2020 정보보안 중간고사

텍스트, 폰트, 화이트, 대수학이(가) 표시된 사진

자동 생성된 설명

1. Diffie-Hellman은 송수신간 비밀키 안전한 교환을 위해서 사용된다.

Alice와 Bob가 서로 통신을 위하여 키를 교환한다고 가정하면,   
Alice는 먼저 매개변수 p(소수), g(적당한 수)를 정의한다.  
Alice는 A = g^a mod p (a는 무작위 정수)를 만들고 Bob에게 p, q, A를 전송한다.

Bob은 B = g^b mod p (b는 무작위 정수)를 만들고 Alice에게 B를 전송  
Alice는 전송받은 B를 이용해 B^a mod p 연산을 한다.

Bob는 전송받은 A를 이용해 A^b mod p 연산을 한다. mod연산의 특징을 이용해  
이때 Alice는 (g^b)a mod p가 되고, Bob은 (g^a)b mod p가 된다.  
따라서 (g^b)a mod p = (g^a)b mod p가 되기 때문에 서로 직접키를 전달하지 않아도 같은 키를 공유할 수 있게 되었다.

1. FS : 세션의 비밀 정보를 현재 또는 미래의 공격자로부터 보호하는 보안 속성이다. 통신 세션을 위한 키를 생성하여 과거에 사용된 키에 대한 정보를 저장하지 않아 현재와 미래의 통신에 영향을 미치지 않는다.  
   PFS : PFS는 FS의 더 강화된 형태로, 모든 통신 세션에 대해 각각 고유한 키를 사용하여 완벽한 순방향 비밀 보장을 제공합니다. FS는 이전 통신 세션의 정보를 보호하고 새로운 통신에 대한 새로운 키 생성을 지원하지만, 덜 엄격하게 동작합니다. PFS는 모든 통신 세션에 대한 고유한 보안 키를 사용하여 모든 정보 유출 가능성을 제거합니다.

텍스트, 폰트, 화이트, 서예이(가) 표시된 사진

자동 생성된 설명

데이터의 비트 또는 바이트를 한번에 하나씩 암호화하는 대칭키 암호화 알고리즘이다.

암호화 : 키 스케줄링 이후 PRNG와 암호키를 사용하여 키 스트림을 생성한다. 그리고 평문과 bit단위로 xor연산을 통해 암호문을 얻는다.

복호화 : 동일한 방법으로 키 스케줄링 이후 동일한 암호키를 이용해 키 스트림을 생성한다. 그리고 암호문과 생성한 키 스트림을 xor연산을 통해 평문을 얻는다.

텍스트, 폰트, 화이트, 타이포그래피이(가) 표시된 사진

자동 생성된 설명

1. **Nonce (Number Used Once):**
   * Nonce는 오직 한 번만 사용되는 값입니다. 이것은 특히 인증 및 암호화에서 중요한 역할을 합니다.
   * Nonce는 주로 키 스트림 생성, 플레이너 텍스트와 암호문의 매칭, 무결성 검사, 중복 메시지 방지 등 다양한 보안 작업에 사용됩니다.
   * Nonce는 보통 난수 생성기를 사용하여 생성하며, 매번 다른 값을 가져야 합니다.
2. **IV (Initialization Vector):**
   * IV는 대칭 암호화에서 사용되는 고유한 초기화 값으로, 블록 암호화 모드 (예: CBC - Cipher Block Chaining)에서 주로 사용됩니다.
   * IV의 주요 역할은 같은 평문 블록이 동일한 암호문 블록으로 변환되는 것을 방지하고, 암호문의 예측 불가능성을 확보하는 것입니다.
   * IV는 각 암호화 블록마다 사용되며, 무작위성과 고유성이 필요합니다. 일반적으로 랜덤하게 생성되거나, 카운터, 타임스탬프 또는 다른 방법을 사용하여 고유한 값을 얻습니다.
3. **Salt:**
   * Salt는 주로 비밀번호 저장 및 해싱에서 사용되는 임의의 값을 가리킵니다.
   * Salt는 사용자의 비밀번호를 보다 안전하게 저장하도록 도와줍니다. 이것은 레인보우 테이블 공격과 같은 공격을 어렵게 만듭니다.
   * 각 사용자에게 다른 Salt를 할당하여 동일한 비밀번호를 가진 사용자들이 동일한 해시 값을 가지지 않도록 합니다. 이렇게 함으로써 레인보우 테이블과 같은 사전 공격을 효과적으로 방지합니다.

텍스트, 폰트, 화이트, 타이포그래피이(가) 표시된 사진

자동 생성된 설명