TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-12.xxxx-Part2 제정일: 2018년 12월 xx일

해시 함수 기반 메시지 인증 코드 (HMAC) - 제2부: 해시 함수 SHA-2

The Keyed-Hash Message Authentication Code (HMAC) - Part2: Hash Function SHA-2

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-Part2
표준 초안 작성자	한상윤	NSR	선임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.xxxx-Part2
	주왕호	NSR	연구원	-	TTAK.KO-12.xxxx-Part2
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 SHA-2를 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, SHA-2를 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 NIST ISO/IEC 10118-3에 규정된 해시 함수 SHA-2를 적용한 결과로, SHA-2는 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 SHA-2 about implementation conformance.

2 Summary

The standard specifies the test vectors of HMAC based on SHA-2 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 SHA-2 specified in ISO/IEC 10118-3, the HMAC mechanism specified in Part 1: General. And, SHA-2 conforms to the specifications of the standard.

목 차

해시 함수 기반 메시지 인증 코드 (HMAC)
- 제2부: 해시 함수 SHA-2
(The Keyed-Hash Message Authentication Code (HMAC)
- Part2: Hash Function SHA-2)

1 적용 범위

이 표준은 해시 함수 SHA-2를 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	SHA-224	SHA-256	SHA-384	SHA-512
출력 블록 크기 L (바이트)	28	32	48	64
입력 블록 크기 B (바이트)	64	64	128	128

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	SHA-224
	5.2	SHA-256
	5.3	SHA-384
	5.4	SHA-512
(6절) 암호 키 길이가 입력 블록 크기보다 큰 경우 HMAC 참조구현값	6.1	SHA-224
	6.2	SHA-256
	6.3	SHA-384
	6.4	SHA-512
(7절) 암호 키 길이가 입력 블록 크기보다 작은 경우 HMAC 참조구현값	7.1	SHA-224
	7.2	SHA-256
	7.3	SHA-384
	7.4	SHA-512

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)

- FIPS PUB 180-4, “Secure Hash Standard(SHS)”, 2015. 8.

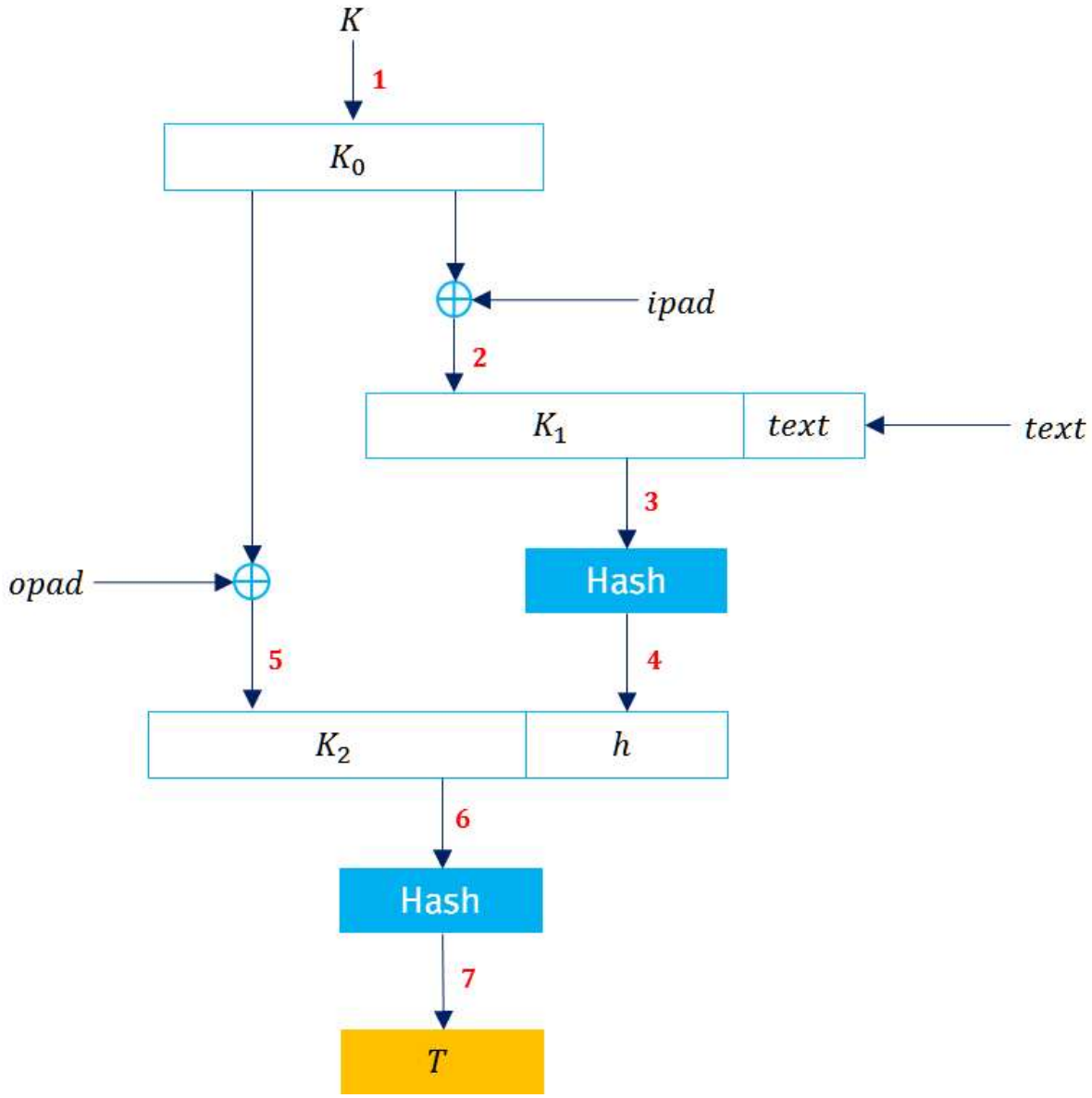
3 용어 정의

- 해당없음

4 약어

- 해당없음

5 암호 키 길이가 입력 블록 크기와 같은 경우 HMAC 참조 구현값



5.1 SHA-224의 단계별 참조 구현값

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

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	ef05578b1da2da8446d80cfae3e8f3b03f2874e3729f4651177cb94a
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 ef05578b1da2da8446d80cfae3e8f3b03f2874e3729f4651177cb94a
7	T	4fba592827fc48f737168d2093621e867bf9099d90feaa0b840928a2

5.2 SHA-256의 단계별 참조 구현값

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

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	a36ad086877874b7725f7f8da8048b5e2d8bfec2326995a4c712c6b5a37081fc
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 a36ad086877874b7725f7f8da8048b5e2d8bfec2326995a4c712c6b5a37081fc
7	T	f81f235e7c4abcf72fdf90fbcc03e38f2d352dc757b5ee452476d1d2903ee528

5.3 SHA-384의 단계별 참조 구현값

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

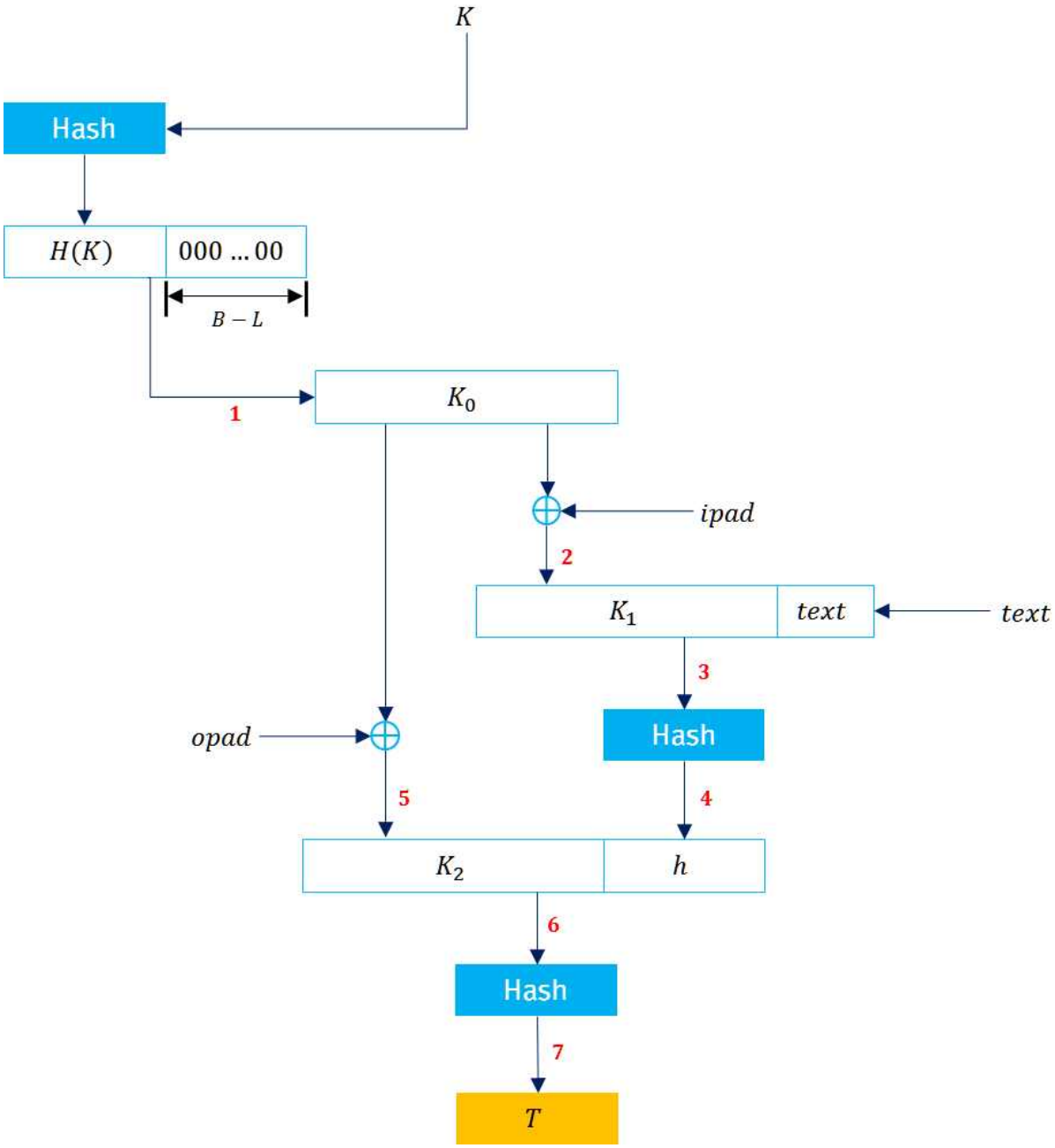
위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	38185a15b169d3fa3596104b6bdf3a269e9cbea4bb53e5de0dfbe36e3b51b58b 60a88208f6a783b5288a9cb9a7f37e1f
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 38185a15b169d3fa3596104b6bdf3a269e9cbea4bb53e5de0dfbe36e3b51b58b 60a88208f6a783b5288a9cb9a7f37e1f
7	T	58f64a63eb1ce882e87cbe42d5a86d62c3b3c6c523249da47a966a1d5549dcd8 966b940247d4b5b74f95cbb252c4f7bd

5.4 SHA-512의 단계별 참조 구현값

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	51908f9505b86a23928e92d7456e87b935aa6fe7ad2eec5b87df53fcd94da870 8bd03dc2cb780992d42fab1499eb1ad4fa05ea3d2416d132990ccf38ae96c6dd
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 51908f9505b86a23928e92d7456e87b935aa6fe7ad2eec5b87df53fcd94da870 8bd03dc2cb780992d42fab1499eb1ad4fa05ea3d2416d132990ccf38ae96c6dd
7	T	36b89649a59e58bdb83daef360ff65aac2630460ca606b1bfc1eb0172e56c7c3 f956a3a840ae99c845cf2cbfc92c09b1614375f57b59054439d8d94e898a15cf

6 암호 키 길이가 입력 블록 크기보다 큰 경우 HMAC 참조 구현값



6.1 SHA-224의 단계별 참조 구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	00001111222233334444555566667777888899999aaaabbbbccccddddeeeeffff 00001111222233334444555566667777888899999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	3f28db86d824ca45f878c34c9cc0fe97263ccc1af5bfdb8b88bb0dea00000000 0000000000000000000000000000000000000000000000000000000000000000
2	K_1	091eedb0ee12fc73ce4ef57aaaf6c8a1100afa2cc389edbdbe8d3bdc36363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	091eedb0ee12fc73ce4ef57aaaf6c8a1100afa2cc389edbdbe8d3bdc36363636 3636363636363636363636363636363636363636363636363636363636363636 00001111222233334444555566667777888899999aaaabbbbccccddddeeeeffff 00001111222233334444555566667777888899999aaaabbbbccccddddeeeeffff
4	h	0fe109eb6fa07c87c37d262884b44d04f5165c3b7b01911b2bf5e951
5	K_2	637487da84789619a4249f10c09ca2cb7a609046a9e387d7d4e751b65c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	637487da84789619a4249f10c09ca2cb7a609046a9e387d7d4e751b65c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 0fe109eb6fa07c87c37d262884b44d04f5165c3b7b01911b2bf5e951
7	T	c945b4d5390219cbc161afd8116473c7aebf2e97a63aeb3056da8511

6.2 SHA-256의 단계별 참조 구현값

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

위치	변수	중간값(16진수)
1	K_0	01292f14b6a98e99bad04755108ec11182e59962003783effeefdc2a8d9c744f 0000000000000000000000000000000000000000000000000000000000000000
2	K_1	371f1922809fb8af8ce6716326b8f727b4d3af543601b5d9c8d9ea1cbbaa4279 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	371f1922809fb8af8ce6716326b8f727b4d3af543601b5d9c8d9ea1cbbaa4279 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	9a9d542227cccb1a9b19cec32243bf0d2160cbcf48b45665fd28025c447c80d6
5	K_2	5d757348eaf5d2c5e68c1b094cd29d4ddeb9c53e5c6bdfb3a2b38076d1c02813 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	5d757348eaf5d2c5e68c1b094cd29d4ddeb9c53e5c6bdfb3a2b38076d1c02813 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 9a9d542227cccb1a9b19cec32243bf0d2160cbcf48b45665fd28025c447c80d6
7	T	f92029c46bd46d5cc36098018be87f16d369b574c71058a85059d1ce477f5025

6.3 SHA-384의 단계별 참조 구현값

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

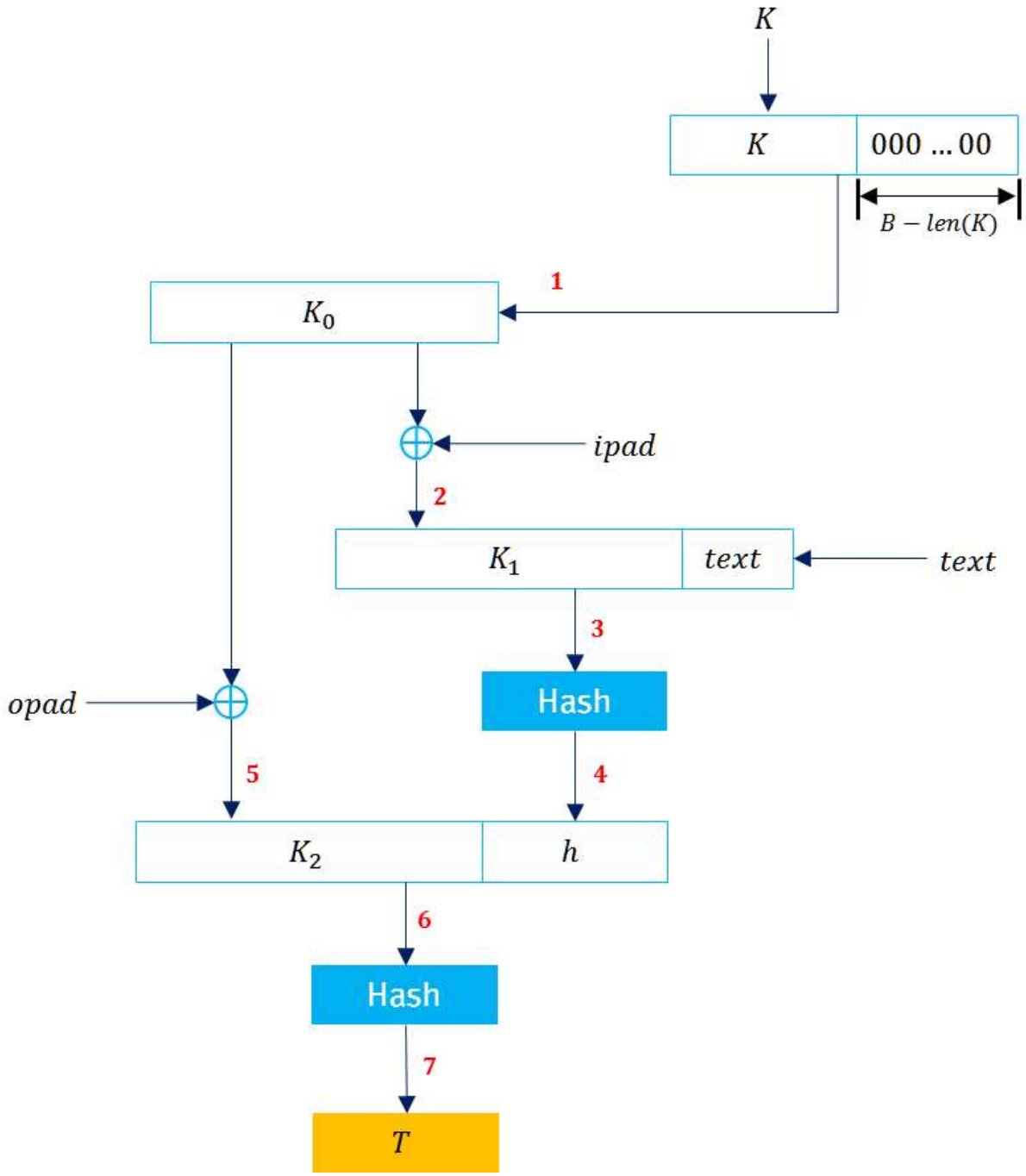
위치	변수	중간값(16진수)
1	K_0	7851116b205398d2a49f3392317b0f8e8459c0fdaa7e467aeced63328cd13eeb aad9a4df4d032de51f9eb0ac8025546800000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
2	K_1	4e67275d1665aee492a905a4074d39b8b26ff6cb9c48704cdadb5504bae708dd 9cef92e97b351bd329a8869ab613625e36363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	4e67275d1665aee492a905a4074d39b8b26ff6cb9c48704cdadb5504bae708dd 9cef92e97b351bd329a8869ab613625e36363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff
4	h	fde96e8cd240824805b9ad1e128ca5c6ec7513d603e7777a4b9797992018c0aa 827e25a016527281a732c52328eff8e8
5	K_2	240d4d377c0fc48ef8c36fce6d2753d2d8059ca1f6221a26b0b13f6ed08d62b7 f685f883115f71b943c2ecf0dc7908345c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	240d4d377c0fc48ef8c36fce6d2753d2d8059ca1f6221a26b0b13f6ed08d62b7 f685f883115f71b943c2ecf0dc7908345c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c fde96e8cd240824805b9ad1e128ca5c6ec7513d603e7777a4b9797992018c0aa 827e25a016527281a732c52328eff8e8
7	T	9f6d368724679805ec4984e3992851244c371fc062e0ac1c9756028b67d193da ed909b1e75d30d5f3f1b4a5c3c152780

6.4 SHA-512의 단계별 참조 구현값

입력	암호 키 (K)	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
	메시지 (text)	00001111222233334444555566667777888899999aaaabbbbccccddddeeeeffff 00001111222233334444555566667777888899999aaaabbbbccccddddeeeeffff

위치	변수	중간값(16진수)
1	K_0	f0c862f703d6369852ddbc0bb4df71cc6dd045aaa5cb577efbd5dddddd5d167e 68f5627ae810e376787465772b9dff5170d1bb9cf512bf1d66b0e8517210dd60 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
2	K_1	c6fe54c135e000ae64eb8a3d82e947fa5be6739c93fd6148cde3ebebeb6b2048 5ec3544cde26d5404e4253411dabc96746e78daac324892b5086de674426eb56 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	c6fe54c135e000ae64eb8a3d82e947fa5be6739c93fd6148cde3ebebeb6b2048 5ec3544cde26d5404e4253411dabc96746e78daac324892b5086de674426eb56 3636363636363636363636363636363636363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 00001111222233334444555566667777888899999aaaabbbbccccddddeeeeffff 00001111222233334444555566667777888899999aaaabbbbccccddddeeeeffff
4	h	d61e08c8788b74b0c40964453471e95a7e407dfd837855fd6a16391ae9eacba3 5dfd38de9fdee08ebc9f7371804e1417e85a594d15a66ec16904ab5d36b610f8
5	K_2	ac943eab5f8a6ac40e81e057e8832d90318c19f6f9970b22a789818181014a22 34a93e26b44cbf2a2428392b77c1a30d2c8de7c0a94ee3413aecb40d2e4c813c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	ac943eab5f8a6ac40e81e057e8832d90318c19f6f9970b22a789818181014a22 34a93e26b44cbf2a2428392b77c1a30d2c8de7c0a94ee3413aecb40d2e4c813c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c d61e08c8788b74b0c40964453471e95a7e407dfd837855fd6a16391ae9eacba3 5dfd38de9fdee08ebc9f7371804e1417e85a594d15a66ec16904ab5d36b610f8
7	T	6b7f0f9c8bcd3ed65af8efa2abdc030790dec7719f7d6191abda9e01c0d3430b 0deba93fba8df69e45368b2cfe773ef1b213a3c02a31681184b8a02f074f0b00

7 암호 키 길이가 입력 블록 크기보다 작은 경우 HMAC 참조 구현값



7.1 SHA-224의 단계별 참조 구현값

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

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00000000000000000000000000000000000000000000000000000000
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3636363636363636363636363636363636363636363636363636363636363636 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff
4	h	ff3ec43ee7c262a5df599abc7d00347a94a5914648d502ad65b5bf99
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c ff3ec43ee7c262a5df599abc7d00347a94a5914648d502ad65b5bf99
7	T	12fcb0e9fa3592a13c759d41b187e74ef52c0bc14a918d6faf39bc6d

7.2 SHA-256의 단계별 참조 구현값

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

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00000000000000000000000000000000000000000000000000000000000000000000000000000000
2	K_1	3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 36363636363636363636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	3627140572635041beaf9c8dfaebd8c93627140572635041beaf9c8dfaebd8c9 36363636363636363636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	32b2cf1924152a6ad68ff7a719e394a7dbcc99bd0d6e12977499cce2755c24f9
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 32b2cf1924152a6ad68ff7a719e394a7dbcc99bd0d6e12977499cce2755c24f9
7	T	ac2b70900244479378b652ef46f990a8471c2b59428fb0ab49b9e4cc2467ab05

7.3 SHA-384의 단계별 참조 구현값

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

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c936363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c936363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff 000011112222333344445555666677778888999aaaabbbbccccddddeeeeffff
4	h	48562630d1507d4a32a65f267bec9bd78bc8fbaa5529b48a828e837d0c77f421 55129fa14702951a8d78bad9da4ab82d
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 48562630d1507d4a32a65f267bec9bd78bc8fbaa5529b48a828e837d0c77f421 55129fa14702951a8d78bad9da4ab82d
7	T	676d781e4d119f8159ab94fb3bc7a8ad2c5c2c9dfbbf25b453a498ae9199bbee 6b82fdb962f65dc2a40dac292439b478

7.4 SHA-512의 단계별 참조 구현값

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

위치	변수	중간값(16진수)
1	K_0	00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff 00112233445566778899aabbccddeeff00000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000
2	K_1	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c936363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636
3	$data_1$	3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c9362714057263504 1beaf9c8dfaebd8c9 3627140572635041beaf9c8dfaebd8c936363636363636363636363636363636 3636363636363636363636363636363636363636363636363636363636363636 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff
4	h	bd447118ecb83a6fa76ff79691d3fb897d33bea39066e1bac2239200a3cfda5f a2f3af849b628116bd05b7a3299363d52b12aab6b7484c9b13c65d6621ed114e
5	K_2	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c
6	$data_2$	5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c4d7e6f18093a2bd4c5f6e79081b2a3 5c4d7e6f18093a2bd4c5f6e79081b2a35c5c5c5c5c5c5c5c5c5c5c5c5c5c5c 5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c bd447118ecb83a6fa76ff79691d3fb897d33bea39066e1bac2239200a3cfda5f a2f3af849b628116bd05b7a3299363d52b12aab6b7484c9b13c65d6621ed114e
7	T	4c793575e14ef25c81737c54142ca953d48d62da64886f5efdffeeeeb680f0c8 b3bebd5f8a2b0ec1ef88c40d70e5a7c5b670ccc03cf3d33a6ca57f7e895ad432

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 SHA-2를 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.

[2] ISO/IEC 10118-3, “Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions”, 2004.

※ 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)