suppose Bob has made an important discovery.

He wants to record publicly what he has done. but he does not want anyone else to know.

**Goal** allow Alice to sign a document without knowing its contents.

Alice — Bob.

1. execute RSA.KeyGen($1^n$).

$pk = (n, e_A)$. $sk = (p, q, d_A)$

2. choose a random $r \xleftarrow{\$} \mathbb{Z}_n$ with $\gcd(r, n) = 1$.

compute $\underline{t \equiv r^{e_A} m \pmod n}$

reveals no information of $m$. ($\because$ $r$: random)

3. compute $s \equiv t^{d_A} \pmod n$

4. compute $\sigma := s/r$

Since $s/r \equiv t^{d_A}/r \equiv (r^{e_A} m)^{d_A}/r \equiv m^{d_A} \bmod n$,

$\sigma$ is a signed message of $m$.

**Dangers of RSA Blind Signature**

Suppose Bob has a ciphertext $c = \mathrm{Enc}(m)$ encrypted through RSA.

In Step 2, $t \equiv r^e c \equiv (m^e \bmod n)\, r^e \equiv (mr)^e \bmod n$

In Step 3, $s \equiv t^d \equiv (mr)^{ed} \equiv mr \bmod n$

In Step 4, $\sigma = s/r \equiv m \bmod n$ since $\gcd(r, n) = 1$