T2 Asymmetric Analysis
Question Time

Maria Eichlseder **Florian Mendel**

Applied Cryptography 2 – ST 2016

A Wiener's Attack on RSA

Wiener's Attack on RSA **4 Points**

Implement Wiener's attack on RSA to recover small d ($\rightarrow$ L6):

- a Compute n-th convergents of continued fractions for $\mathbb{Q}$
- b Recover private key from given 1024-bit RSA public key

A Questions

Example:

$N = 9449868410449$, $e = 6792605526025$, $d < \frac{1}{3}\sqrt[4]{N} \approx 584.$

1. Perform Wiener's attack by computing the convergents of $\frac{e}{N}$:

$$\frac{p_i}{q_i} = \quad \frac{1}{1}, \quad \frac{2}{3}, \quad \frac{3}{4}, \quad \frac{5}{7}, \quad \frac{18}{25} \quad \frac{23}{32}, \quad \frac{409}{569}, \quad \dots$$

2. Test: $d = 569$ if $M^{e\cdot 569} = M$ ✓

3. Pick $x = 2$:

$$x^{(ed-1)/2^1} = x^{(ed-1)/2^2} = \ldots = x^{(ed-1)/2^5} = 1$$

$$x^{(ed-1)/2^6} = x^{60390508504816} \equiv 8233548335126 = y \neq \pm 1$$

4. $p = \gcd(N, y-1) = 1234577 \;\Rightarrow\; N = 1234577 \cdot 7654337$

B Discrete Logarithms with Pollard-ρ

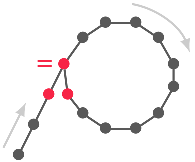
Discrete Logarithms with Pollard-ρ	8 Points

Implement Pollard-ρ algorithm to find discrete logarithms ($\rightarrow$ L5)

- a Implement Pollard-ρ and apply to 32-bit challenge
- b Solve resulting equation to complete the solution
- c Solve 64-bit challenge

B Questions

To solve $y = g^x \pmod{p}$, find $r_j = y^{a_j} g^{b_j} = y^{a_k} g^{b_k} = r_k \pmod{p}$.
Then $x \cdot (a_j - a_k) \equiv (b_k - b_j) \pmod{p-1}$.



$$(r_0, a_0, b_0) = (1, 0, 0)$$

$$(r_{i+1}, a_{i+1}, b_{i+1}) = \begin{cases} ([y \cdot r_i]_p, [a_i + 1]_{p-1}, [b_i]_{p-1}) & 0 < r_i < \frac{p}{3} \\ ([r_i^2]_p, [2a_i]_{p-1}, [2b_i]_{p-1}) & \frac{p}{3} < r_i < \frac{2p}{3} \\ ([g \cdot r_i]_p, [a_i]_{p-1}, [b_i + 1]_{p-1}) & \frac{2p}{3} < r_i < p \end{cases}$$

C Factoring with Continued Fractions

Factoring with Continued Fractions — 12 Points

Implement CFRAC factorization ($\rightarrow$ L6):

- a Implement factoring with factor bases and random squares
- b Compute n-th convergents of continued fractions for $\mathbb{R}$
- c Piece this together to get CFRAC and factor 32-bit N
- d Factor 64-bit N

C Questions

Example: Factor $n = 9073$ with CFRAC with $\mathcal{B} = \{-1, 2, 3, 5, 7\}$

1. Compute convergents for $\sqrt{9073} = 95.2523\ldots$:

$$\frac{p_0}{q_0} = \frac{95}{1}, \quad \frac{p_1}{q_1} = \frac{286}{3}, \quad \frac{p_2}{q_2} = \frac{381}{4}, \quad \frac{p_3}{q_3} = \frac{10192}{107}, \quad \frac{p_4}{q_4} = \frac{20765}{218}$$

2. Smallest absolute residue b_i of p_i^2 mod 9073:

$$b_0 = -48,\ b_1 = 139,\ b_2 = -7,\ b_3 = 87,\ b_4 = -27$$

3. Check smoothness of the b_i and factorize:

$$b_0 = (1, 4, 1, 0, 0), \quad b_2 = (1, 0, 0, 0, 1), \quad b_4 = (1, 0, 3, 0, 0).$$

4. Combine to get $(-36)^2 \equiv 3834^2 \pmod{9073}$:

$$x = b_0 \cdot b_4 = -1 \cdot 2^2 \cdot 3^2 = -36$$

$$y = p_0 \cdot p_4 = 95 \cdot 20765 \equiv 3834 \pmod{9073}$$

5. Factor n: $\gcd(3834 + 36, 9073) = 43 \Rightarrow 9073 = 43 \cdot 211$