2017년 정보보안 중간

텍스트, 폰트, 화이트, 영수증이(가) 표시된 사진

자동 생성된 설명

1. confidentiality (기밀성) : 외부 다른 사용자에게 정보가 노출되지 않도록 하는 특성. 통신중에 정보가 노출 되는 것을 막는 암호화 과정을 거친다. 인가 된 사용자만 정보에 접근할 수 있게한다.
2. integrity (무결성) : 승인되지 않은 사람이 정보를 수정할 수 없게 한다. 통신중에 외부에서 메시지를 변경, 손상시키지 않고 전달해야 한다.

텍스트, 폰트, 화이트, 영수증이(가) 표시된 사진

자동 생성된 설명

텍스트, 폰트, 번호, 스크린샷이(가) 표시된 사진

자동 생성된 설명




1. AES 키 길이(대칭키 알고리즘) : 128bits 이상의 키 길이를 사용한다. 부루트 포스 방식의 공격을 막기 위해 키의 길이가 충분히 커야한다.
2. RSA 키 길이(비대칭키 알고리즘) : 1024, 2048 bit를 가장 많이 사용한다. 키 길이가 길어질 수록 안전해지지만, 암호화 복호화 시간이 길어진다.
3. ECC 키 길이(비대칭키 알고리즘) : 타원곡선을 사용한 암호화 기법으로 이산대수를 활용한 암호화 방식을 사용하기 때문에 복잡한 구조를 갖고있다. RSA 보다 짧은 키를 사용한다.
4. 송수신자가 서로 비밀 key를 공유하고 이 key를 가지고 암호화, 복호화에 사용한다. 그렇기 때문에 처리속도는 비대칭키 알고리즘보다는 빠르다.
5. 암호화하는public key와 복호화하는 private key와 같이 key를 2개 사용한다. 하지만 암호화 복호화 방식이 매우 복잡해지기 때문에 처리속도는 대칭키보다 느리다.
6. RSA와 ECC의 보안 강도가 같다고 할 때 키의 길이는 RSA가 더 길고 ECC의 Key의 길이는 더 짧다. 때문에 처리 속도는 ECC가 RSA 보다 더 빠르다.
7. Message 인증코드로 사용 할 수 있다.
8. 인증과 전자 서명에 이용