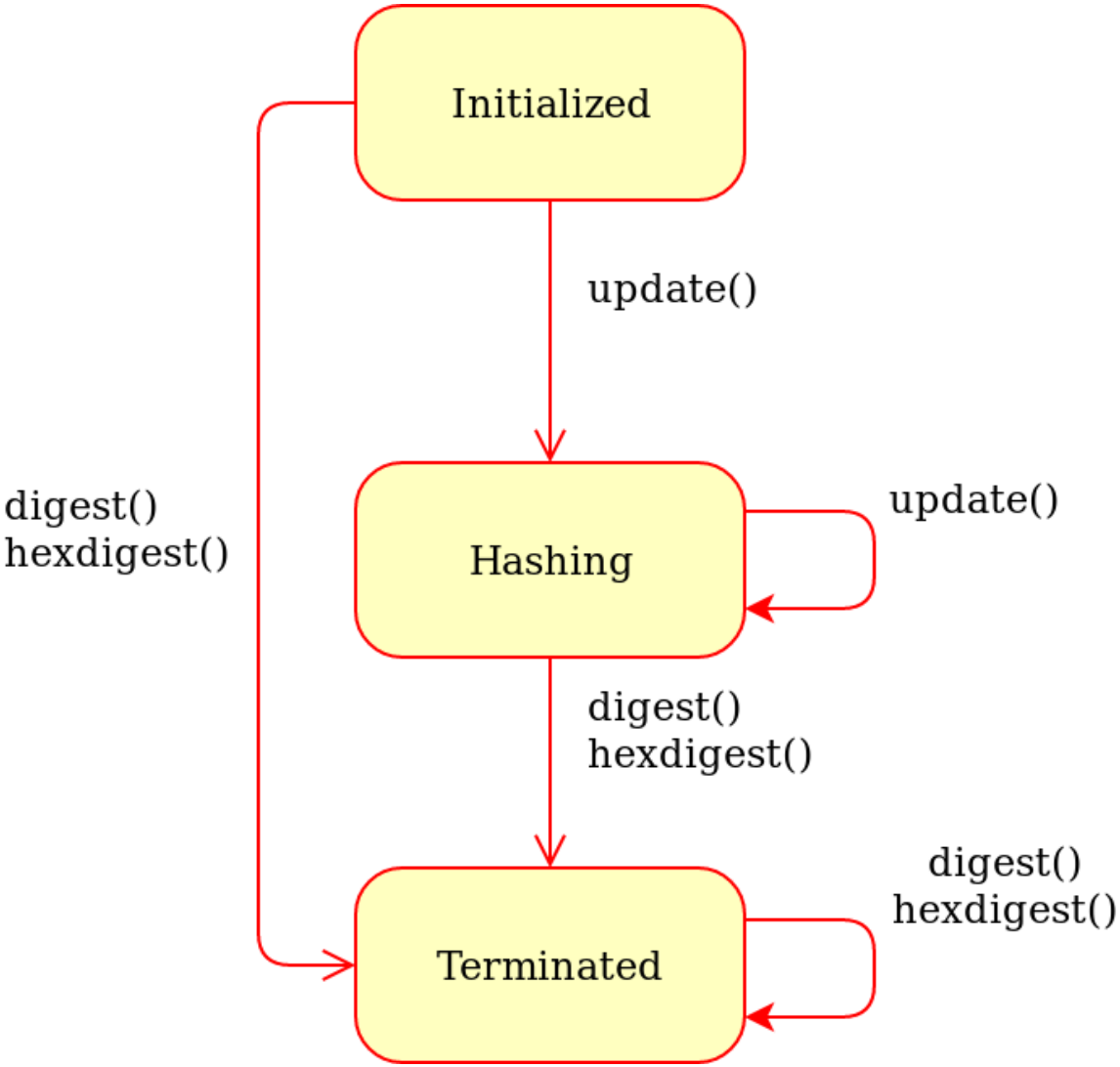
해시와 HMAC 실습

HASH


Initialized
update()
digest()
hexdigest()
Hashing
update()
digest()
hexdigest()
Terminated
digest()
hexdigest()

HASH

Instance Methods	
	__init__(self, data=None) Initialize the hash object.
	new(self, data=None) Return a fresh instance of the hash object.
Inherited from hashalgo.HashAlgo	
	copy(self) Return a copy ("clone") of the hash object.
	digest(self) Return the **binary** (non-printable) digest of the message that has been hashed so far.
	hexdigest(self) Return the **printable** digest of the message that has been hashed so far.
	update(self, data) Continue hashing of a message by consuming the next chunk of data.

Class Variables	
	oid = '₩x06₩t`₩x86H₩x01e₩x03₩x04₩x02₩x03' ASN.1 Object identifier (OID):
	digest_size = 64 The size of the resulting hash in bytes.

HASH

▶ 기본 사용 흐름

```
>>> from Crypto.Hash import SHA512
>>> hash_obj= SHA512.new ( data = b'First')  # 반드시 byte string
>>> hash_obj.update(b'Second')
>>> print ( hash_obj.digest()  )   # 종료하려면 digest or hexdigest
>>> print ( hash_obj.hexdigest() )
```

▶ 단축 실행

```
>>> print ( SHA512.new( b'FirstSecond').digest () )
>>> print ( SHA512.new( b'FirstSecond.').hexdigest () )
```

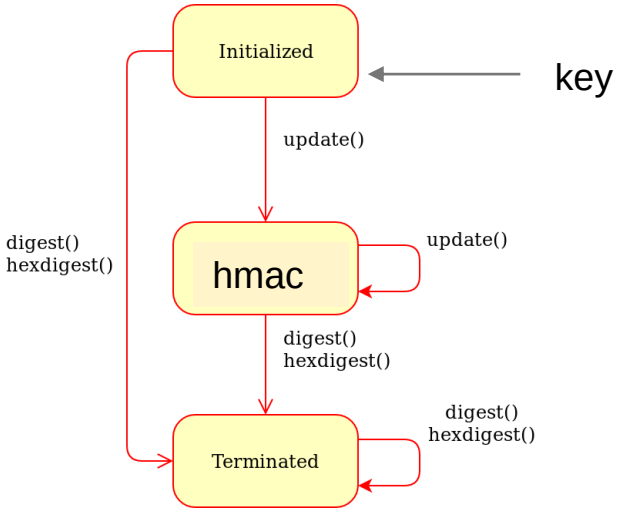
▶ 입력 차이에 따른 출력값 차이

```
>>> print ( SHA512.new( b'FirstSecond').hexdigest () )
>>> print ( SHA512.new( b'FirstSecone').hexdigest () )
```

PROOF OF WORK

- N개의 0 bit으로 hash값이 나오는 입력값 찾기
  - Brute force
  - N=1 이면 2번 시도
  - N=8 이면 2^8= 256번 시도 <- 확률적
- 0.py
  - SHA384
  - N bytes
- 과제 0 : 24 bits 00이 나오는 소스값 구하기
  - 0.py 및 0.jpg

HMAC




```
>>> from Crypto.Hash import HMAC
>>> h= HMAC.new ( b'password' )  # key
>>> h.update( b'First' )
>>> print ( h.digest()  )
>>> print ( h.hexdigest() )
```

무결성 비교

- 1.py
  - 동일하게 메시지를 HMAC하여 나오는 해시값 비교

과제1

- 1a.py
  - 1.txt를 읽어서 HMAC을 생성 (key를 사용자에게 입력받기)
    - 1.txt는 아무 파일이나 자신이 선택
    - HMAC 값을 print
  - 1.txt 파일 끝에 HMAC을 붙여서 H.txt로 저장
- 1b.py
  - H.txt을 읽어서 파일 무결성 검사 (key를 사용자에 입력 받기)
    - HMAC 값을 print
    - 무결하면 "OK" 아니면 "NOK"를 print

- 다음 순서대로 실행 후 화면 캡처 1-1.jpg

  $ python3 1a.py 실행

  $ cat H.txt

  $ python3 1b.py

- H.txt를 일부 수정 후 , cat과 1b.py를 다시 실행한 화면 캡처 1-2.jpg

숭실대학교 Soongsil University

과제 제출

- 모든 파일 (.py, .txt, .jpg) 을 03.zip으로 묶어서 제출