ECE 471/571 Digital Signature Applications

Cube root problem:

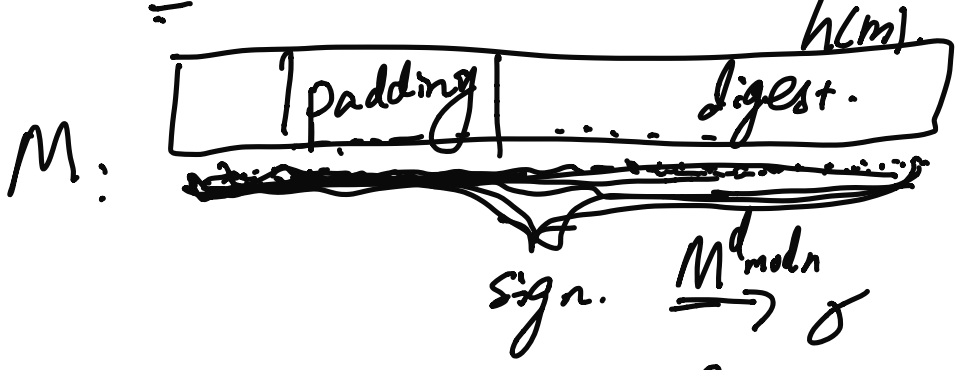
$\sigma = (h(m))^d \bmod n$

$e = 3.$

$\sigma' \simeq \sqrt[3]{h(m)}$ → round → integer σ

$h(m) = \sigma^3 \bmod n$

$(m, \sigma) \rightarrow$ verify $\rightarrow$ true/false



$M \simeq \sigma'^3 \bmod n$

---

① $sig_{sk_A}\{E_{PK_B}[sig_{sk_A}(x) \| x]\}$

$sig_{sk_A}\{E_{pk_C}[sig_{sk_A}(x) \| x]\}$ ✗ Bob cannot forward to charlie as he needs to forge Alice's

(2).

signature

$$E_{PK_B}\left[E_{PK_B}(X),\ sig_{SK_A}(E_{PK_B}(X))\right]$$