TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-12.xxxx-Part3 제정일: 2018년 12월 xx일

해시 함수 기반 메시지 인증 코드 (HMAC) - 제3부: 해시 함수 LSH

The Keyed-Hash Message Authentication Code (HMAC) - Part3: Hash Function LSH

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 정보보호기반 프로젝트그룹(PG501)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	한상윤	NSR	선임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.xxxx-Part3
표준 초안 작성자	한상윤	NSR	선임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.xxxx-Part3
	주왕호	NSR	연구원	-	TTAK.KO-12.xxxx-Part3
사무국 담당	박수정	TTA	책임	-	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.12

서 문

1 표준의 목적

이 표준은 LSH를 기반 해시 함수로 사용하는 HMAC의 참조 구현값을 제시하여, HMAC의 구현 정확성을 확인할 수 있도록 한다.

2 주요 내용 요약

이 표준은 암호 키 크기 조건에 따라 달라지는 HMAC 알고리즘의 동작 방식을 반영하여, LSH를 기반 해시 함수로 사용하는 HMAC의 참조 구현값을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준에 제시된 참조 구현값은 제1부 일반에 규정된 HMAC의 기반 해시 함수로 TTAK.KO-12.0276에 규정된 해시 함수 LSH를 적용한 결과로, LSH는 해당 표준의 상세 규격을 준용한다.

3.2 인용 표준과 본 표준의 비교표

- 해당없음

Preface

1 Purpose

The standard provides test vectors of HMAC based on LSH about implementation conformance.

2 Summary

The standard specifies the test vectors of HMAC based on LSH about implementation conformance

3 Comparison to Reference Standards

3.1 Relationship to Reference Standards

The test vectors in this standard are result of applying the hash function LSH specified in TTAK.KO-12.0276, the HMAC mechanism specified in Part 1: General. And, LSH conforms to the specifications of the standard.

목 차

해시 함수 기반 메시지 인증 코드 (HMAC)
- 제3부: 해시 함수 LSH
(The Keyed-Hash Message Authentication Code (HMAC)
- Part3: Hash Function LSH)

1 적용 범위

이 표준은 해시 함수 LSH를 기반으로 동작하는 HMAC의 참조 구현값을 제시한다. 참조 구현값 생성에 사용된 해시 함수는 <표 1-3>과 같다.

<표 1-1> HMAC 참조 구현값 생성에 사용되는 해시 함수

해시 함수	LSH-224 LSH-512-224	LSH-256 LSH-512-256	LSH-384	LSH-512
출력 블록 크기 L (바이트)	28	32	48	64

HMAC은 입력 암호 키와 입력 블록 크기와의 관계에 따라 다른 동작 절차를 따른다. 이러한 HMAC의 특징을 고려하여 설정한 참조 구현값 생성 시나리오를 정리하면 <표 1-4>와 같다.

<표 1-2> 암호 키 크기 따른 시험 분류

구분		해시함수
(5절) 암호 키 길이가 입력 블록 크기와 같은 경우 HMAC 참조구현값	5.1	LSH-224
	5.2	LSH-256
	5.3	LSH-384
	5.4	LSH-512
	5.5	LSH-512-224
	5.6	LSH-512-256
(6절) 암호 키 길이가 입력 블록 크기보다 큰 경우 HMAC 참조구현값	6.1	LSH-224
	6.2	LSH-256
	6.3	LSH-384
	6.4	LSH-512
	6.5	LSH-512-224
	6.6	LSH-512-256
(7절) 암호 키 길이가 입력 블록 크기보다 작은 경우 HMAC 참조구현값	7.1	LSH-224
	7.2	LSH-256
	7.3	LSH-384
	7.4	LSH-512
	7.5	LSH-512-224
	7.6	LSH-512-256

2 인용 표준

- TTAK.KO-12.0xxx-Part1, “해시 함수 기반 메시지 인증 코드(HMAC) - 제1부 일반”, 2018. 12.
  (※ 이 표준의 용어 정의, 약어 및 기회는 해당 표준을 따름)

- TTAK.KO-12.0276, “해시 함수 LSH”, 2015.12.16.

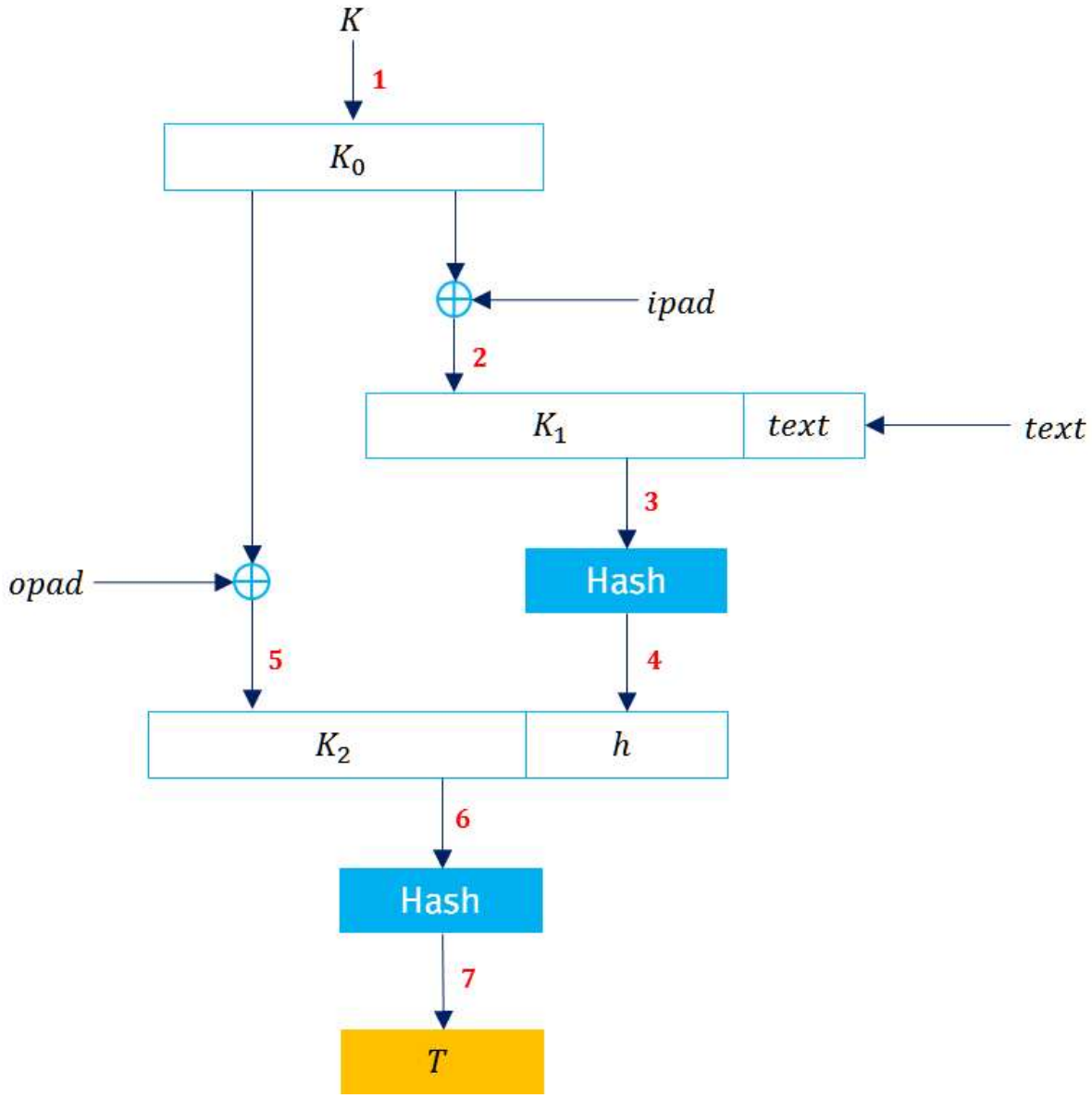
3 용어 정의

- 해당없음

4 약어

- 해당없음

5 암호 키 길이가 입력 블록 크기와 같은 경우 HMAC 참조구현값



5.1 LSH-224의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	7b249fd6a49303c755ea21fe25f6c54afbe806f43527987fe4dbd6d1
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 7b249fd6a49303c755ea21fe25f6c54afbe806f43527987fe4dbd6d1
7	T	2b0b1980345dc741246d45256de128d1b8bbee9121cdf4d2d2756ee3

5.2 LSH-256의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	867c60513f82d500b2030dea6c658d388147b076cd06fbdd58e8baf94fd43705
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 867c60513f82d500b2030dea6c658d388147b076cd06fbdd58e8baf94fd43705
7	T	c1decf9c7b9464c668d9737b8c9814502546bbe81ae7c38fd2065b6749f10e9b

5.3 LSH-384의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
2	K_1	3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9
3	$data_1$	3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff
4	h	0903bb26bd961dc3141bf6e805c1aea56b08184928e6ccaccb0b446c4815011b 14ef0fa638fe3bc93c435f2c2288bffb

5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 0903bb26bd961dc3141bf6e805c1aea56b08184928e6ccaccb0b446c4815011b 14ef0fa638fe3bc93c435f2c2288bffb
7	T	1d1558a77da044a7a5dbc022d56884888819d0141a329347d838b4b11c5744c7 918f9b75ce1bd52e3d2cf614c572fa83

5.4 LSH-512의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
2	K_1	3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9
3	$data_1$	3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff
4	h	7dcb50404eb6af2f6f44de959dce40a8f2c5fdfc5c80f3b68d97f0a0078a82ce a019551ea0667e0d9b3fa45d54d1249575cdcec128fa2a487d449c3d2b649043

5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 7dcb50404eb6af2f6f44de959dce40a8f2c5fdfc5c80f3b68d97f0a0078a82ce a019551ea0667e0d9b3fa45d54d1249575cdcec128fa2a487d449c3d2b649043
7	T	82aebed54a8f706d3573eaa5a4eb9b2e5a0fdab9d47ee0b879471f56687cf4bb 6f3bb5c34bf88832593da423dc8e317f79127a73fc206a0895416c38de3dcb4e

5.5 LSH-512-224의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
2	K_1	3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9
3	$data_1$	3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff
4	h	ac3a70b9f93c5b4de3b763e15577396c8b96347fc48e7cee488618e1

5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3
6	data_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 ac3a70b9f93c5b4de3b763e15577396c8b96347fc48e7cee488618e1
7	T	a24b5793bbd6f60c69f4de7f6db372cc414de64fd3599b1ae10652e7

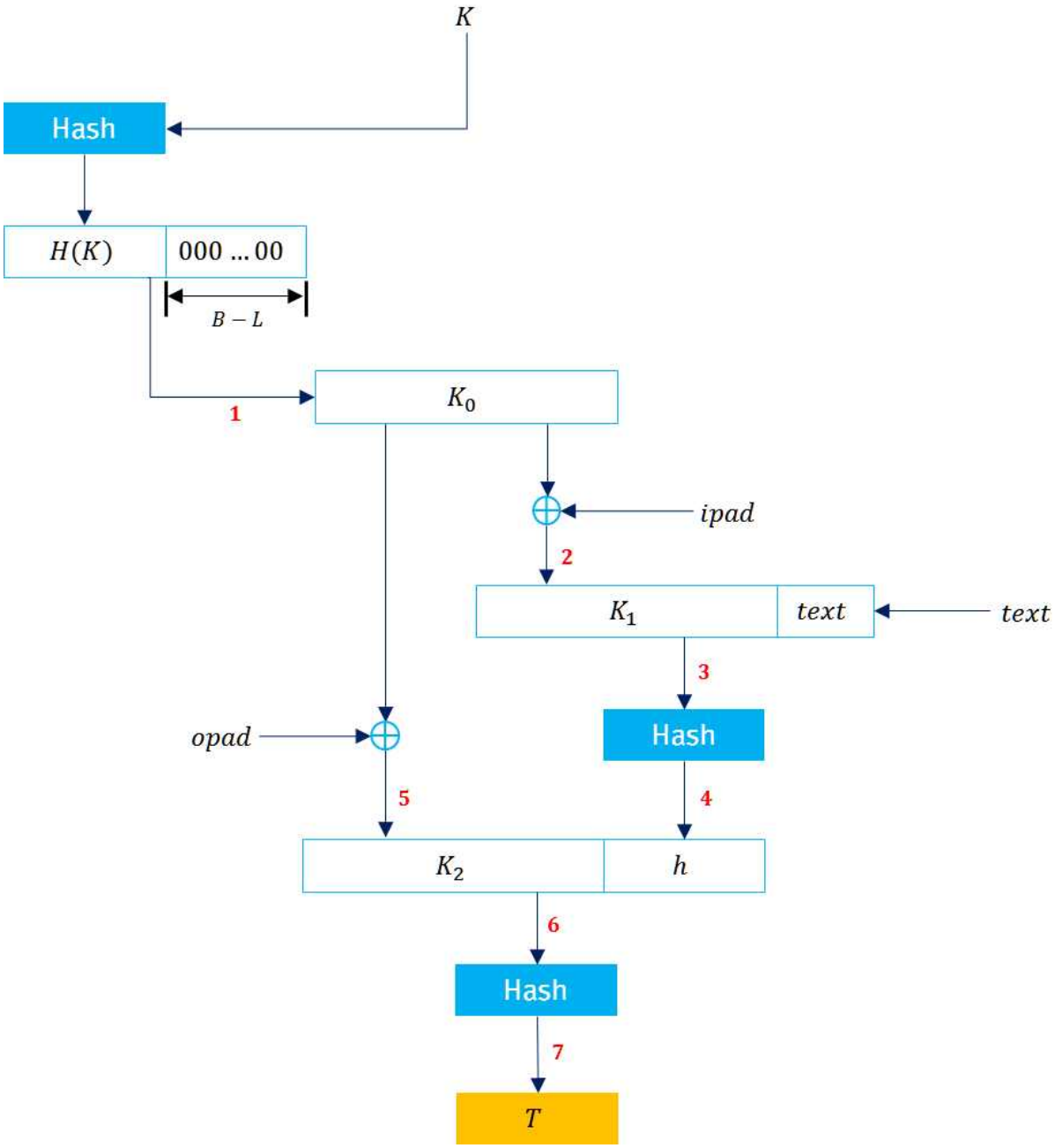
5.6 LSH-512-256의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
2	K_1	3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9
3	$data_1$	3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff
4	h	842e3456a64293af219c9e37e03c886d9f2ed7c3c3e0200d4dd69322e7863e2b

5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 842e3456a64293af219c9e37e03c886d9f2ed7c3c3e0200d4dd69322e7863e2b
7	T	8a2cf20bc53990facc59f977734a3f9aeb50f53cc1e8eab2db3819db0acba3bd

6 암호 키 길이가 입력 블록 크기보다 큰 경우 HMAC 참조구현값



6.1 LSH-224의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	f35d4ec2b58e73720bfd0c19f312a1de0c207a1e9a364a93ccec0f9e00000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
2	K_1	c56b78f483b845443dcb3a2fc52497e83a164c28ac007ca5fada39a836363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	c56b78f483b845443dcb3a2fc52497e83a164c28ac007ca5fada39a836363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	771a4e3e56f1c44c0a7a426eee6e277ee4247ccf68a8ae7ea0668789
5	K_2	af01129ee9d22f2e57a15045af4efd82507c2642c66a16cf90b053c25c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	af01129ee9d22f2e57a15045af4efd82507c2642c66a16cf90b053c25c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 771a4e3e56f1c44c0a7a426eee6e277ee4247ccf68a8ae7ea0668789
7	T	96d610569d6cb135b0cade0a8825d7b0463609a680b33b445ff0d3e2

6.2 LSH-256의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	3bf00f4cad079be7410f829452c2cb700a9460135877ee95815c52c99797c9a2 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000
2	K_1	0dc6397a9b31add17739b4a264f4fd463ca256256e41d8a3b76a64ffa1a1ff94 36363636363636363636363636363636363636363636363636363636363636 36363636363636363636363636363636363636363636363636363636363636 36363636363636363636363636363636363636363636363636363636363636
3	$data_1$	0dc6397a9b31add17739b4a264f4fd463ca256256e41d8a3b76a64ffa1a1ff94 36363636363636363636363636363636363636363636363636363636363636 36363636363636363636363636363636363636363636363636363636363636 36363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	818db016d449082100f5b5d062c374b7b86b189d28b1cefa400568bf70295884
5	K_2	67ac5310f15bc7bb1d53dec80e9e972c56c83c4f042bb2c9dd000e95cbcb95fe 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	67ac5310f15bc7bb1d53dec80e9e972c56c83c4f042bb2c9dd000e95cbcb95fe 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 818db016d449082100f5b5d062c374b7b86b189d28b1cefa400568bf70295884
7	T	db62750070f35202d3a5b42e4ecd3fd8add5b441f1a4fbe466e728a30c1fc686

6.3 LSH-384의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	de68b02699233b6a3ba5e9a59c21ce27c7f49818f71275b907052b103e84fe82 cec4be5abefb369d83761e49cf38a613000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
2	K_1	e85e8610af150d5c0d93df93aa17f811f1c2ae2ec124438f31331d2608b2c8b4 f8f2886c88cd00abb540287ff90e902536363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	e85e8610af150d5c0d93df93aa17f811f1c2ae2ec124438f31331d2608b2c8b4 f8f2886c88cd00abb540287ff90e902536363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	a6388004171f974211590f2ebc0b8b15403bbbdcee409c837f364d77d2f2f67c 7ecbe7fc5bb3a09cc9bc9ce3821ca5ec

5	K_2	8234ec7ac57f673667f9b5f9c07d927b9ba8c444ab4e29e55b59774c62d8a2de 9298e206e2a76ac1df2a42159364fa4f5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	8234ec7ac57f673667f9b5f9c07d927b9ba8c444ab4e29e55b59774c62d8a2de 9298e206e2a76ac1df2a42159364fa4f5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c a6388004171f974211590f2ebc0b8b15403bbbdcee409c837f364d77d2f2f67c 7ecbe7fc5bb3a09cc9bc9ce3821ca5ec
7	T	8bf9ac3628d1c49987bb8f4fdf9f1b9fbc43e1692e4d8109088d596c5a8afefe 5e163f5093e36dda427f4a4fda3a5d95

6.4 LSH-512의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	8d12d98875f4271c26b24a59ccf2c71747aba5f5d60ca784204fe91b2a97aba4 b653336b0f90671bbc27526f2411a5ee3d562af7569a60d042624f490f69a3ea 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
2	K_1	bb24efbe43c2112a10847c6ffac4f121719d93c3e03a91b21679df2d1ca19d92 8065055d39a6512d8a116459122793d80b601cc160ac56e67454797f395f95dc 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	bb24efbe43c2112a10847c6ffac4f121719d93c3e03a91b21679df2d1ca19d92 8065055d39a6512d8a116459122793d80b601cc160ac56e67454797f395f95dc 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	bbdaef030c2f7d8122374eb7eb56249a28c3eccfc88f4ba38a4339538fecefbc 1fa533bea9f51207d198b03ed25c645d693ebc7cc66de80e7c59f240841fbdc8

5	K_2	d14e85d429a87b407aee160590ae9b4b1bf7f9a98a50fbd87c13b54776cbf7f8 ea0f6f3753cc3b47e07b0e33784df9b2610a76ab0ac63c8c1e3e13155335ffb6 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	d14e85d429a87b407aee160590ae9b4b1bf7f9a98a50fbd87c13b54776cbf7f8 ea0f6f3753cc3b47e07b0e33784df9b2610a76ab0ac63c8c1e3e13155335ffb6 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c bbdaef030c2f7d8122374eb7eb56249a28c3eccfc88f4ba38a4339538fecefbc 1fa533bea9f51207d198b03ed25c645d693ebc7cc66de80e7c59f240841fbdc8
7	T	48fc93d712d26b499c1598c82638bfb4b87baf020f3eac5254cde2866251dac8 9418282740e118f524de281a213327d9d2e56efb04f81c87d567cf17d1197e03

6.5 LSH-512-224의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	fb69bd3e01817313e2013076db1b72987aa62729bb1b478e0d76e2d800000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
2	K_1	cd5f8b0837b74525d4370640ed2d44ae4c90111f8d2d71b83b40d4ee36363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	cd5f8b0837b74525d4370640ed2d44ae4c90111f8d2d71b83b40d4ee36363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	4c5f7dc206a9fccb0f7caf1e3a4038ad9c7386404ace0ad8dd673a46

5	K_2	a735e1625ddd2f4fbe5d6c2a87472ec426fa7b75e7471bd2512abe845c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	a735e1625ddd2f4fbe5d6c2a87472ec426fa7b75e7471bd2512abe845c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 4c5f7dc206a9fccb0f7caf1e3a4038ad9c7386404ace0ad8dd673a46
7	T	5e35bdbe198d6267f44e1cb54370b111c08a53230a7204cecea241ff

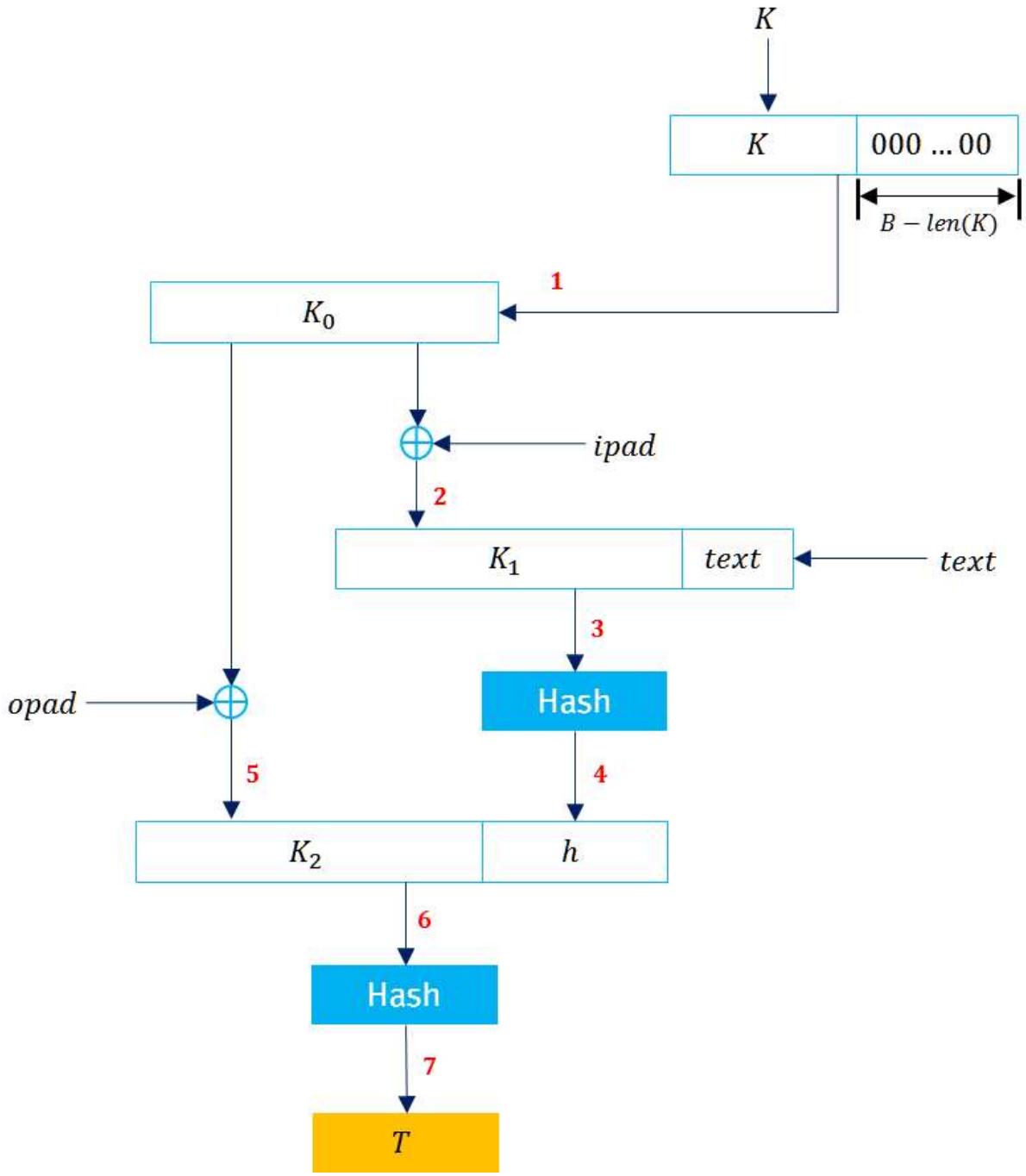
6.6 LSH-512-256의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	a2523391ef24f9c6abc797e2b25e6a54b797fac854779be153e66333932b313b 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
2	K_1	946405a7d912cff09df1a1d484685c6281a1ccfe6241add765d05505a51d070d 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	946405a7d912cff09df1a1d484685c6281a1ccfe6241add765d05505a51d070d 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	11b9d27c76f19f40b3f0ebc0f8b295a197d281c8f007cff943203deab9807874

5	K_2	fe0e6fcdb378a59af79bcbbeee023608ebcba694082bc7bd0fba3f6fcf776d67 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	fe0e6fcdb378a59af79bcbbeee023608ebcba694082bc7bd0fba3f6fcf776d67 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 11b9d27c76f19f40b3f0ebc0f8b295a197d281c8f007cff943203deab9807874
7	T	38267177accd62492078da956bfdf6587385dbbc52a1ea24bb4badabd77e6620

7 암호 키 길이가 입력 블록 크기보다 작은 경우 HMAC 참조구현값



7.1 LSH-224의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff0011223344556677889 9aabbccddeeff 00112233445566778899aabbccddeeff0011223344556677889 9aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999 9aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999 9aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff0011223344556677889 9aabbccddeeff 00112233445566778899aabbccddeeff0011223344556677889 9aabbccddeeff 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999 9aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999 9aaaabbbbccccddddeeeeffff
4	h	cc924a35063933f1f9035c961a5677554e108a195c0d038223f1014a
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c cc924a35063933f1f9035c961a5677554e108a195c0d038223f1014a
7	T	2e770a8e20008981e18ca05dcf4044309035287309889928a1d336fa

7.2 LSH-256의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	707bc8f3406bb886614bf7a1c5da9c137cd951bd4deb30ffe9c6da416c671b2c
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 707bc8f3406bb886614bf7a1c5da9c137cd951bd4deb30ffe9c6da416c671b2c
7	T	3857476a26c86fb08a83bc85a5efbd8d27970a840e4e6be2f079e276a9da3c28

7.3 LSH-384의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	fc9d977fd6f5733f2aea96ae6d6d75499f202099ae2831d2bbe6a903090b0c7b 5209ab8db57d2546dbfe9d3d246a6f15
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c

6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c fc9d977fd6f5733f2aea96ae6d6d75499f202099ae2831d2bbe6a903090b0c7b 5209ab8db57d2546dbfe9d3d246a6f15
7	T	1878f8c70a6e645bcbdf50b48b9688e43a583754ad89d8e40c92ee87f84f38e6 085dd5ce788c1ce525f1bf2ac141d210

7.4 LSH-512의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	281c1bbcac170f7ddb3b61848ad2ea8085b17b0cfd22777f2e5c913e743c2c7f 0fa1bb407610c823bbe5959ecb313080b30e4193bae77ff2365d20a0354f781e
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c

6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 281c1bbcac170f7ddb3b61848ad2ea8085b17b0cfd22777f2e5c913e743c2c7f 0fa1bb407610c823bbe5959ecb313080b30e4193bae77ff2365d20a0354f781e
7	T	e114c81e493de87bb011b350099949a41205f6f378b93c13bdc41aed1905fcf2 bde36701e6a007648aa1da155bb72709bd8b01c5e59bb8ad71e5a03ce598dd71

7.5 LSH-512-224의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	1ca809406aba474f76224ebb95c59b4b5d600eeb50621835e227e1e4
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c

6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 1ca809406aba474f76224ebb95c59b4b5d600eeb50621835e227e1e4
7	T	d6af7395daa3d8df1450ecec085079c03246e9941680ba6da1ed8d60

7.6 LSH-512-256의 단계별 참조구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	db0314575b1d098e15a343db318a887cd53a72a31fee825b1cff2413c3fa2d8b
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c

6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c db0314575b1d098e15a343db318a887cd53a72a31fee825b1cff2413c3fa2d8b
7	T	f2641cabad431106835e0592e3513a84f15fdf1c348a977fd88f8515d823e52e

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

해당 사항 없음

Ⅰ-2.2 시험표준 제정 현황

해당 사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

Ⅰ-3.1 TTAK.KO-12.0xxx-Part1

이 표준에서 제시하는 LSH를 사용하는 경우의 참조구현값에 대한 구성, 용어 정의 및 약어를 제시하는 '제1부 일반' 표준임

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] ISO/IEC 9797-2, “Information technology - Security techniques - Message Authentication Codes(MACs) - Part 2: Mechanisms using a dedicated hash- functions”, 2011.

※ 상기 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따름

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2018.12.xx	제정 TTAK.KO-12.0xxx-Part2	-	정보보호기반 (PG501)