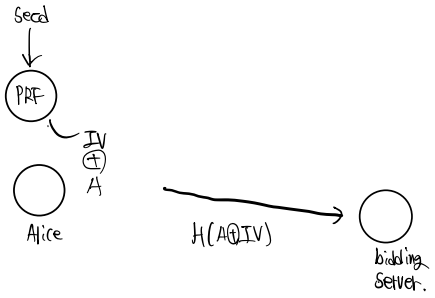
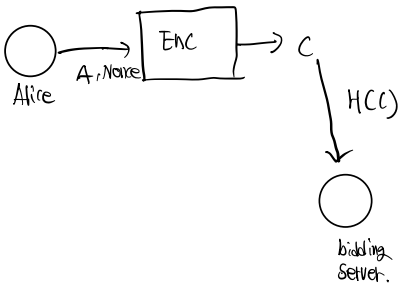
문제: online bidding을 통해 입찰을 했을 경우 사용자의 입찰금액을 hash함수에 넣어 나온 결과를 입찰서버로 전달한다.
하지민 해당 과정에서 한가지 문제가 나온다. -> 다른이의 입찰금액을 흘러가는 hash값을 보고 추정할 수 있다.

Sol 1. Random한 IV를 통해 문제를 해결한다.



1. Alice가 A라는 금액을 입찰금액으로 설정하였을때 서버쪽으로
IV라는 random한 값을생성해 X라는 값과 A의 값을
Hash함수에 넣어 제공한다.
2. 추출금액 공개를 할때 원래 결제금액 A와 IV를 생성한 Seed값을
알려준다.
3. 나머지 결제사항은 IV를 생성한 Seed와 A의 값을 AES하여
한다.

Sol 2. 값을 암호화하고 이것을 hash 함수에 넣어서 전송한다.



1. Alice가 Nonce based CBC를 통해 생성한 암호문을
hash 함수에 넣어 bidding Server에 제공
2. 추후 값을 제공할때 Nonce는 서버서버와 공유 했다 가정하면
A를 통해 일치가능.