ECE 471/571 RSA (cont'd)

RSA signature

- sign with private key: $(d)$ $S = m^d \bmod n$
- Verify with public key: $(e,n)$ $m \overset{?}{=} S^e \bmod n$

Efficiency

Fast exponentiation alg.

simple.alg

$x^{16} \bmod n = x \cdot x \cdot x \cdot x \cdots x.$ 15 mul.

$x^d$, $d$ of 1000 bits. $d \approx 2^{1000}$

$16 = 2^4$ $\left(\left(\left(x^2 \bmod n\right)^2 \bmod n\right)^2 \bmod n\right)^2 \bmod n = x^{16} \bmod n$

4 mul. $\log_2 16$

$16_2 = 10000$

$x \; x^2 \; x^4 \; x^8 \; x^{16}$

$x^{11} = x^{1+2+8} = x \cdot x^2 \cdot x^8.$

$11_2 = 1011$

$x \cdot x^2 \cdot x^4 \cdot x$

$x^5 \to x^{10} \cdot x = x^{11}$

$$d = \sum_{d_i \neq 0} 2^i$$

if $d_i = 1$. $i \geq 1$.

$x_{i-1}^2 \cdot x$ $x_0 = x.$

| if $d_i = 0$ $\underline{x_{i-1}}$

square-and-multiply alg. $O(\log_2 d)$ multiplications

$\underbrace{1000\ldots0}_{n \text{ bits}}$

$1111111111$

$x\ x^2 \cdot x \ldots$

$\underbrace{\qquad\qquad}_{n-1 \text{ bits} \times 2}$ $= 2(n-1)$.

---

CRT. $X$ soldiers.

$m_1 = 3$ $r_1 = 2$

$m_2 = 5$ $r_2 = 3$

$m_3 = 7$ $r_3 = 2$

$3 \times 5 \times 7 = 105$

$\begin{cases} X \equiv 2 \bmod 3 \\ X \equiv 3 \bmod 5 \end{cases} \Rightarrow$ unique. $X \bmod (m_1 m_2 m_3)$

$x \equiv 2 \bmod 7$

$$\begin{cases} x \equiv 0 \bmod 2 \\ x \equiv 3 \bmod 5 \end{cases}$$

| $x$ | mod 2 | mod 5 |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 0 | 2 |
| 3 | 1 | 3 |
| 4 | 0 | 4 |
| 5 | 1 | 0 |
| 6 | 0 | 1 |
| 7 | 1 | 2 |
| 8 | 0 | 3 |
| 9 | 1 | 4 |

$x = 8 \bmod 10$

$$X \equiv a_i \bmod m_i \quad 1 \le i \le r.$$

$$X = \sum_{i=1}^{r} a_i \cdot M_i\, y_i \bmod \left(\prod_{i=1}^{r} m_i\right)$$

$$M = \prod_{i=1}^{r} m_i$$

$m_i$ are primes

$$M_i = \frac{M}{m_i}$$

$$y_i = \underline{M_i^{-1}} \bmod \underline{m_i} \quad 1 \le i \le r$$

---

Ex. $x \equiv 2 \bmod 3$ $\quad x = ? \bmod 15$

$x \equiv 3 \bmod 5.$

$m_1 = 3 \quad m_2 = 5. \quad M = 15.$

$a_1 = 2, \quad a_2 = 3. \quad M_1 = 5 \quad M_2 = 3$

$y_1 = 5^{-1} \bmod 3$

$y_2 = 3^{-1} \bmod 5$

$$X = 2 \cdot 5 \cdot 2 + 3 \cdot 3 \cdot 2$$

$= 20 + 18 \bmod 15$

$= 38 \bmod 15 = 8$