AES에서 키 생성

■ AES에서 키 생성

- 암호화와 복호화에 사용할 비밀키(secret key)를 무작위로 생성하는 과정
- 키의 길이는 보안 수준에 따라 128, 192, 또는 256비트 중 하나로 선택됨

■ AES 키 생성의 핵심 개념

- 대칭키 암호화 방식

  * AES는 하나의 키로 암호화와 복호화를 모두 수행

  * 이 키는 반드시 송신자와 수신자 사이에 안전하게 공유되어야 함

  * 키 길이
    - AES-128 : 128비트 키 (16바이트)
    - AES-192 : 192비트 키 (24바이트)
    - AES-256 : 256비트 키 (32바이트)

  * 랜덤성 확보
    - 키는 예측 불가능해야 하므로, 보안적으로 안전한 난수 생성기 (CSPRNG)를 사용해 생성함

■ 키 생성 시 주의사항

- 절대 예측 가능한 값 사용 금지
  * 날짜, 사용자 입력, 단순한 패턴 등은 키로 부적합
- 키 저장 위치 보안
  * 생성된 키는 안전한 저장소(HSM, 키 관리 시스템 등)에 보관해야 하며, 노출되면 전체 암호화 시스템이 무력화됨

- 키 교환은 별도 방식 사용
  * 대칭키는 안전하게 공유해야 하므로, 일반적으로 RSA 같은 비대칭키 암호화로 키를 전달하거나, TLS 같은 보안 프로토콜을 사용함