ECE 471/571 RSA (cont'd).

$e=3$

①. $c = m^3 \bmod n$ if $m < n^{\frac{1}{3}}$

$m^3 < n$.

$m = \sqrt[3]{c}$ cube root problem

solution? pad m s.t $m > n^{\frac{1}{3}}$

$m \| 0010001\ldots$

②. encryt m using 3 public keys $e=3$

$$c_1 = m^3 \bmod n_1 \equiv a_1 \bmod n_1$$
$$c_2 = m^3 \bmod n_2 \equiv a_2 \bmod n_2$$
$$c_3 = m^3 \bmod n_3 \equiv a_3 \bmod n_3$$

$m^3 > n_1$. solve for

$> n_2$

$> n_3$

$$C \equiv m^3 \bmod n_1 n_2 n_3$$

$m^3 < n_1 \cdot n_2 n_3$

CRT. $C^{\frac{1}{3}} = m$

solution? pad m w/ different numbers for n_1. n_2. n_3.

1st $m \| 000\cdots1$.

$m \| 100\cdots1$.

$m \| 110\cdots$

$\vdots$

chosen ciphertext attack for RSA.

$$C_1 = m_1^e \bmod n.$$

$$C_2 = m_2^e \bmod n.$$

$$C = \underline{C_1 \cdot C_2} = m_1^e m_2^e \bmod n.$$

$$= \underline{(m_1 \cdot m_2)}^e \bmod n$$

$$m = m_1 \cdot m_2$$

Adv: homomorphic. encryption.

given.

$$\langle \underline{C}, m \rangle \xrightarrow{\hspace{2cm}} \underline{C_2}, \rightarrow \underset{\longrightarrow}{\frac{m}{m_1}}.$$

$$\xrightarrow{D}$$

recover

$$\langle \underline{C_1}, m_1 \rangle$$

$$\xrightarrow{D}$$