VU Network Security Advanced Topics
Lecture 2

CRT RSA

Tanja Zseby
TU Wien

WS 2018/19

Summary from Last Lecture

- Recap
  - Asymmetric crypto
  - RSA
- Extended Euclidean Algorithm
  - Calculating a Multiplicative Inverse

CRT RSA

CRT-RSA

- Using the Chinese Remainder Theorem in
  - RSA signature calculation
  - RSA decryption
- Advantage
  - Calculation with p and q instead of n
  - Smaller modulus
  - Smaller exponents

CRT-RSA Claim

RSA Signature:

$$sig = m^d \; mod \; n$$

With Chinese Remainder Theorem we can calculate signature with smaller exponents and modulus using:

$$m_1 = m^{d_p} \quad mod \; p \qquad \text{with} \qquad d_p = d \quad mod(p-1)$$

$$m_2 = m^{d_q} \quad mod \; q \qquad \text{with} \qquad d_q = d \quad mod(q-1)$$

Chinese Remainder Theorem (CRT)

- Goal: Find x that solves a system of linear congruencies
- $n_1, n_2, n_3, \dots n_k$ are pairwise coprime

$$
\begin{aligned}
x &\equiv a_1 \quad mod\, n_1 \\
x &\equiv a_2 \quad mod\, n_2 \\
&\quad \dots \\
x &\equiv a_k \quad mod\, n_k
\end{aligned}
$$

- **Chinese Remainder Theorem:** The system of linear congruencies has a ***unique solution mod N*** with

$$N = n_1 \cdot n_2 \cdot n_3 \cdot \dots n_k$$

Chinese Remainder Theorem (CRT): Example

$$x \equiv 2 \quad mod\, 3$$
$$x \equiv 3 \quad mod\, 4$$
$$x \equiv 1 \quad mod\, 5$$

Check if pairwise coprime: gcd(2,3)=1, gcd(2,1)=1, gcd(3,1)=1 ➔ ok

Solutions: x=11, x=71, x= 131, …

$$N = 3 \cdot 4 \cdot 5 = 60$$

All solutions fulfill:

$$x \equiv 11 \quad mod\, 60$$

➔ x=11 is unique solution mod 60

CRT: Finding a Solution

One solution: $$x = \sum_{i=1}^{k} a_i \cdot e_i$$

with: $$e_i = \frac{N}{n_i} \cdot \left[\left(\frac{N}{n_i}\right)^{-1}\right]_{n_i}$$

Multiplicative inverse of N/n_i when using mod n_i

$$e_i \equiv \begin{cases} 1 & mod\, n_i \\ 0 & mod\, n_j \quad j \neq i \end{cases}$$

Example

$$x \equiv a_1 \quad mod\, n_1$$
$$x \equiv a_2 \quad mod\, n_2$$

$$N = n_1 \cdot n_2$$

One solution: $x = a_1 \cdot e_1 + a_2 \cdot e_2$

with:

$$e_1 = \frac{N}{n_1} \cdot \left[\left(\frac{N}{n_1} \right)^{-1} \right]_{n_1} = n_2 \cdot [{n_2}^{-1}]_{n_1}$$

$$e_2 = \frac{N}{n_2} \cdot \left[\left(\frac{N}{n_2} \right)^{-1} \right]_{n_2} = n_1 \cdot [{n_1}^{-1}]_{n_2}$$

$$x = a_1 \cdot\ n_2 \cdot [{n_2}^{-1}]_{n_1} + a_2 \cdot\ n_1 \cdot [{n_1}^{-1}]_{n_2}$$

Why x is a Solution

$$x = a_1 \cdot \; n_2 \cdot [n_2{}^{-1}]_{n_1} + a_2 \cdot \; n_1 \cdot [n_1{}^{-1}]_{n_2}$$

x mod n_1:

$$x = a_1 \cdot \underbrace{\boxed{n_2 \cdot [n_2{}^{-1}]_{n_1}}}_{\textbf{1} \text{ if taken mod } n_1} + a_2 \cdot \underbrace{\boxed{n_1 \cdot [n_1{}^{-1}]_{n_2}}}_{\textbf{0} \text{ if taken mod } n_1}$$

$$x \equiv \; a_1 \quad mod\, n_1$$

x mod n_2:

$$x = a_1 \cdot \underbrace{\boxed{n_2 \cdot [n_2{}^{-1}]_{n_1}}}_{\textbf{0} \text{ if taken mod } n_2} + a_2 \cdot \underbrace{\boxed{n_1 \cdot [n_1{}^{-1}]_{n_2}}}_{\textbf{1} \text{ if taken mod } n_2}$$

$$x \equiv \; a_2 \quad mod\, n_2$$

Calculate Signature with CRT RSA

RSA Signature (without CRT)

- Chose large primes p,q
- Compute n $n = p \cdot q$
- Compute $\varphi(n)$
- Choose e
- Find inverse d
- Publish n,e
- Calculate signature (traditional way):

$$sig = m^d \, mod \, n$$

Express RSA Signature with CRT

CRT:

$$x \equiv a_1 \quad mod\, n_1$$
$$x \equiv a_2 \quad mod\, n_2$$

$$N = n_1 \cdot n_2$$

Solution for x ➔ can find solution mod N:

Express m^d with congruencies:

$$m^d \equiv m_1 \qquad mod\, p$$
$$m^d \equiv m_2 \qquad mod\, q$$

$$n = p \cdot q$$

If we find solution for m^d ➔ can find solution mod n:

$$m^d \equiv sig \qquad mod\, pq$$

Calculate Signature with CRT

$$m^d \equiv m_1 \qquad mod\ p$$

express d as multiple of φ(p): $d = k \cdot \varphi(p) + d\ mod\ \varphi(p)$

$$m^d \quad mod\ p = m^{k \cdot \varphi(p) + d\ mod\ \varphi(p)}\ mod\ p$$
$$= m^{k \cdot \varphi(p)} \cdot m^{d\ mod\ \varphi(p)}\ mod\ p$$

Using Euler's Theorem $m^{\varphi(n)} \equiv 1 \qquad mod\ n$ if m,n coprime

$$\left(m^{\varphi(n)}\right)^k \equiv 1 \qquad mod\ n$$

$$m^d \quad mod\ p = m^{d\ mod\ \varphi(p)} mod\ p$$ with φ(p)=p-1
$$= m^{d\ mod\ (p-1)}\ mod\ p$$

$m_1 = m^{d_p} \quad mod\ p$ with $d_p = d \quad mod(p-1)$

CRT-RSA

To calculate RSA signature

$$sig = m^d \ mod \ n \qquad\qquad n = p \cdot q$$

Formulate congruencies:

$$m^d \equiv m_1 \qquad mod \ p$$

$$m^d \equiv m_2 \qquad mod \ q$$

with

$$m_1 = m^{d_p} \ \ mod \ p \qquad \text{with} \quad d_p = d \ \ mod(p-1)$$

$$m_2 = m^{d_q} \ \ mod \ q \qquad \text{with} \quad d_q = d \ \ mod(q-1)$$

Find solution for m^d using Chinese Remainder Theorem:

$$m^d = m_1 \cdot \ q \cdot [q^{-1}]_p + m_2 \cdot \ p \cdot [p^{-1}]_q$$

Signature is unique solution mod n: $m^d \equiv sig \quad mod \ n$

RSA Example

RSA Example

➔ see separate Document

Thank you!