F2,00,CB,05,01,9D,67,B5,92,F6, FC,82,1C,49,47,9A,B4,86,40,29,2E,AC,B3,B7,C4,BE, 14,1E,96,61,6F,B1,39,57,69,2C,C7,ED,D0,B4,5A,E3, DC,07,22,3C,8E,92,93,7B,EF,84,BC,0E,AB,86,28,53, 34,9E,C7,55,46,F5,8F,B7,C2,77,5C,38,46,2C,50,10, D8,46,C1,85,C1,51,11,E5,95,52,2A,6B,CD,16,CF,86, F3,D1,22,10,9E,3B,1F,DD,94,3B,6A,EC,46,8A,2D,62, 1A,7C,06,C6,A9,57,C6,2B,54,DA,FC,3B,E8,75,67,D6, 77,23,13,95,F6,14,72,93,B6,8C,EA,B7,A9,E0,C5,8D, 86,4E,8E,FD,E4,E1,B9,A4,6C,BE,85,47,13,67,2F,5C, AA,AE,31,4E,D9,08,3D,AB,4B,09,9F,8E,30,0F,01,B8, 65,0F,1F,4B,1D,8F,CF,3F,3C,B5,3F,B8,E9,EB,2E,A2, 03,BD,C9,70,F5,0A,E5,54,28,A9,1F,7F,53,AC,26,6B, 28,41,9C,37,78,A1,5F,D2,48,D3,39,ED,E7,85,FB,7F, 5A,1A,AA,96,D3,13,EA,CC,89,09,36,C1,73,CD,CD,0F, AB,88,2C,45,75,5F,EB,3A,ED,96,D4,77,FF,96,39,0B, F9,A6,6D,13,68,B2,08,E2,1F,7C,10,D0,4A,3D,BD,4E, 36,06,33,E5,DB,4B,60,26,01,C1,4C,EA,73,7D,B3,DC, F7,22,63,2C,C7,78,51,CB,DD,E2,AA,F0,A3,3A,07,B3, 73,44,5D,F4,90,CC,8F,C1,E4,16,0F,F1,18,37,8F,11, F0,47,7D,E0,55,A8,1A,9E,DA,57,A4,A2,CF,B0,C8,39, 29,D3,10,91,2F,72,9E,C6,CF,A3,6C,6A,C6,A7,58,37, 14,30,45,D7,91,CC,85,EF,F5,B2,19,32,F2,38,61,BC, F2,3A,52,B5,DA,67,EA,F7,BA,AE,0F,5F,B1,36,9D,B7, 8F,3A,C4,5F,8C,4A,C5,67,1D,85,73,5C,DD,DB,09,D2, B1,E3,4A,1F,C0,66,FF,4A,16,2C,B2,63,D6,54,12,74, AE,2F,CC,86,5F,61,8A,BE,27,C1,24,CD,8B,07,4C,CD, 51,63,01,B9,18,75,82,4D,09,95,8F,34,1E,F2,74,BD, AB,0B,AE,31,63,39,89,43,04,E3,58,77,B0,C2,8A,9B, 1F,D1,66,C7,96,B9,CC,25,8A,06,4A,8F,57,E2,7F,2A

< 데이터 2 - 1,600비트 >

메시지(M)	A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3, A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,A3,
--------	--

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0
해시값(H)	89,1D,A7,86,E8,6A,86,D2,BB,F5,15,36,E7,1D,89,D5, D6,B2,90,D9,9A,04,93,4D,5B,E2,5E,C5,00,D7,05,E9, D4,4E,21,BF,A4,96,26,09,C3,0C,8F,15,8D,31,62,8A, 9B,A2,F8,FF,8F,14,98,EC,74,C8,C2,F0,0B,93,9C,5B, FA,C2,F2,E3,D1,C8,3C,05,8E,EA,D5,63,82,41,1C,67, E5,27,F5,95,60,C0,EE,15,50,93,DD,27,9B,5A,74,2F, 8E,FA,C1,6C,66,EF,61,50,BD,22,A1,E4,A7,9E,2B,60, 58,BD,B4,34,B9,45,DC,31,81,80,CE,1E,3C,6D,96,A7, 70,09,AB,4F,F2,80,3C,FA,67,87,6C,61,CD,79,38,94, 65,86,6F,37,F0,F3,A3,82,4B,B5,12,C5,84,19,60,3F, DA,E1,AF,EE,83,CC,C4,35,14,8C,67,69,1B,21,82,BA, 1D,68,1A,ED,3C,1D,CB,43,F4,E8,54,12,43,FA,BD,0E, 9C,20,88,DB,3A,72,07,6C,63,23,0E,42,66,42,3B,3B, 74,CA,2B,AF,7B,C9,E5,76,07,BB,B8,78,F9,C1,5D,87, D9,CD,77,11,11,9D,39,5A,0D,71,9D,FD,7E,10,A0,E2, D2,8C,A4,0A,B4,82,70,49,F5,7C,F7,64,86,9B,F1,9F, 9C,DF,CF,F9,49,A7,A9,67,76,84,FA,E6,7D,58,1E,4D, C9,36,8C,25,DC,5F,EF,1F,5C,2A,1F,16,59,BC,C5,D0, 1F,39,F6,25,08,F9,FD,58,63,D2,6D,0B,B8,70,95,B5, A4,25,63,E3,F0,A5,36,EA,56,C9,F0,00,A3,70,B3,AD, 16,41,B4,5A,F4,D7,F2,E8,6D,1D,AA,21,FB,56,80,FA, 78,58,9A,BD,65,DC,FB,3F,F0,6C,92,F9,E4,F8,18,7D, E2,12,46,12,D1,F9,F0,5C,B0,57,9D,B6,EF,D2,85,9D, AF,96,40,0E,D2,66,F9,8A,34,69,AC,AA,02,A0,D6,B1, 70,77,FA,40,AC,68,57,71,FF,39,2D,0D,26,93,18,66, D1,3E,FD,C5,BC,D6,33,FB,3D,EE,57,73,13,64,EE,17, FE,D6,D6,38,D5,7A,A7,2E,E2,4D,6E,15,87,F1,86,80, 8E,2B,B8,64,A2,D1,7A,D7,FC,30,CD,06,70,62,2C,61, 07,B3,C9,B8,76,50,4D,36,4E,54,87,E1,D9,7C,55,4D, 83,40,F9,22,FF,81,63,67,A6,CA,CD,B6,FE,42,08,E4,

	E8,78,CB,DC,A5,66,04,64,0F,35,82,8E,F6,5D,50,12, E2,52,A2,B5,5D,9A,18,64,F5,A2,4E,B9,AB,09,CC,DF
--	---

< 데이터 4 - 3,200비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A
해시값(H)	36,1B,4D,37,E8,3C,79,B7,B1,48,3E,D1,71,C0,52,14, 2F,74,B9,06,E3,63,9C,EA,E8,1A,3C,D3,F3,F7,C2,AC, 58,11,AE,67,35,09,3D,4D,23,2C,EC,52,AA,B4,75,29, 97,2B,51,3E,DF,DE,CA,EE,A1,AC,26,A6,81,13,C5,33, FD,F3,47,AB,A1,04,B6,69,69,F7,5A,DB,BE,20,CE,04, 52,07,64,06,28,08,D5,50,90,CB,77,A7,E5,54,12,6B, DC,AE,D9,74,18,54,40,45,0E,FA,1D,0F,0A,28,50,A8, 7C,49,11,74,A9,E1,0D,DD,10,98,CA,65,14,40,BB,BB, 5C,E4,08,AB,C9,F3,93,96,CC,B4,1E,1E,4A,EC,3C,82, E3,0B,06,A4,32,F0,A1,AB,D7,5A,A7,2D,42,38,B7,3F, E0,53,74,AA,0B,1E,69,2C,00,90,F5,EF,BF,66,99,43, 75,8F,B3,A4,BB,8D,E5,17,16,AC,66,49,E6,EF,44,DC,

	4C,BF,F8,4F,52,72,0B,0D,15,42,12,C1,DB,DF,88,52, BD,02,EC,4B,09,03,13,F0,92,85,AC,2C,5F,03,0D,06, 34,AA,F8,47,91,4A,AD,55,77,45,E0,53,11,F7,7C,5E, 40,0D,82,30,CA,4C,91,31,0B,FF,17,64,16,E8,B7,DA, 3E,C9,6F,93,7A,F1,8E,6D,FC,9C,43,0F,F3,40,DF,9B, B7,51,B2,7A,A1,B5,B8,CD,B5,07,05,AD,B8,AD,2A,C5, 63,6B,EB,79,52,29,5E,56,38,BF,E9,A6,B5,AF,B4,90, 6A,C7,AF,45,A2,30,62,70,C9,BB,F1,8D,91,F7,43,7E, BD,D4,A9,BC,EC,EA,A0,17,CB,D8,F2,43,52,55,A3,0E, 9C,64,A8,A6,32,8D,B6,E1,0D,C1,C1,32,81,88,E0,E7, 92,CD,69,84,E0,CE,EC,67,B4,0D,85,BC,86,F9,89,FF, 12,4D,73,FA,2F,93,DB,2D,D3,24,78,29,F4,2E,79,74, C3,57,34,F0,77,2A,67,61,5D,71,96,FE,47,01,82,4C, EB,5A,D4,C2,1F,A0,95,27,C5,23,6D,01,AB,27,84,2A, 46,34,D7,3C,C2,F1,14,91,A2,56,1F,56,00,86,55,C9, CB,B5,2F,00,5E,82,4E,6A,4F,94,BA,1C,80,B1,B5,42, 50,3D,E9,46,39,D7,62,66,D9,1F,9D,15,45,FE,12,29, 6E,47,1B,AF,BB,AC,1D,5E,58,1E,B3,AF,A0,FD,6C,29, 93,C8,1A,2E,95,5A,3C,C8,B3,CF,31,C2,15,8A,7A,95, 92,B5,E0,B1,E9,D9,A6,1A,9E,F9,39,31,7E,0B,F4,44
--	---

< 데이터 5 - 4,800비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA,
--------	--

	ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59
해시값(H)	61,34,12,FF,6A,B7,4E,D6,E8,10,F6,6D,5A,64,63,E1, CC,53,F2,2B,A4,19,D0,25,DF,8C,77,95,72,10,8A,6D, 84,FF,EE,8F,C8,D5,49,F8,29,34,EA,20,D4,68,D7,60, 3D,68,2C,C9,9F,CB,99,F8,D5,6C,87,83,E9,65,55,E9, 64,5C,9B,2A,71,8C,3F,4C,85,7C,CC,86,98,E2,B2,A1, 13,C9,D6,BF,7B,CA,15,42,B1,7B,AF,AF,BB,C7,BA,4D, C0,F6,51,3B,EF,6F,4F,E5,64,06,63,2E,0B,13,D3,50, 5F,34,21,61,F4,03,03,2F,CD,FA,2A,CB,93,8B,78,BE, 56,1E,2E,06,8A,30,80,A4,6F,0C,E6,07,F6,2C,CB,51, 89,69,77,1F,47,F8,8B,85,91,3A,85,9E,BE,5F,29,FD, 06,E1,BB,1C,FE,AA,4E,C0,71,1E,A8,4D,BF,48,12,21, AE,A0,B4,30,58,A1,8C,61,3C,02,C8,07,73,EA,77,74, 2C,BC,47,55,0E,B2,6D,C2,6F,40,00,70,B4,10,DE,11, B8,EA,3E,E6,B7,DF,6F,E2,5E,10,B9,E0,64,4D,C6,0C, A3,91,F2,7B,04,1A,C2,97,F8,EB,F5,3E,64,32,1F,C6, 11,20,F9,EA,7F,39,5D,26,7D,6F,E8,4D,BA,87,89,B6, D2,BF,22,93,6F,E4,13,23,F2,7A,8A,84,A4,C2,6A,C8, CD,3B,ED,45,C3,5C,28,43,98,15,2B,24,8B,33,03,DB, CD,90,2D,20,0C,A7,9E,67,8A,E5,43,87,2D,C8,AE,6A, 6C,01,A9,4B,A5,4A,11,F1,0C,0C,30,58,09,4C,61,5F, 98,CE,C0,A9,BF,F9,67,13,69,0A,5F,6D,52,5C,CF,1F, DF,4D,5F,47,37,6F,06,1C,F7,40,75,DE,F3,F1,50,79, 5F,03,4E,CB,21,7A,42,6C,05,39,A4,AB,EB,19,2F,C6, 70,70,05,44,57,E3,6F,60,52,E2,3F,7A,7E,A8,08,F8,

	71,4F,3D,EC,66,26,6A,88,01,57,D8,A5,C8,89,6D,E6, 4C,97,6D,6F,80,82,66,92,A9,02,72,BF,38,1A,76,7D, A0,29,35,0A,53,88,30,24,32,75,99,74,40,DD,1F,92, 0B,11,41,58,48,C7,74,74,69,2F,C9,10,B4,85,A6,1D, E8,36,4A,8D,BD,44,F0,F3,46,D4,35,F7,BD,31,D2,99, 65,F3,96,3E,69,D8,09,69,59,49,06,FB,26,28,A6,7E, 22,AB,FF,FC,D9,DE,87,C9,94,93,07,AF,10,C2,F2,82, 20,42,F9,14,78,1C,68,6D,BC,A0,8C,2C,70,98,31,3A
--	---

< 데이터 6 - 6,400비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74,
--------	--

	8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9, EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59,63,3B,57,09,C5,59,81,F3, 21,DB,8D,62,DD,8C,B1,38,FE,22,D9,4F,D7,98,FF,E6, B9,72,23,4B,FC,24,B0,22,D5,71,33,C9,E2,7B,0F,43, 9E,13,45,2B,17,FC,DC,5F,55,DB,BE,FF,3D,25,49,C8, E4,D6,D3,D6,8A,4F,28,C3,CD,77,D4,B6,73,4F,E3,BB, 31,79,EE,11,30,94,1A,D1,AF,F3,84,AD,EC,71,C1,FC, 3B,75,9D,AC,50,57,F6,DA,69,0B,3A,4B,4B,AB,9F,23, 32,C4,3F,5B,E5,BB,C7,53,2B,35,64,E6,DF,CE,26,95, 65,F5,99,70,9A,59,0C,71,4F,E6,32,36,70,71,51,FB, B7,0B,32,07,78,BA,70,5C,6C,04,A4,D9,9E,FB,D8,D4, BE,88,7F,1B,1D,E0,6D,6E,FE,FE,E9,22,DD,23,79,10, F5,DA,F1,AC,08,E8,58,23,03,40,B6,1D,C0,57,DC,84, C8,F9,C8,43,78,81,48,76,40,64,8C,AA,09,CA,33,08
해시값(H)	F0,A9,26,06,5D,07,75,05,20,31,12,AC,12,4A,10,01, 34,EB,33,FE,8C,55,81,51,39,42,79,F1,1F,83,B4,F1, 35,DB,2C,1D,99,00,D7,C5,38,9E,32,B3,02,8E,58,9B, 62,C8,EA,D0,E8,DC,A6,38,4A,F9,66,52,C7,36,EE,27, BF,AA,F3,B2,47,2A,8A,2B,90,46,3C,BD,35,F3,3A,16, C7,0F,12,E1,BA,0F,A7,BB,AF,06,3E,89,B6,76,94,ED, B7,DF,E6,03,AC,69,8F,2E,DC,07,21,08,73,CD,D1,D2, 23,A0,07,F6,FD,42,48,B9,D5,53,CD,53,C4,78,2D,E9, D2,D3,53,26,78,89,7F,72,22,9F,8A,C0,42,C3,DA,4E, CC,74,5A,43,5F,D1,6A,9E,65,56,E7,A6,31,D2,63,35, 6E,5E,0F,AA,3C,A9,F7,23,D0,E7,06,C9,94,C3,CD,4F, 92,E9,AF,E2,2A,D3,7C,BC,17,2C,F6,45,E6,1E,75,4A, 6F,2C,EC,1D,76,03,F0,2C,55,70,A9,01,77,7A,64,93, 54,1D,C3,5A,DF,11,25,B6,21,51,5B,50,49,A9,81,83, B7,24,24,FB,A4,86,14,99,BE,27,F3,D8,ED,B6,9B,13, 9A,5F,59,D6,50,EC,6F,D1,D9,0F,A5,09,E0,D1,4E,49, C4,0F,B6,5D,05,BA,33,58,94,D1,28,DD,38,14,C5,FE, FA,01,DF,EC,4B,DE,A7,2A,7E,47,35,AF,D9,86,0A,39, 0C,DE,40,E4,8B,8D,EE,3E,43,F3,60,FC,51,EE,17,D8, E9,A7,46,47,5F,4A,2D,DA,41,5E,AD,DF,D5,36,D8,C5, BB,B6,BA,89,30,C2,8A,0F,B2,DF,19,C6,0C,17,B2,60, B7,C1,0C,9D,0D,99,72,ED,37,0F,E4,1C,E9,06,F0,CB, F7,D8,5C,47,48,16,9C,2B,AD,33,58,AD,93,27,C4,F0, 30,83,61,55,25,6F,3F,AC,29,E3,04,85,54,B1,33,03, 0C,22,7A,DA,3B,54,B1,C1,34,DB,BA,6D,10,AC,4F,43,

	AE,12,D9,80,14,7F,54,ED,1F,9F,E3,B7,A5,80,D4,96, B5,DA,63,B1,29,D5,A9,4E,B4,D9,7D,E1,46,D5,26,02, 4A,39,2C,BC,11,34,A3,99,A5,66,6D,EC,A6,9A,FF,1C, 0D,D7,39,F6,EB,DF,A3,9B,CC,96,14,DD,80,45,BD,14, 24,9D,73,55,82,48,CE,90,6A,C6,43,AE,7E,E0,7A,0E, 23,F4,89,BB,C3,C4,9E,8D,4B,6B,D9,82,1E,6A,79,C4, 61,74,0A,90,41,4B,05,8A,24,D9,3E,38,B3,76,AE,84
--	---

< 데이터 7 - 8,000비트 >

메시지(M)	B7,3B,C1,7B,69,BE,25,A4,F5,94,B7,11,60,F4,20,25, B9,4E,53,45,DD,9F,70,B7,13,B6,D6,9D,D0,D1,9D,35, AE,EE,55,FF,46,DB,FD,89,54,31,07,C7,32,37,D4,CB, A0,09,7F,79,05,BB,0E,03,E0,87,46,EE,1B,7E,E6,0F, 15,C9,C8,3E,2D,92,A2,01,BE,E8,49,65,7D,BD,E5,2B, F7,A3,DD,9E,DB,E3,52,A1,BA,33,05,5F,64,A2,55,6E, AA,DF,46,C3,0A,4B,0B,7B,60,E1,41,D9,3C,AE,D6,59, 68,10,FE,A7,71,E8,5D,1A,23,EA,C8,F9,E0,E9,11,AD, 66,9F,4F,E6,A6,D0,20,FC,71,F1,E3,2E,ED,1E,86,90, 9C,92,DB,BA,C3,80,DF,8A,51,B5,6D,98,2A,D8,52,68, 06,F3,27,4E,C6,87,89,06,1B,15,1A,69,8D,0C,8A,73, 85,DD,D7,CE,F6,79,1C,CB,56,6B,A4,14,9E,C8,07,89, 8B,6B,AC,7D,A4,B0,87,E0,69,B3,2D,B3,5D,77,75,85, BF,9E,FC,39,24,60,3A,D5,AD,5E,79,2A,F9,C5,9A,0B, 09,AE,DD,12,B6,0E,40,CE,9A,18,BE,DE,A0,E5,4C,5B, 0F,F5,11,FE,0D,34,75,FD,39,9D,C1,A4,E9,F6,C6,BB, 2B,E2,B8,B6,04,6D,E1,74,14,1C,05,DA,C5,4C,1B,D7, 89,14,C0,2B,6A,8E,20,0C,EB,A5,BE,2E,87,F6,19,2B, D9,9A,BD,2F,C0,A0,3D,06,EA,F3,53,3C,81,E8,E2,CA, ED,D2,31,ED,BA,61,D2,18,AE,4D,8A,E9,F2,CF,01,43, 9F,72,5C,3B,27,EB,D4,18,75,8A,FE,1A,EF,85,7B,7A, 60,66,3F,5C,88,42,04,0B,61,C7,C6,6D,7D,E2,EE,C9, 22,84,03,56,3F,A1,18,B3,46,F7,4E,2E,21,C9,94,FF, 35,76,D5,C7,4E,63,1F,87,25,CE,44,86,F5,1E,2C,90, CF,68,C2,0F,73,BE,BD,76,ED,E8,DD,6C,37,E2,92,9A, 1B,22,03,9D,2C,42,A4,EE,B5,66,6C,B3,E0,9E,B0,E8, 86,00,9F,32,F1,16,D9,81,B0,B1,A1,3C,CF,A6,8A,11, 56,E9,45,FD,50,A4,8F,64,24,38,23,56,EB,BC,88,08, BF,9C,E1,42,F1,DC,32,FD,D9,72,B6,51,64,18,1C,45, 0B,DB,61,DC,AE,06,5C,4C,0C,8E,C1,59,49,F6,0C,0C, 82,70,60,7B,F4,E5,6C,17,B2,BB,F1,78,9C,DA,33,80, 96,FF,68,ED,F0,8C,51,90,4A,B0,1A,0F,88,99,6E,74, 8F,A7,58,B8,E0,BC,18,B3,28,E0,C7,F0,BC,1E,9C,A9,
--------	--

	EA,A6,8A,E7,18,F1,18,58,CF,23,07,4D,D4,EA,9E,4C, F8,EA,C6,D2,77,2F,45,6D,24,2D,80,66,35,D3,8E,F7, E9,6F,AB,CA,07,1A,78,BC,30,44,72,FF,01,49,FA,B4, 7A,42,B4,E6,06,17,7B,E0,BD,BB,83,16,31,B3,23,AF, 80,B7,AF,BA,6E,95,5E,59,63,3B,57,09,C5,59,81,F3, 21,DB,8D,62,DD,8C,B1,38,FE,22,D9,4F,D7,98,FF,E6, B9,72,23,4B,FC,24,B0,22,D5,71,33,C9,E2,7B,0F,43, 9E,13,45,2B,17,FC,DC,5F,55,DB,BE,FF,3D,25,49,C8, E4,D6,D3,D6,8A,4F,28,C3,CD,77,D4,B6,73,4F,E3,BB, 31,79,EE,11,30,94,1A,D1,AF,F3,84,AD,EC,71,C1,FC, 3B,75,9D,AC,50,57,F6,DA,69,0B,3A,4B,4B,AB,9F,23, 32,C4,3F,5B,E5,BB,C7,53,2B,35,64,E6,DF,CE,26,95, 65,F5,99,70,9A,59,0C,71,4F,E6,32,36,70,71,51,FB, B7,0B,32,07,78,BA,70,5C,6C,04,A4,D9,9E,FB,D8,D4, BE,88,7F,1B,1D,E0,6D,6E,FE,FE,E9,22,DD,23,79,10, F5,DA,F1,AC,08,E8,58,23,03,40,B6,1D,C0,57,DC,84, C8,F9,C8,43,78,81,48,76,40,64,8C,AA,09,CA,33,08, E7,AE,3A,27,1F,40,4A,6D,33,BE,DE,EA,98,6C,3A,FD, CD,1C,B3,37,4B,93,AA,23,59,D7,37,6E,CD,F3,29,BD, 63,C6,0B,88,19,CA,3E,50,7B,92,0E,B0,6A,DA,AC,AD, BB,A1,4A,9A,AF,62,BB,24,D1,B2,D7,0F,94,08,91,AB, 3D,4E,7C,D6,C7,BD,DF,0D,EC,98,CC,AE,C2,D1,00,4B, 43,24,50,BC,F7,96,E7,35,A1,C3,2E,A2,D9,D5,CA,AE, 42,41,EA,70,28,D3,56,C1,78,36,3F,2A,F9,21,76,CA, 3C,A4,2F,AF,73,47,18,A9,D2,CE,D1,84,FD,3F,27,C1, 82,2D,FB,7C,DC,8F,DE,16,23,08,8F,DB,7E,0A,A4,F5, DB,03,2B,3C,E7,9E,67,58,88,8E,2C,76,28,E9,49,39, 3A,8B,F5,5D,C4,89,F8,9F,A6,5B,8B,84,B0,41,62,DE, BA,E2,0D,EA,78,EA,56,A4,4B,0D,CE,48,08,01,67,34, 21,C3,FB,FD,9E,A9,01,01
해시값(H)	18,5A,49,70,91,D8,5A,CC,6A,F8,7E,44,E6,B5,F2,B4, 92,C2,E3,42,B5,CC,BC,0E,3F,BE,1A,37,2E,F8,2E,90, 75,1E,29,8A,54,5E,F4,90,B7,77,7C,E3,1A,5A,CF,0B, F3,74,A3,D2,43,8D,1E,A7,C1,E3,46,59,26,21,0B,0C, EA,5D,85,CD,DF,68,34,C1,9C,B1,14,C7,4F,09,2F,74, 25,14,D9,99,74,D8,94,69,74,8D,00,39,6E,9A,65,B0, B3,3B,0B,D9,F2,CA,75,6B,CD,18,41,35,63,D7,84,95, D2,BC,AE,DE,DE,11,B1,B5,1F,E5,77,9F,9B,28,43,D7, 8A,BC,DD,F8,A1,97,41,16,AC,EB,2F,6D,B9,CF,70,E5, 10,24,C9,EC,09,B5,F5,1D,5C,37,CA,CA,97,EC,10,E0, 25,4B,70,C8,7F,AF,39,FF,1D,D1,53,52,06,ED,01,5E, 8C,E1,51,B8,D9,C5,E2,0D,D9,7A,7F,A3,63,2C,1B,7D, 48,C8,D4,B5,85,0F,C1,7F,4E,D9,76,CC,24,AD,41,5A,

	A7,6C,FF,EA,1A,F2,04,B3,8F,C8,2F,A1,77,8A,AF,21, CA,EB,8B,23,76,74,47,71,1A,4D,73,99,B0,11,C4,83, B3,79,E1,D0,7D,2C,48,86,F1,90,62,56,CD,79,E5,28, C5,3D,51,6E,E3,CB,3B,56,3D,22,06,2B,6C,74,B7,F4, 47,88,8B,4A,BC,E9,3E,FA,DE,C8,03,59,56,CC,A8,94, 0D,DD,EF,BA,CF,B8,BA,76,14,35,50,0B,9C,7D,D9,A3, CF,4B,CB,6E,4F,A5,53,30,16,39,AA,49,B6,FC,F2,7F, 2A,A9,5A,C7,E1,59,FB,2B,C4,32,9B,9B,1D,C4,A2,D3, 89,72,8A,41,94,D5,53,47,A7,CF,54,06,BB,A4,37,EE, 95,EE,C2,91,40,02,6E,8D,12,65,00,B5,61,06,B9,46, 55,DD,EE,73,51,D4,03,F5,9A,14,62,7E,CF,C4,11,68, FC,08,7D,05,89,B8,48,B0,AF,44,16,3B,59,D3,9C,67, 17,AE,73,3D,CF,40,AA,C5,28,77,C0,97,E6,F1,E7,74, 32,7F,AA,CA,7D,CF,FE,D9,7C,98,D3,3E,B2,0C,C1,F0, 91,A0,B3,40,34,7D,14,E8,DB,A5,63,A9,F1,52,BE,90, 25,F8,81,2E,FD,9C,3B,7E,9D,E9,A6,F8,0A,99,51,18, 6E,21,E2,92,63,CD,DD,88,43,D2,B2,DA,F3,74,5D,A2, E6,A7,3E,CC,61,81,E6,AD,0F,EB,93,0E,28,76,C1,FE, 33,C1,85,A8,D3,E4,7A,27,8B,AC,20,C4,10,A9,08,ED
--	---