AES 같은 대칭키 암호화에서의 키 공유 방식

■ 키 공유 방식은 중요

* 암호화와 복호화에 같은 키를 사용하기 때문에, 이 키가 안전하게 전달되지 않으면 전체 보안이 무너질 수 있기 때문임

■ 대칭키 공유 방식의 대표적인 방법

- 실제 보안 시스템에서는 대칭키의 속도 + 비대칭키의 안전성을 결합한 하이브리드 암호화 방식이 널리 사용됨

- 예를 들어, 웹사이트 접속 시 HTTPS는 RSA로 AES 키를 안전하게 교환한 뒤, 본문은 AES로 빠르게 암호화!!!

1. 오프라인 방식 (물리적 전달)
    * USB, 보안 토큰, 종이 등에 키를 저장해 직접 전달
    * 장점 : 네트워크를 통하지 않아 도청 위험 없음
    * 단점 : 느리고 불편하며 분실 위험 있음

2. 비대칭키 암호화를 이용한 키 교환 (하이브리드 방식)
    * RSA, ECC 같은 공개키 암호화로 대칭키를 암호화해 전달
    * 예 : Alice가 Bob의 공개키로 AES 키를 암호화 → Bob만 자신의 개인키로 복호화 가능
    * TLS(HTTPS)에서도 이 방식 사용

3. Diffie-Hellman 키 교환 (DH, ECDH)
    * 서로 키를 직접 주고받지 않고, 공개된 수학적 값을 교환해 동일한 비밀키를 계산
    * 중간자 공격(MITM) 방지를 위해 인증서나 서명과 함께 사용해야 안전

4. 키 분배 센터 (KDC, Key Distribution Center)
    * 중앙 서버가 각 사용자에게 키를 안전하게 배포
    * Kerberos 같은 인증 시스템에서 사용