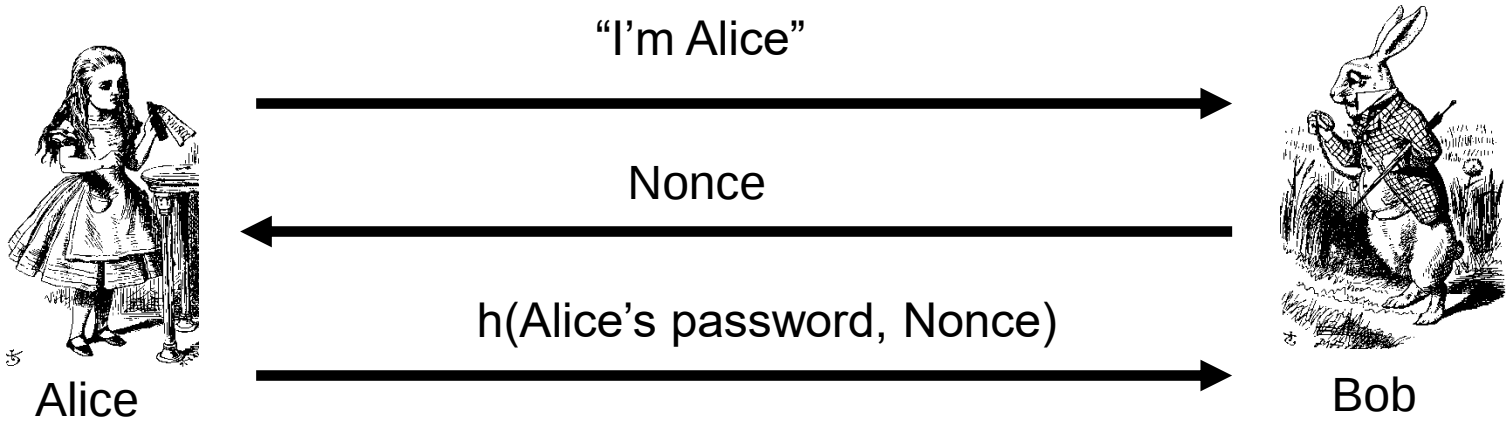
숭실대학교 Soongsil University

실습 05

CHALLENGE-RESPONSE



- Challenge 로 Nonce (Number once) random number
- Response 로 nonce로 부터 유도된 & Alice를 확인할 수 있는 값
- Hash 함수를 사용할 수도
- Replay 방지됨

CRYPTO PRIMITIVES

- Nonce

```
>>> from Crypto import Random
>>> nonce=Random.get_random_bytes (8)
```

- Hash

```
>>> from Crypto.Hash import SHA
>>> pw=b'1234'
>>> SHA.new ( pw+nonce ).digest ()
```

ENCODING

- JSON : text

```
>>> import json
>>> msg= json.dumps ( {'uid': "Alice }}
>>> json.loads ( msg )
```

- Bytes via JSON

```
>>> import base64
>>> msg = json.dumps ( {'nonce' : base64.b64enc
ode ( nonce ).decode() } )
```

SOCKET

- Client

```
>>> import socket
>>> c= socket.socket()
>>> c.connect ( ('127.0.0.1' , 2500))
>>> c.send ( "hello".encode() )
```

- Server (다른 터미널, 먼저)

```
>>> import socket
>>> s= socket.socket()
>>> s.bind ( ('127.0.0.1' , 2500))
>>> s.listen (10)
>>> con, a= s.accept()
>>> con.recv ( 1024 ).decode()
```

실습 파일

- c.py s.py

과제1

- Hash 대신 hmac 을 사용하기
  - c.py , s.py 수정하여 제출
  - 양쪽 실행결과 캡처 1.jpg