TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-12.0274-Part1 개정일: 2018년 12월 xx일

패스워드 기반 키 유도 함수 - 제1부: 일반

Password-based Key Derivation Function - Part1: General

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	박제홍	NSR	책임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.xxxx
표준 초안 작성자	박제홍	NSR	책임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.xxxx
	김우환	NSR	책임연구원	-	TTAK.KO-12.xxxx
	한상윤	NSR	선임연구원	정보보호기반 프로젝트그룹 위원	TTAK.KO-12.0274
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

비밀로 관리되는 암호 키의 난수성은 암호 알고리즘의 안전성을 보장하는 핵심 요소이다. 그러나 사용자가 선택할 수 있는 암호 알고리즘의 비밀 요소가 패스워드(password)에 한정될 경우, 패스워드가 가지는 낮은 엔트로피와 약한 난수성으로 인해 암호 키로 직접 사용하는 데 한계가 있다.

이 표준의 목적은 패스워드(또는 패스프레이즈(passphrase))로부터 암호 키를 유도하는 방법을 제시하여, 저장 데이터 또는 데이터 보호에 사용되는 암호 키(data protection key)를 안전하게 보호하기 위한 것이다.

2 주요 내용 요약

이 표준은 패스워드(또는 패스프레이즈)를 입력으로 하여 암호 키를 생성하는 키 유도 함수를 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준은 NIST SP 800-132를 준용한다.

3.2 인용 표준과 본 표준의 비교표

TTAK.KO-12.0274-Part1	NIST SP 800-132	비고
1. 적용 범위	4. General Discussion	동일(번역)
2. 인용 표준	-	추가
3. 용어 정의	3. Definitions, Acronyms and Symbols	동일(번역)
4. 약어		
5. 패스워드 기반 키 유도 함수	5. Password-Based Key Derivation Functions	수정 (마스터 키 활용 방법 제외)

Preface

1 Purpose

The randomness of secret cryptographic keys is essential for the security of cryptographic applications. When passwords may be the only input required from the users who are eligible to access the data, however, they are not suitable to be used directly as cryptographic keys due to the low entropy and possibly poor randomness of those passwords.

The standard presents a mechanism for deriving cryptographic keys from a password(or a passphrase) for the protection of electronically-stored data or for the protection of data protection keys.

2 Summary

The standard provides a family of password-based key derivation functions (PBKDFs) for deriving cryptographic keys from a password(or a passphrase).

3 Relationship to Reference Standards

The standard conforms to the specification of PBKDFs in NIST SP 800-132.

목 차

패스워드 기반 키 유도 함수
- 제1부: 일반
(Password-based Key Derivation Function
- Part1: General)

1 적용 범위

패스워드(password)나 패스프레이즈(passphrase)는 일반적으로 사용자에 의해 선택되는 문자열로, 자원에 접근하려는 사용자를 인증하는 용도로 주로 사용된다. 사용자에 의해 선택된 패스워드의 대다수는 낮은 엔트로피와 약한 난수성을 가지기 때문에, 이러한 패스워드는 암호 키로 직접 사용할 경우 암호 알고리즘의 안전성을 보장할 수 없다. 하지만 저장 장치에 보관하는 데이터를 보호해야 하는 경우와 같은 특정 응용에서, 패스워드가 암호 알고리즘에 적용 가능한 유일한 비밀 정보일 수 있다. 이 표준에서는 패스워드로부터 암호 알고리즘에 사용 가능한 암호 키를 유도할 수 있는 패스워드 기반 키 유도 함수를 규정한다.

패스워드 기반 키 유도 함수는 사용자의 패스워드를 비밀 요소로 사용해야 하는 다양한 정보보호 시스템 및 암호제품에 활용되어 데이터의 안전성과 신뢰성을 제고할 수 있다.

2 인용 표준

NIST SP 800-132 (2010) Recommendation for Password-Based Key Derivation - Part 1: Storage Applications.

3 용어 정의

3.1 마스터 키(master key)
패스워드 기반 키 유도 함수로부터 출력된 키 요소

3.2 메시지 인증 코드(MAC, message authentication code)
데이터에 대한 무결성 제공을 위해 사용되는 대칭 키 암호 알고리즘으로, 임의 길이 입력 데이터에 작용하여 고정된 길이의 인증 태그(authentication tag)를 생성

3.3 솔트(salt)
패스워드 기반 키 유도 함수에 입력으로 사용되는 비트열로, 비밀로 관리되지 않으며 주어진 패스워드에 대응하는 키 후보 집합의 크기를 확장함

3.4 암호 키(cryptographic key)
암호 알고리즘에 의해 비밀 파라미터로 사용되는 비트열로, 고정된 길이의 랜덤 비트열이거나 랜덤 비트열과 계산상으로 구별 불가능한 같은 길이의 의사 난수 비트열

3.5 엔트로피(entropy)
데이터가 가지는 정보량을 수치로 나타낸 것. 무질서도(disorder) 또는 난수성(randomness)의 측정 기준

3.6 의사 난수 함수(PRF, pseudo random function)
주어진 정의역(domain)과 치역(range)에 대해 정의되는 모든 함수(function)의 집합에서 균등한 확률(uniform probability)에 따라 무작위로 선택된 함수(random function)와 구별이 어려우면서, 효율적으로 계산 가능한 함수

3.7 키 요소(key material)
요구 길이를 가지는 중첩되지 않는 각 부분(non-overlapping segments with the required lengths)이 대칭 키 암호 알고리즘의 암호 키로 사용될 수 있는 비트열

3.8 키 유도(key derivation)
하나의 암호 키로부터 키 요소(keying material)를 얻는 과정

3.9 키 유도 키(key derivation key)
다른 암호 키를 얻기 위해 키 유도 함수의 입력으로 사용되는 암호 키

3.10 키 유도 함수(KDF, key derivation function)
비밀 정보인 키 유도 키와 다른 (공개) 파라미터를 입력으로 받아, 키 요소(key material)를 출력하는 함수

3.11 패스워드(password)
특정 개체만이 알고 있는 문자열로 전산 시스템에 대한 사용자 인증이나 시스템 자원에 대한 접근 권한 확인에 사용되는 정보

3.12 패스프레이즈(passphrase)
단어의 조합으로 통상 20개 이상의 문자로 구성. 특정 개체만이 알고 있는 문자열로 전산 시스템에 대한 개체 인증이나 시스템 자원에 대한 접근 권한 확인에 사용. 이 표준에

서 패스워드의 사용과 관련하여 패스프레이즈가 패스워드와 함께 언급되지 않으면, 패스프레이즈의 사용 또한 허용되는 것으로 간주

3.13 해시 함수(hash function)

임의 길이의 메시지를 입력으로 받아 일정 길이의 출력값으로 압축하며, 다음 두 가지 성질을 가지는 암호 알고리즘

- 주어진 출력값에 대응하는 입력 메시지를 찾는 것이 어려움
- 주어진 입력 메시지에 대해, 같은 출력값을 가지는 다른 메시지를 찾는 것이 어려움

[출처] NIST SP 800-132

4 약어

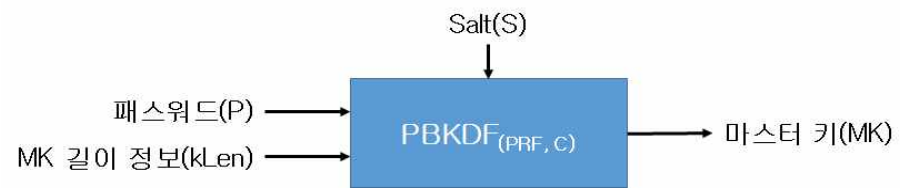
HMAC	Keyed-hash Message Authentication Code
PBKDF	Password-based Key Derivation Function
SHA	Secure Hash Algorithm

5 패스워드 기반 키 유도 함수

5.1 개요

키 유도 함수는 패스워드와 같이 비밀로 관리되는 값으로부터 암호 키 요소(key material)를 유도하는 데 사용되는 결정론적 알고리즘이다. 특히 패스워드를 입력받는 키 유도 함수는 기반이 되는 의사 난수 함수(PRF)와 반복 횟수(C)에 의해 정의된다.

패스워드 기반 키 유도 함수의 입력은 패스워드(P), 솔트(S), 마스터 키(MK)의 비트 길이 정보(kLen)를 포함한다. 패스워드 기반 키 유도 함수의 일반적인 구조는 (그림 5-1)과 같다.



(그림 5-1) 패스워드 기반 키 유도 함수 구조

이를 기호로 표기하면 다음과 같다.

$$MK \leftarrow PBKDF_{(PRF,\ C)}(P, S, kLen)$$

패스워드 기반 키 유도 함수의 계산 결과로 생성된 마스터 키는 데이터 보호에 사용되는 다수의 데이터 보호용 키(data protection key)를 생성하거나, 데이터 보호용 키의 안전한 관리에 사용되는 키 보호 키를 생성하기 위한 용도로 사용된다.

5.2 파라미터 요구사항

5.2.1 솔트(Salt)

솔트는 전체 또는 일부가 난수 발생기로부터 생성되어야 한다. 솔트에서 난수 발생기의 출력이 차지하는 부분의 비트 길이는 최소한 128 이상이어야 한다.

5.1.2 반복 횟수

반복 횟수 C는 고정값으로, 마스터 키의 한 블록을 생성하기 위해 필요한 의사 난수 함수(PRF)의 실행 횟수를 결정한다. 반복 횟수는 사용자로부터 입력되는 패스워드를 사용하여 암호 키를 생성하는데 필요한 시간이 허용되는 만큼 크게 설정하는 것이 좋다. 따라서 사용자 기기의 다양한 계산 능력에 따라 합리적으로 설정 가능한 반복 횟수가 달라진다.

권고하는 최소한의 반복 횟수는 1,000이지만, 고성능 시스템이나 사용자가 감지하는 성능(user-perceived performance)이 중요하지 않은 시스템에서의 반복 횟수는 10,000,000번이 적절하다.

5.1.3 출력 길이

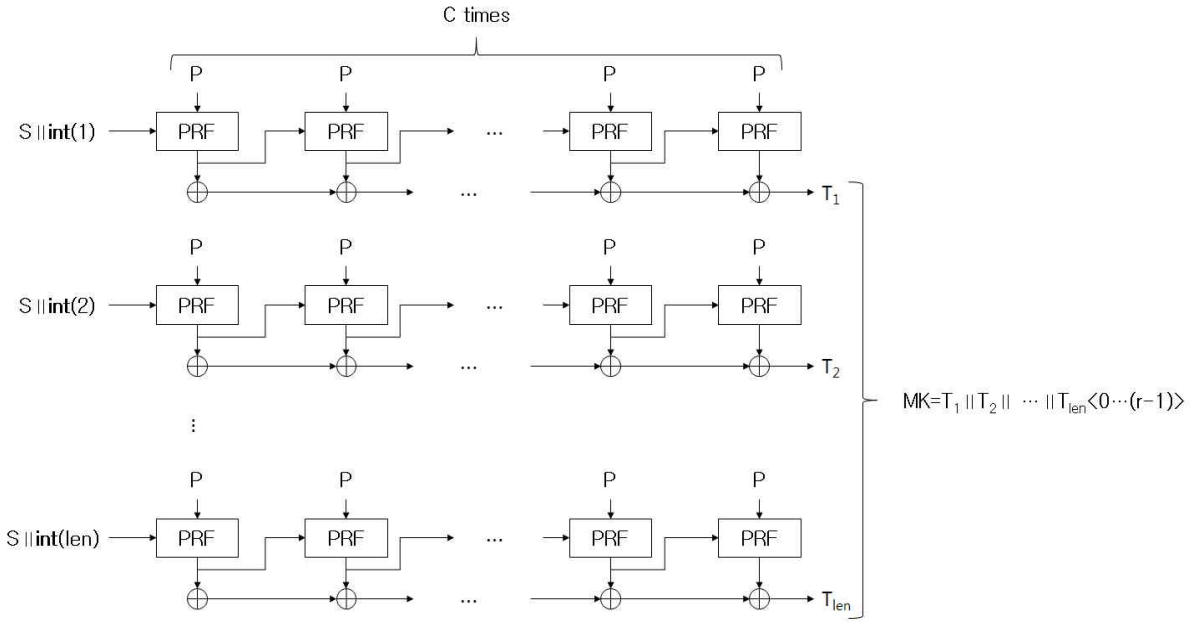
마스터 키의 비트 길이(kLen)는 최소 112 이상이어야 한다.

5.3 규격

패스워드 기반 키 유도 함수의 규격을 설명하기 위해 사용하는 기호를 정리하면 다음과 같다.

⌈x⌉	x와 같거나 큰 가장 작은 정수. x의 올림
hLen	의사 난수 함수(PRF) 출력의 비트 길이
int(i)	정수 i의 32 비트 표현
len(a)	문자열 a의 비트 길이
T<0…(r-1)>	비트열 T의 맨 왼쪽 r 비트 절삭

패스워드부터 마스터 키를 유도하는 방법은 (그림 5-2)와 같다.



(그림 5-2) 패스워드 기반 키 유도 함수 동작 과정

패스워드부터 마스터 키를 유도하는 구체적인 절차는 알고리즘 1과 같다. 이 표준에서는 의사 난수 함수(PRF)로 해시 함수 기반 메시지 인증 코드 알고리즘인 HMAC[2]을 사용한다.

알고리즘 1 패스워드 기반 키 유도 함수 PBKDF(·, ·, ·, ·)
입력: 비트열 *P*(패스워드), 비트열 *S*(솔트), 정수 *C*(반복 횟수), 정수 *kLen* 출력: 비트열 *mk*, len(*mk*) = *kLen*
1: **if** (*kLen* > ((2^{32} − 1) × *hLen*)) **then**
2: **return** an error indicator and stop
3: **end if**
4: *len* ← ⌈*kLen* / *hLen*⌉
5: *r* ← *kLen* − (*len* − 1) × *hLen*
6: **for** i = 1 **to** len **do**
7: T_i ← 0
8: U_0 ← *S*‖ **int**(i)
9: **for** j = 1 **to** *C* **do**
10: U_j ← HMAC(*P*, U_{j-1})
11: T_i ← T_i ⊕ U_j
12: **end do**
13: **end do**
14: *mk* ← T_1 ‖ T_2 ‖ ··· ‖ T_{len}<0···(r-1)>
15: **return** *mk*

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

해당 사항 없음

※ 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-12.0274-Part2

이 표준에서 제시하는 키 유도 함수의 기반 해시 함수로 SHA-2[3]를 사용할 경우의 참조 구현값을 제시함

Ⅰ-3.2 TTAK.KO-12.0274-Part3

이 표준에서 제시하는 키 유도 함수의 기반 해시 함수로 LSH[1]를 사용할 경우의 참조 구현값을 제시함

Ⅰ-3.3 TTAK.KO-12.0273-Part1

해시 함수 기반 메시지 인증 코드 알고리즘인 HMAC[2]을 의사 난수 함수(PRF)로 사용하는 세 가지 키 유도 함수의 상세 규격을 정의함

Ⅰ-3.4 TTAK.KO-12.0272

블록 암호 기반 메시지 인증 코드 알고리즘인 CMAC을 의사 난수 함수(PRF)로 사용하는 세 가지 키 유도 함수의 상세 규격을 정의하고, 국내 개발 주요 블록 암호 알고리즘(SEED, ARIA, HIGHT, LEA)을 CMAC의 기반 함수로 사용하는 경우의 참조 구현값을 제시함

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] TTA, TTAK.KO-12.0276, “해시 함수 LSH”, 2015. 12.

[2] TTA, TTAK.KO-12.0xxx, “해시 함수 기반 메시지 인증 코드 (HMAC) - 제1부: 일반”, 2018. 12.

[3] ISO, Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions, 2004. 3.

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	2015.12.16	제정 TTAK.KO-12.0274	-	정보보호기반 PG (PG501)
제2판	2018.12.xx	개정 TTAK.KO-12.0274-Part1	개별 해시 함수를 이용한 참조 구현값을 연계 표준으로 분리	정보보호기반 PG (PG501)