텍스트, 폰트, 화이트이(가) 표시된 사진

자동 생성된 설명

RSA : RSA 공개키 암호화 방식은 메시지를 암호화 할때 사용되는 공개키, 암호화된 메시지를 복호화하기 위한 개인키가 존재하며 두개의 키는 한쌍으로 생성되어 관리된다. (비대층키 암호화 알고리즘) AES 대칭키 암호화 방식에 비해 속도가 느린 단점을 갖지만 보안에 강점을 갖는다.

RSA 단점 : RSA를 이용해 digital signiture을 교환하는 용도로만 사용하고, key exchange를 사용하면 위험하다. key exchange는 Diffie-hellman을 사용하는게 안전하다. 위험한 이유는 PFS를 해야하기 때문이다. 숭수신측은 Shared key를 가지고 세션이 시작할때 계속 같은 Shared key를 사용하기 때문에 이전과 이후에 전달하는 세션이 모두 해킹에 노출된다.

1. RSA는 송신할 A측은 두개의 public key(ku)와 private key(kr)를 만들고 public key를 B에게 보낸다. 수신한 B는 무작위로 shared key(sk)를 만들고, A측의 public key를 사용해 암호화해서 다시 A에게 암호화된 shared key를 보낸다. 이러한 과정으로 다음부터 사용할 shared key를 양측이 공유하게 된다. 만약 A가 B에게 public key로 암호화된 c를 보내는데 중간자가 mitm acttack으로 c를 가로채 중간에 c를 c’으로 바꿔치기를 할수 있다. 이때 c’은 A의 public key와 n(mod n)값을 가지고 변형된 c’을 만든다. 이때 만들어진 c’는 암호문(c)을 복호화 하지 않고도 평문을 추측해 잘못된 평문으로 B에게 전달시킬수 있다.
2. 이 문제가 발생하는 이유는 가)의 RSA방식은 암호화 할 때 난수를 사용하지 않아서 같은 메시지를 암호화하면 항상 같은 암호문이 나오기 때문이다. 때문에 메시지를 암호화 할때마다 난수를 생성하고 이 난수로 메시지를 암호화해 X와 Y를 만들어 사용한다. 이 방법을 사용하면 같은 메시지라도 다른 암호문으로 나오기 때문에 평문을 추측할 수 없다.

텍스트, 폰트, 영수증, 화이트이(가) 표시된 사진

자동 생성된 설명

Digital signature (전자 서명)은 위조될 가능성이 매우 희박하고, 전달하는 메시지가 수정 되었는지 누가 보냈는지 알 수 있다.

1. m(메시지)을 hash 함수(sha2,sha3)를 사용해 message digest로 만든 뒤 수신측의 private key로 암호화해 Digital signature을 만들어낸다. 만들어진 Digital signature는 m와 함께 송신된다.  
    텍스트, 도표, 스크린샷, 원이(가) 표시된 사진

   자동 생성된 설명
2. 수신측은 m(메시지)와 암호화된 Digital signature를 수신한다. m은 hash 함수(sha2,sha3)를 사용해 message digest로 만들고 암호화된 Digital signature를 public key를 사용해 복호화 한다. 복호화된 값과 message digest을 비교해 같다면 데이터가 공격 받지 않고 변경, 위조되지 않았다고 생각할 수 있다.   
   텍스트, 스크린샷, 도표, 폰트이(가) 표시된 사진

   자동 생성된 설명

텍스트, 영수증, 폰트, 대수학이(가) 표시된 사진

자동 생성된 설명

# 2016 중간

1. discuss why secret-key encryption, decryption can not be used for non repudiation

**- 비밀키 암호화 방식(대칭키)이 복호화를 부인 방지에 사용할 수 없는 이유는?**

비밀키(대칭키) 암호화 방식 : 데이터를 암호화및 복호화 하는데 동일한 비밀키 한 개를 사용한다. 비밀키 암호화 방식에서 비밀키의 크기는 [공개키](https://terms.tta.or.kr/dictionary/dictionaryView.do?subject=%EA%B3%B5%EA%B0%9C+%ED%82%A4)에 비해 상대적으로 작고 [암호 알고리즘](https://terms.tta.or.kr/dictionary/dictionaryView.do?subject=%EC%95%94%ED%98%B8%EC%95%8C%EA%B3%A0%EB%A6%AC%EC%A6%98) 내부 구조가 단순하여 암호화와 [복호화](https://terms.tta.or.kr/dictionary/dictionaryView.do?subject=%EB%B3%B5%ED%98%B8%ED%99%94) [처리 속도](https://terms.tta.or.kr/dictionary/dictionaryView.do?subject=%EC%B2%98%EB%A6%AC+%EC%86%8D%EB%8F%84)가 [공개키](https://terms.tta.or.kr/dictionary/dictionaryView.do?subject=%EA%B3%B5%EA%B0%9C+%ED%82%A4) 암호화 방식에 비해 매우 빠르다. 반면 송신자와 수신자가 동일한 비밀키를 공유해야 하는데 비밀키를 분배하는 과정 중 누출이 되면 누구라도 암호문을 [복호화](https://terms.tta.or.kr/dictionary/dictionaryView.do?subject=%EB%B3%B5%ED%98%B8%ED%99%94)할 수 있는 단점이 있다.

부인방지란 송신자나 수신자가 메시지를 주고받은 사실을 부인하지 못하도록 방지하는 것 을 말한다. 비밀키 암호화 방식은 같은 비밀키를 송신자와 수신자가 공유하며 메시지를 복호화하고 암호화한다. 송신하는 측과 수신하는 측은 항상 같은 키로만 복호화 암호화하기 때문에 수신측이 암호화 하였는지 송신측이 암호화 하였는지 알 수 없다. 예를 들어 A(송신자), B(수신자)가 메시지를 주고 받는데 A가 보낸 메시지를 A가 부정하며 B가 만들어낸 메시지라고 주장한다면 B는 A가 만든 메시지라고 증명할 수 없다.

텍스트, 폰트, 화이트, 대수학이(가) 표시된 사진

자동 생성된 설명