RSA Signature

- Keygen(1^λ) ; choose two large prime p and q. and $n = pq$.
  choose e_A s.t. $1 < e_A < \phi(n) = (p-1)(q-1)$
  $\gcd(e_A, \phi(n)) = 1$
  compute d_A s.t. $e_A d_A \equiv 1 \mod \phi(n)$.
  output $pk = (e_A, n)$ and $sk = (d_A, p, q)$.
  (cf. in RSA-PKE, $pk = (d_A, n)$ and $sk = (e_A, p, q)$)

- Sign(sk, m) ; output $(m, m^{d_A} \mod n)$:

- Verify(pk, m, σ) ; compute $\sigma^{e_A} \mod n$. $(\sigma^{e_A} \equiv m^{d_A e_A} \equiv m)$.
  if $m = \sigma^{e_A}$, output 1.
  if $m \neq \sigma^{e_A}$, output 0.

- A signed message m is revealed.
- How to generate a signature while protecting a message?.
  → blind signature which will be covered in the next time.

- If m is long, $(m, \sigma(H(m)))$ instead of $(m, \sigma(m))$ where H is a hash function.
  Suppose $(m, \sigma(H(m)))$: for Alice's signature. and Eve has $m' \neq m$ to which she wants to add $\sigma(H(m))$.
  It implies that $\sigma(H(m)) = \sigma(H(m')) \Rightarrow H(m) = H(m')$.
  By Hash function, it is hard to find m and m' s.t. $H(m) = H(m')$.