Review:

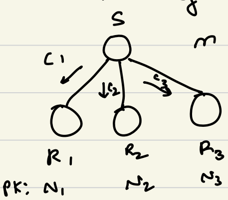
- → EL Gamal PKC is CPA secure but <u>not</u> CCA secure
- → RSA: textbook version is "insecure" (deterministic), PCS v1.5 is <u>not</u> CPA secure

A couple of "attacks" on RSA:

→ e is low (say 3)

$c = m^e \bmod N = m^3 \bmod N$

if $m < \sqrt[3]{N}$ then it is insecure, do cube root of c to get m.



$c_i = m^3 \bmod N_i$

using Chinese Remainder Theorem

Chinese Remainder Theorem

$x \equiv a_1 \pmod{p_1}$

$x \equiv a_2 \pmod{p_2}$

$\vdots$

$x \equiv a_k \pmod{p_k}$

p_i's are mutually pairwise coprime

Find x.

Ex: solve for $x \ni x \% 2 = 0, x \% 3 = 1, x \% 5 = 2$. 22, 52, 82... $30n + 22$

In general, $x = \left(\prod_{i=1}^{k} p_i\right) n + (?)$

For, $n = 0$ since m^3 must be $< N_i$ & thus is $< N_1 N_2 N_3$. Broadcasting using textbook RSA is a bad choice.

CRT: $x = \left(\prod_{i=1}^{k} p_i\right) \cdot n + \sum_{i=1}^{k} a_i \left\{ \left[a_i^{-1} \left(\bmod \frac{\prod_{i=1}^{k} p_i}{p_i} \right) \cdot \frac{\prod_{i=1}^{k} p_i}{p_i} \right] \right\}$

Derivation:

Easiest version: all a_i's are 0,

$x \equiv 0 \bmod p_1$

$\vdots$

$x \equiv 0 \bmod p_k$

$x = \left(\prod_{i=1}^{k} p_i\right) \cdot n + 0$

Next: $x \equiv 1 \pmod{p_1}$, $x \equiv 0 \pmod{p_2}$ ... $x \equiv 0 \pmod{p_k}$

$x \equiv \left(\prod_{i=1}^{k} p_i\right)\left(\left(\prod_{i=2}^{k} p_i\right)^{-1} \bmod p_i\right) + m \prod_{i=1}^{k} p_i$

Next: $x \equiv 0 \pmod{p_1}$, $x \equiv 1 \pmod{p_2}$ ... $x \equiv 0 \pmod{p_k}$

$x \equiv \left(\frac{\prod_{i=1}^{k} p_i}{p_2}\right)\left(\left(\frac{\prod_{i=1}^{k} p_i}{p_2}\right)^{-1} (\bmod p_2)\right) + m \prod_{i=1}^{k} p_i$

Next: $x \equiv a_1 \pmod{p_1}$, $x \equiv 0 \pmod{p_2}$ ... $x \equiv 0 \pmod{p_k}$

$$x \equiv a_1\left[\left(\frac{\prod_{i=1}^{k} p_i}{p_1}\right)\left(\left(\frac{\prod_{i=1}^{k} p_i}{p_1}\right)^{-1} \bmod p_1\right)\right] + m \prod_{i=1}^{k} p_i$$

In general,

$$x \equiv \sum_{i=1}^{k} a_i\left[\left(\frac{\prod_{j=1}^{k} p_j}{p_i}\right)\left(\left(\frac{\prod_{j=1}^{k} p_j}{p_i}\right)^{-1} \bmod p_i\right)\right] + m \cdot \left(\prod_{i=1}^{k} p_i\right)$$

Smallest Solution:

$$x = \sum_{i=1}^{k} a_i\left[\left[\left(\frac{\prod_{j=1}^{k} p_j}{p_i}\right)^{-1} \bmod p_i\right]\left(\frac{\prod_{j=1}^{k} p_j}{p_i}\right)\right] \bmod \left(\prod_{i=1}^{k} p_i\right)$$

$\exists$ isomorphism b/w $\mathbb{Z}_{\prod_{i=1}^{i} p_i}$ and

$\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \dots \mathbb{Z}_{p_k}$

Efficient algorithm to multiply 2 numbers exists