Presented by Bowen Dai, Chengcheng Li, Ziyi Zhao

Limitation of RSA

WIENER'S ATTACK

RSA BRIEF REVIEW

- Public key: (m, k)
- Private key: (d, p, q)

p & q are distinct prime numbers, $m = p * q$ and $kd \equiv 1 \mod \varphi(m)$

Factorization is hard.

However, if we know private exponent d, we do not need to find the factor of m.

WIENER'S THEOREM

Let $m = p \ * q$ with q < p < 2q.

Let $d < \frac{1}{3} m^{\frac{1}{4}}$.

Given (m, k) with k * d ≡ 1 mod φ(m), an attacker can efficiently find d.

PROOF

- Based on approximations using continued fractions
- Only needs a linear-time algorithm for recovering the secret key d

$$\left|\frac{k}{\varphi(\mathrm{m})} - \frac{c}{d}\right| = \frac{1}{d * \varphi(\mathrm{m})}$$ where k * d - c * φ(m) = 1

By approximating m and replace φ(m), $\left|\frac{k}{\mathrm{m}} - \frac{c}{d}\right| \leq \frac{3c}{d\sqrt{m}}$

$$\left|\frac{k}{\mathrm{m}} - \frac{c}{d}\right| \leq \frac{1}{d \ * m^{\frac{1}{4}}} < \frac{1}{2d^2}$$

- $\frac{c}{d}$: convergent of the continued fraction expansion of $\frac{k}{\mathrm{m}}$

SOME IMPORTANT OBSERVATIONS

When m is large:

φ(m) = (p-1)(q-1) = pq – (p+q) + 1 ≈ m

From kd = 1 (mod φ(m)):

There exists an integer k such that

kd - c φ(m) = 1

$\frac{k}{\varphi(m)} - \frac{c}{d} = \frac{1}{d\varphi(m)}$ Since N is very large, φ(m) is also very large

$\frac{k}{m} \approx \frac{c}{d}$

FINDING $\frac{k}{m}$

Use continued fractions to find a set of convergent $\frac{c}{d}$ that approximate $\frac{k}{m}$

Convergent: approximation of a number using continued fraction

To find the convergent, we should first write the fraction as a continued fraction

SOME REMARKS ABOUT THE CONVERGENT

Since kd $\equiv$ 1 mod φ(m) and φ(m) is the product of two even numbers, φ(m) is even and both k and d are odd

➔If we find a convergent with even d, this convergent is not the one we look for

Since φ(m) is an integer, and kd - c φ(m) = 1

We rearrange the equation and get $\varphi(\mathrm{m}) = \frac{kd-1}{c}$ which should also be an integer

MORE REMARKS ABOUT THE CONVERGENT

φ(m)= (p-1)(q-1)

= pq –(p+q) +1

= m – (p+q) + 1

Rearrange:

p+q = m - φ(m) + 1

Consider the quadratic:

$$(x-p)(x-q) = 0$$

$$x^2 - (p+q)x + pq = 0$$

$$x^2 - (m - \varphi(m)+1)x + m = 0$$

If the value of φ(m) is correct, the root of this equation is integers

CONTINUED FRACTIONS

Usually denoted as $< q_0, q_1, q_2, q_3, \dots, q_n >$

Finite for any rational number, cyclic for any quadratic irrational number

quadratic irrational numbers: solutions of quadratic equation with irreducible square root i.e. : $\frac{a+b\sqrt{c}}{d}$
where a, b, c, d are integers, d$\neq 0$ and c is square free

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\dots}}}}$$

WRITE ANY FRACTION AS A CONTINUED FRACTION

Using Euclidean Algorithm with the numerator as the bigger number and the denominator as the smaller number regardless the real value of the numerator and denominator

Write the quotient in each equation as the q in the continued fraction

EXAMPLE AND PROOF

Reduce $-\frac{551}{802}$ to continued fraction

-551 = -1 * 802 + 251

802 = 3 * 251 + 49

251 = 5 * 49 + 6

49 = 8 * 6 + 1

6 = 6 * 1 + 0

$$-\frac{551}{802} = -1 + \frac{251}{802}$$

$$= -1 + \frac{1}{\frac{802}{251}}$$

$$= -1 + \frac{1}{3+\frac{1}{\frac{251}{49}}}$$

$$\vdots$$

$$= -1 + \frac{1}{3 + \frac{1}{5+\frac{1}{8+\frac{1}{6}}}}$$

FIND THE CONVERGENT OF A FRACTION USING CONTINUED FRACTION

$$n_0 = q_0$$
$$n_1 = q_0 q_1 + 1$$
$$n_i = q_i n_{i-1} + n_{i-2}$$

$$d_0 = 1$$
$$d_1 = q_1$$
$$d_i = q_i d_{i-1} + d_{i-2}$$

EXAMPLE

In an RSA encryption system, m = 64741 and the public exponent e = 42667. Find the decryption exponent d

First find some quotients we will use to calculate the convergent

42667 = 0 * 64741 + 42667

64741 = 1 * 42667 + 22074

42667 = 1 * 22074 + 20593

22074 = 1 * 20593 + 1481

:

Now we get the first few values of q_i: <0, 1, 1, 1, …>

Then calculate the convergent

First convergent: $\frac{n_0}{d_0} = \frac{0}{1}$ -> d = 1 obviously not the d we need

Second convergent: $\frac{n_1}{d_1} = \frac{q_0 q_1 + 1}{q_1} = \frac{1}{1}$ -> d = 1

Third convergent: $\frac{n_2}{d_2} = \frac{q_2 n_1 + n_0}{q_2 d_1 + d_0} = \frac{1}{2}$ -> d = 2, impossible because d must be odd

Forth convergent: $\frac{n_3}{d_3} = \frac{q_3 n_2 + n_1}{q_3 d_2 + d_1} = \frac{2}{3}$ -> d = 3 possible d

Now we check other properties of d

φ(m) = $\frac{kd-1}{c}$ = = $\frac{42667*3-1}{2}$ = 64000 <- an even integer

d = 3 passes the second check. Pass on the next check

If the value is correct, both roots of the following quadratic should be integers:

$x^2 - (m\ -\ \varphi(m) + 1)x + m$ = $x^2 - 742x + 64741$

Use quadratic formula to find the roots:

$$x = \frac{-b\pm\sqrt{b^2-4ac}}{2a} = \frac{742\pm\sqrt{(-742)^2-4*1*64741}}{2*1}$$

We get x = 641 or x = 101

PRACTICES TO PREVENT WIENER'S ATTACK

LARGE K

- Recall:

Public key: (m, k)

m = p * q

A random number relative prime to φ (m)

- k’ = k + t * φ(m)   (t is some large number)
- k’ > $m^{1.5}$, the proof based on approximation does not work
- Pitfall: increase encryption time

CHINESE REMAINDER THEOREM

- Powerful tool for enhancing RSA decryption efficiency by breaking down the computation into smaller, more manageable tasks.
- When decrypting a ciphertext, instead of performing modular exponentiation modulo k, CRT allows us to perform modular exponentiation modulo the prime factors of k separately.
- Apply to speed up the decryption process in RSA
- Reduce the computational complexity of decryption.

CHINESE REMAINDER THEOREM

Let m and n be relatively prime positive integers. For all integers a and b, the pair of congruences

$x \equiv a \pmod{p}$ $x \equiv b \pmod{q}$

has a solution, and this solution is uniquely determined modulo (pq).

$X \equiv m\ (pq)$

What is important here is that q and q are relatively prime. There are no constraints at all on a and b.

GENERAL FORMULA TO APPLY:

$$\begin{cases} x \equiv p \pmod{m} \\ x \equiv q \pmod{n} \end{cases} \qquad \gcd(m,n)=1$$

Lemma: (Euclidean Algorithm)

Since $\gcd(m,n)=1$, there exists a & $b \in \mathbb{Z}$ such that

$$am+bn=1$$

We decompose x into a sum of 2 integers.

Let $x=k+l$ such that

$$\begin{cases} k \equiv p \pmod{m} \\ k \equiv 0 \pmod{n} \end{cases} \qquad \begin{cases} l \equiv 0 \pmod{m} \\ l \equiv q \pmod{n} \end{cases}$$

We have $am+bn=1$

Multiply each side by p:

$$amp+bnp=p$$

$$bnp=p-amp$$

$$\Downarrow$$

$$k$$

Since $n \mid k$ and $k \equiv p \pmod{m}$

Multiply each side by q:

$$amq+bnq=q$$

$$amq=q-bnq$$

$$\Downarrow \qquad \Updownarrow$$

$$l \qquad bnq-q$$

Since $m \mid l$ and $l \equiv q \pmod{n}$

So $x=k+l$

$=bnq+amq$

General form:

$$=bnq+amq+\underbrace{mnk}_{\text{multiple of the modulo}}, \quad k \in \mathbb{Z}$$

$$\begin{cases} x \equiv \boxed{p} \pmod{\boxed{m}} \\ x \equiv \boxed{q} \pmod{\boxed{n}} \end{cases}$$

EXAMPLE OF USAGE

Find x given that:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

$\gcd(3,2,7)=1$

1. We first find x that satisfy:

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

$$\begin{cases} x \equiv \boxed{p} \pmod{\boxed{m}} \\ x \equiv \boxed{q} \pmod{\boxed{n}} \end{cases}$$

$= bnq + amq + mnk, \quad k \in \mathbb{Z}$

Using euclidean Algorithm:

$3a+5b=1$

$3\times2+5\times(-1)=1$

$\Downarrow$

$x=3\times2\times3+5\times(-1)\times2=8$ using the general formula.

$x=8+15k, \ k\in\mathbb{Z}$

$$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 2 \pmod{7} \end{cases}$$

$\gcd(15,7)=1$

Using euclidean Algorithm:

$1=1\times15+(-2)\times7$

$\Downarrow$

By formula: $x=1\times15\times2+(-2)\times7\times8$

$x=-82$

$x=-82+105k, \ k\in\mathbb{Z}$

Let $k=1$, $x=23$

$23=3\times7+2$

$23=5\times4+3$

$23=7\times3+2$

V

HOW DOES IT ACCELERATE THE DECRYPTION IN RSA

To decrypt a message, we need to solve

$$M \equiv c^d \pmod{n}$$
$$M \equiv c^d \pmod{pq}$$

Using CRT:

Let $\begin{cases} x \equiv m_1 \pmod{p} \\ x \equiv m_2 \pmod{q} \end{cases}$, $\begin{cases} m_1 \equiv c^d \pmod{p} \\ m_2 \equiv c^d \pmod{q} \end{cases}$

Suppose $M \equiv 11^{17} \pmod{21}$
$\equiv 11^{17} \pmod{3 \times 7}$

Let $\begin{cases} x \equiv m_1 \pmod{3} \\ x \equiv m_2 \pmod{7} \end{cases} \Rightarrow \begin{cases} m_1 \equiv 11^{17} \pmod{3} \\ m_2 \equiv 11^{17} \pmod{7} \end{cases}$

Let $\begin{cases} x \equiv m_1 \pmod{3} \\ x \equiv m_2 \pmod{7} \end{cases} \Rightarrow \begin{cases} m_1 \equiv 11^{17} \pmod{3} \\ m_2 \equiv 11^{17} \pmod{7} \end{cases}$

$$\begin{aligned} m_1 &\equiv 11^{17} \pmod{3} \\ &\equiv (11^2)^8 \cdot 11 \pmod{3} \\ &\equiv 1^8 \cdot 11 \pmod{3} \\ &\equiv 2 \pmod{3} \end{aligned}$$

$$\begin{aligned} m_2 &\equiv 11^{17} \pmod{7} \\ &\equiv (11^6)^2 \cdot 11^5 \pmod{7} \\ &\equiv 4^5 \pmod{7} \\ &\equiv 2 \pmod{7} \end{aligned}$$

$\Leftarrow$ Apply Fermat little theorem
$a^{p-1} \equiv 1 \pmod{p}$

$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{7} \end{cases}$

$1 = 7 \times 1 - 3 \times 2$

$x = 7 \times 1 \times 2 - 3 \times 2 \times 2$

$x = 2 + 21k, \ k \in \mathbb{Z}$

$\Uparrow$

M

THANK YOU FOR LISTENING!