SC4001 Applied Cryptography Project

Weiner's Attack and Shor's Algorithm

Adrian Alviento, Jim Sean

School of Computer Science and Engineering, SCSE
Nanyang Technological University

November 24, 2023

Table of Contents

Weiner's Attack

Theorem 1 [1] [3]

- Let $N = pq$ with $q < p < 2q$. Let $d < \frac{1}{3}N^{1/4}$. Given $\langle N, e\rangle$ with $ed \equiv 1 \mod \phi(N)$, then d is the denominator of a convergent of the continued fraction expansion of $\frac{e}{n}$

NANYANG TECHNOLOGICAL UNIVERSITY

A More Precise Bound

Theorem 2 [2]
If the following conditions are satisfied:

- (i) $q < p < 2q$
- (ii) $0 < e < \phi(N)$
- (iii) $ed - k\phi(N) = 1$
- (iv) $d \leq \frac{1}{18^{\frac{1}{4}}} N^{\frac{1}{4}}$

- $\Rightarrow \frac{k}{d}$ is equals to a convergent of the continued fraction of $\frac{e}{N}$

A More Precise Bound

Proof

Recall:

$kN - k\phi(N) = kN - k(p-1)(q-1) = kN - k(N-p-q+1) = k(p+q-1)$ – (1)

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{k}{d} - \frac{e}{N}\right| < \left|\frac{kN - ed}{Nd}\right|$$

$$= \left|\frac{kN - k\phi(N) - ed + k\phi(N)}{Nd}\right|$$

$$= \left|\frac{k(p+q-1) - 1}{Nd}\right| \quad \text{(By 1)}$$

$$< \frac{k(p+q)}{Nd}$$

$$\Rightarrow \left|\frac{e}{N} - \frac{k}{d}\right| < \frac{k(p+q)}{Nd}$$

A More Precise Bound

Proof Cont'd

Since $ed - k\phi(N) = 1$ and $e < \phi(N)$

$$
\begin{aligned}
1 = ed - k\phi(N) &< (d-k)\phi(N) \\
0 &< (d-k)\phi(N) \\
k &< d
\end{aligned}
$$

$$\Rightarrow \left| \frac{e}{N} - \frac{k}{d} \right| < \frac{k(p+q)}{Nd} < \frac{p+q}{N} \quad - (2)$$

A More Precise Bound

Proof Cont'd

It follows from $q < p < 2q$ that $1 < \sqrt{\frac{p}{q}} < \sqrt{2}$ and since $f(x) = x + \frac{1}{x}$ is increasing on $[1, +\infty)$,

$$\begin{aligned}
\frac{p+q}{\sqrt{N}} = \frac{p}{\sqrt{pq}} + \frac{q}{\sqrt{pq}} &= \sqrt{\frac{p}{q}} + \sqrt{\frac{q}{p}} \\
&= \sqrt{\frac{p}{q}} + \frac{1}{\sqrt{\frac{p}{q}}} = f(\sqrt{\frac{p}{q}}) \\
&< f(\sqrt{2}) \\
&= \sqrt{2} + \frac{1}{\sqrt{2}} \\
&= \frac{3}{\sqrt{2}} \\
\Rightarrow p + q &< \frac{3}{\sqrt{2}}\sqrt{N} \ \textcolor{red}{-\ (3)}
\end{aligned}$$

A More Precise Bound

Proof Cont'd

Combining (2) and (3), we have $\left|\frac{e}{N}-\frac{k}{d}\right|<\frac{p+q}{N}<\frac{\frac{3}{\sqrt{2}}N^{\frac{1}{2}}}{N}=\frac{3}{\sqrt{2}N^{\frac{1}{2}}}$

Since $d<\frac{1}{18^{\frac{1}{4}}}N^{\frac{1}{4}}$, $\frac{1}{2d^2}>\frac{1}{2(\frac{1}{18^{\frac{1}{4}}}N^{\frac{1}{2}})^2}=\frac{3}{\sqrt{2}N^{\frac{1}{2}}}$, we have

- $\left|\frac{e}{N}-\frac{k}{d}\right|<\frac{1}{2d^2}$
- By Legendre's theorem, $\frac{k}{d}$ is a rational number amongst the continued fraction's convergent of $\frac{e}{N}$

Time Complexity

Wiener's Attack Pseudocode

- Get convergents of continued fraction $\frac{e}{N}$ – O(logN)
- For each convergents d', if $(M^e)^{d'} \equiv M(modN)$, then $d' = d$ and we terminate – O(c), for some constant c
- $\Rightarrow$ Wiener's Attack is $O(logN)$

NANYANG TECHNOLOGICAL UNIVERSITY

Time Complexity

Proof

Getting the convergents is based on the euclidean's algorithm

- $e = kN + r$
- append k to an array
- $e \leftarrow N$ and $N \leftarrow r$
- Repeat until $N == 0$

- This is simply Euclidean's Algorithm
- $\Rightarrow$ The time complexity is therefore proportional to the number of steps required to reduce N to 0 $O(logN)$

NANYANG TECHNOLOGICAL UNIVERSITY

Proof Cont'd

- Assume the Euclidean Algorithm for $gcd(a, b)$ reduces in X steps $\Rightarrow a \geq f_{X+2},\ b \geq f_{X+1}$ and $a \geq b$
- Base Case: For $a == 2 == f_3$ and $b == 1 == f_2$, then $gcd(a, b)$ reduces in $X = 1$ step with required conditions
- Inductive Step: Assume statement holds true up to $(X-1)^{th}$ step $\Rightarrow gcd(b, a\%b)$ reduces in $(X-1)$ steps and $b \geq f_{X+1},\ a\%b \geq f_X$
- We know $a == \lfloor \frac{a}{b} \rfloor b + a\%b$, and since $\frac{a}{b} \geq 1$, $a \geq b + (a\%b)$ $\Rightarrow a \geq f_{X+1} + f_X == f_{X+2}$
- Thus, $gcd(a, b)$ reduces in X steps, with $a \geq f_{X+2}$ and $b \geq f_{X+1}$ as required

NANYANG TECHNOLOGICAL UNIVERSITY

Time Complexity

Proof Cont'd

- Now, we know that the number of steps to reduce $gcd(a, b)$ is X steps
- We know that $f_X == \frac{(\frac{1+\sqrt{5}}{2})^X - (\frac{1-\sqrt{5}}{2})^X}{\sqrt{5}} \approx \Phi^X$, where $\Phi \approx 1.618$ is the golden ratio
- $f_X \approx \Phi^X \Rightarrow X \approx log_{\Phi}(f_X)$
- Since $a \geq b$, $f_X \approx f_{X+1} \approx b$
- $\Rightarrow X \approx log_{\Phi} b$
- Thus, $O(X) = log(b)$
- So, gcd(N, e) reduces in $O(log(e)) = O(log(N))$ since $e \approx \frac{k\phi(N)}{d} \approx \frac{k}{\frac{1}{3}N^{1/4}}\phi(N) \approx N^{\frac{3}{4}}$

NANYANG TECHNOLOGICAL UNIVERSITY

Contribution

- Wiener's Attack - Adrian Alviento
- Shor's Algorithm - Jim Sean

References I

[1] D. Boneh and G. Durfee. "Cryptanalysis of RSA with Private Key d Less than N0.292". In: *Advances in Cryptology — EUROCRYPT '99*. Ed. by J. Stern. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1999, pp. 1–11. DOI: 10.1007/3-540-48910-X_1.

[2] W. Susilo, J. Tonien, and G. Yang. "The Wiener Attack on RSA Revisited: A Quest for the Exact Bound". In: *Information Security and Privacy*. Ed. by J. Jang-Jaccard and F. Guo. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019, pp. 381–398. DOI: 10.1007/978-3-030-21548-4_21.

References II

[3] M. J. Wiener. "Cryptanalysis of Short RSA Secret Exponents". In: *Advances in Cryptology — EUROCRYPT '89*. Ed. by J.-J. Quisquater and J. Vandewalle. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1990, pp. 372–372. DOI: 10.1007/3-540-46885-4_36.