X3DH란 ? (보안 관련)

사람	도경원

1. X3DH – 초기 키 교환 (처음 대화 시작)

등장 인물

- 📱 **Alice (보내는 사람)**
- 📲 **Bob (받는 사람)** – 오프라인 상태일 수도 있음
- ☁️ **Server (메시지 서버)** – PreKeys 보관소 역할

Bob이 서버에 미리 올려둔 4가지 키

키 이름	설명
Identity Key (IK)	Bob의 장기 비공개/공개 키
Signed PreKey (SPK)	중간기한 키, 서명되어 있음
One-time PreKey (OPK)	단 한 번 쓰고 버리는 키
PreKey Signature	SPK가 진짜 Bob의 것임을 증명

Alice가 메시지를 보낼 때 하는 일

1. 서버에서 Bob의 키들 (IK, SPK, OPK)을 가져옴
2. **자신의 임시 키(EPK, Ephemeral Key)를 생성**
3. 아래의 4가지로 Diffie-Hellman 계산:

```
DH1 = DH(IK_Alice, SPK_Bob)
DH2 = DH(EPK_Alice, IK_Bob)
DH3 = DH(EPK_Alice, SPK_Bob)
DH4 = DH(EPK_Alice, OPK_Bob) ← optional
```

1. 이 DH 값들을 합쳐 **shared secret** 생성
2. 여기서 나온 secret으로 메시지를 암호화해서 보냄

> 결과: 처음 연결인데도 완벽한 E2EE 가능!