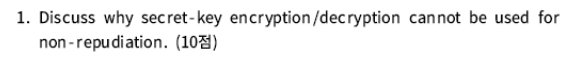
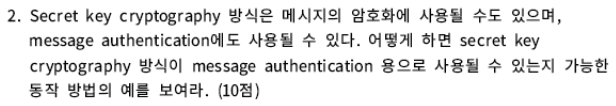
2016년 정보보안 중간



비밀키 암호화 방식의 암호화/복호화는 부인 방지 기능을 제공하지 않는 이유를

|  |
| --- |
| 비밀키 암호화 방식은 A(송신자) , B(수신자)끼리 사전에 둘만 아는 비밀키를 공유하고 송수신측 모두 이 비밀키를 사용해 암호화 /복호화 하는 방법이다. 이처럼 공유한 같은 키를 가지고 암호화 / 복호화가 가능하기 때문에 A가 만들 수 있는 암호문은 B 또한 만들 수 있다. 이때 A가 만든 암호문을 A가 만들지 않았다고 거짓 주장한다면 B는 A가 만든 암호문이라는 것을 증명할 수 없다. 때문에 공유된 같은 키를 가지고 암호화와 복호화를 한다면 부인 방지 기능을 제공할 수 없다. |



|  |
| --- |
| 보낼 데이터인 Message와 사전의 공유한 둘만 아는 비밀키를 같이 hash함수에 넣어서 signature를 만들어낸 뒤 전송할 message뒤에 같이 보낸다.그럼 수신측은 message와 signature를 수신하게 된다. 그러면 message와 공유한 비밀키를 사용해 수신측에서 검증할 signature를 만든다. (수신 측에서 사용한 hash함수 사용) 수신측에서 만든signature와 수신받은 signature를 비교해서 같다면 message가 변경되지 않은 것이고 틀리다면 송신중에 message가 변경됐다고 판단한다. 이는 둘만 아는 비밀키를 사용해 같은 signature를 만들어낼 수 있는 특성을 이용한 것이다. |

텍스트, 폰트, 화이트이(가) 표시된 사진

자동 생성된 설명

|  |
| --- |
| Mac은 비밀키 암호화 방식 중 하나로 공유된 비밀키로 message와 비밀키를 이용해mac값을 만들어 내고 이 값을 수신측에서도 같은 방법으로 이 비밀키를 이용해 mac값을 만들어 냄으로 데이터의 무결성을 검증하고, 송신자를 인증할 수 있다(서로 같은 키를 공유하고 있기 때문에 mac값이 동일하면 key를 공유한 송신자인 것을 인증).  Cryptographic Hash는 hash 함수를 사용해 hash값을 만들어 내는데 이때 키는 필요하지 않으며 공개된 알고리즘의 해쉬를 사용한다. 이는 수학적 함수를 이용해 message를 암호화 하는데 이는 해시값을 통해서 데이터를 역산하기 어려운 방법을 사용한 암호화 방법이다. 서로 공유하는 키를 사용하지 않기 때문에 데이터 무결성 검사는 가능하지만 사용자 인증은 할 수 없다. 그래서 데이터 요약과 데이터 비교에 사용된다. |

텍스트, 폰트, 화이트이(가) 표시된 사진

자동 생성된 설명

|  |
| --- |
| A의 인증서는 인증기관이 A 신원 정보, 공개 키, 인증서의 용도 등을 보장해준다. B가 A에게 인증서를 받았다고 가정했을 때 B는 A의 인증서에 있는 A의 공개키를 확인하는 방법은 먼저 인증서가 인증기관에 CA 서명의 유효성을 확인해야 한다. 이 과정을 통해 인증서가 위조 되지 않고 인증기관에 발급한 인증서임을 확인한다. 또한 인증서에 내용을 확인해 이름과 인증서의 발급자 정보를 확인한다.  혹시 C가 B에게 자신의 C 인증서를 A인증서라고 보낸 경우 인증서의 서명이 유효하지 않기 때문에 이것은 A의 인증서가 아니라고 판단하고 인증서를 신뢰하지 않는다. |