

Attacken auf RSA und Das Rabin Kryptosystem

David Böhme

Institut für Informatik
Universität Potsdam

4. Januar 2005

Überblick

Wiederholung: RSA

Das RSA Kryptosystem

Attacken auf RSA

RSA-FACTOR

Wieners Algorithmus

Das Rabin Kryptosystem

Definition und Eigenschaften

Sicherheit von Rabin

Semantische Sicherheit von RSA

RSA - Kryptosystem

- ▶ Seien p, q Primzahlen und $n = pq$. Definiere

$$K = (n, p, q, a, b)$$

mit

$$a = b^{-1} \pmod{\phi(n)} \text{ d.h.}$$
$$a \cdot b \equiv 1 \pmod{\phi(n)}$$

- ▶ Eulersche ϕ - Funktion

$$\phi(n) = (p - 1)(q - 1)$$

RSA - Verschlüsselung

Für $x, y \in \mathbb{Z}_n$ definiere

- ▶ Verschlüsselungsfunktion

$$e_k(x) = x^b \bmod n$$

- ▶ Entschlüsselungsfunktion

$$d_k(y) = y^a \bmod n$$

- ▶ Öffentlicher Schlüssel:

$$(n, b)$$

- ▶ Privater Schlüssel:

$$(p, q, a)$$



Brute - Force - Angriff

- ▶ Brute - Force - Angriff: Finde Zerlegung von n in p und q
- ▶ (Derzeit) Schwierig!

Bekannter Entschlüsselungsexponent

Wenn der Entschlüsselungsexponent a bekannt ist,
kann n in polynomieller Zeit faktorisiert werden.

Konsequenz: Nicht nur b , sondern auch n ist wertlos!

Quadratwurzeln 1 mod n

- ▶ Für $n = pq$ mit Primzahlen p, q gibt es 4 Quadratwurzeln der Form

$$x^2 \equiv 1 \pmod{n}$$

- ▶ *triviale* Quadratwurzeln $\pm 1 \pmod{n}$
 - ▶ 2 *nichttriviale* Quadratwurzeln
- ▶ Bestimmbar durch Lösen des Systems

$$x_1 \equiv 1 \pmod{p} \quad x_2 \equiv -1 \pmod{p}$$

$$x_1 \equiv -1 \pmod{q} \quad x_2 \equiv 1 \pmod{q}$$

mittels Chinesischem Restsatz

Faktorisierung von n

Mit Hilfe einer nichttrivialen Quadratwurzel x mit

$$x^2 \equiv 1 \pmod{n}$$

lässt sich n faktorisieren:

$$\gcd(x + 1, n) = p$$

$$\gcd(x - 1, n) = q$$

Algorithmus RSA-FACTOR(n , a , b)

- ▶ Bestimme eine Zufallszahl $w < n$
- ▶ Wenn $x = \gcd(w, n) > 1$ ist x Faktor von n , fertig.
- ▶ Zerlege $ab - 1$

$$ab - 1 = 2^s \times r$$

- ▶ Berechne sukzessive die Quadrate $w^r, w^{2r}, w^{4r}, \dots$ bis

$$w^{2^t r} \equiv 1 \pmod{n}$$

Da $w^{ab-1} = w^{2^s r} \equiv 1 \pmod{n}$ terminiert die Schleife immer.

- ▶ Ist die gefundene Quadratwurzel nichttrivial, faktorisiere n .
Ansonsten Fehlschlag.

Komplexität von RSA-FACTOR

- ▶ Erfolg des Algorithmus hängt von Zufall ab (*Las Vegas - Algorithmus*)
- ▶ Erfolgswahrscheinlichkeit von RSA-FACTOR ist mindestens $1/2$
- ▶ Erfolgswahrscheinlichkeit nach m Durchläufen

$$1 - \left(\frac{1}{2}\right)^m$$

Wiener's Low Decryption Exponent Attack

Der Entschlüsselungsexponent a lässt sich berechnen, wenn

$$3a < \sqrt[4]{n} \text{ und } q < p < 2q$$

erfüllt ist.

Vorüberlegungen

Da $ab \equiv 1 \pmod{\phi(n)}$, gibt es einen Integer t mit

$$ab - t\phi(n) = 1$$

Durch einige Umformungen und Abschätzungen folgt daraus

$$\left| \frac{b}{n} - \frac{t}{a} \right| < \frac{1}{3a^2}$$

Kettenbrüche

Ein (endlicher) *Kettenbruch* ist ein m -Tupel

$$[q_1, \dots, q_m]$$

als Abkürzung für den Ausdruck

$$q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots + \frac{1}{q_m}}}$$

Kettenbruchexpansion

- ▶ Alle gekürzten rationalen Zahlen $\frac{a}{b}$ lassen sich eindeutig als Kettenbruch darstellen (*Kettenbruchexpansion*).

$$\frac{a}{b} = [q_1, \dots, q_m]$$

- ▶ Die Kettenbruchexpansion kann aus dem Euklidischen Algorithmus gewonnen werden.
- ▶ Für j mit $1 \leq j \leq m$ ist

$$C_j = [q_1, \dots, q_j]$$

der j -te *Konvergent* von $[q_1, \dots, q_m]$.

Satz

Wenn $\gcd(a, b) = \gcd(c, d) = 1$ und

$$\left| \frac{a}{b} - \frac{c}{d} \right| < \frac{1}{2d^2}$$

gilt, ist $\frac{c}{d}$ einer der Konvergenten von $\frac{a}{b}$.

Anwendung auf RSA

- ▶ Berechne die Konvergenten $\frac{c_j}{d_j}$ von $\frac{b}{n}$
- ▶ Finde den “richtigen” Konvergenten: Für alle j
 - ▶ Berechne $\phi_j = (d_j b - 1)/c_j$
 - ▶ Wenn c_j/d_j der “richtige” Konvergent ist, ist $\phi_j = \phi(n)$.
 - ▶ Versuche, n zu faktorisieren:

$$\phi(n) = (p - 1)(q - 1)$$

Substituiere $q = n/p$, berechne p

$$0 = p^2 - (n - \phi(n) + 1)p + n$$

- ▶ Wenn keiner der Konvergenten n auf diese Weise faktorisiert, war die Anfangsbedingung nicht erfüllt

Das Rabin Kryptosystem

Sei $n = pq$ mit Primzahlen p, q und $p, q \equiv 3 \pmod{4}$.

$$K = (n, p, q)$$

Verschlüsselungsfunktion:

$$e_K(x) = x^2 \pmod{n}$$

Entschlüsselungsfunktion:

$$d_K(y) = \sqrt{y} \pmod{n}$$

für $x, y \in \mathbb{Z}_n^*$. Öffentlicher Schlüssel ist n , privater Schlüssel (p, q) .

Eigenschaften

- ▶ Verschlüsselung ist nicht injektiv,

$$\sqrt{y} \bmod n$$

hat 4 Lösungen

- ▶ Beweisbar sicher gegen *chosen plaintext* Angriffe, wenn das Faktorisierungsproblem schwierig ist.
- ▶ Unsicher gegen *chosen ciphertext* Angriffe

Polynomielle Problemreduktion

- ▶ Ein Problem G ist *polynomiell reduzierbar* auf ein Problem H , wenn eine Lösung von G in polynomieller Zeit aus einer Lösung von H gewonnen werden kann.

$$G \leq_p H$$

- ▶ G ist nicht schwieriger als H

$$H \in \mathcal{P} \Rightarrow G \in \mathcal{P}$$

Sicherheit von Rabins Kryptosystem

- ▶ Wenn Faktorisierung schwierig ist, ist Rabin sicher
- ▶ Zu zeigen: Faktorisierung ist nicht schwieriger als Rabin entschlüsseln

$$\text{FACTOR} \leq_p \text{RABIN_DECRYPT}$$

- ▶ Finde Algorithmus, der FACTOR mithilfe von RABIN DECRYPT löst

Faktorisierungsalgorithmus

- ▶ Bestimme Zufallszahl $r \in \mathbb{Z}_n^*$
- ▶ Berechne $x = \text{RABIN_DECRYPT}(r^2 \bmod n)$
- ▶ Wenn $x \equiv \pm r \pmod{n}$ Fehlschlag (triviale Quadratwurzel)
Sonst faktorisiere n :

$$p = \text{gcd}(x + r, n)$$

$$q = n/p$$

Der Algorithmus faktorisiert n mit einer Erfolgswahrscheinlichkeit von $1/2$.

Semantische Sicherheit

- Totale Entschlüsselung** Ein Angreifer erhält den geheimen Schlüssel und kann jeden Schlüsseltext entschlüsseln
- Partielle Entschlüsselung** Einem Angreifer gelingt es, aus dem Schlüsseltext spezifische Informationen über den Klartext zu erhalten
- Unterscheidbarkeit von Schlüsseltexten** Ein Angreifer ist in der Lage, Schlüsseltexte gegebenen Klartexten zuzuordnen
- Semantische Sicherheit** Ein Kryptosystem ist *semantisch sicher*, wenn es immun gegen Unterscheidbarkeit von Schlüsseltexten ist.

Einige Varianten partieller Entschlüsselung

Parity Berechne $parity(y)$ für gegebenes $y = e_K(x)$, wobei $parity(y) = 0$ falls x gerade und $parity(y) = 1$ falls x ungerade

Half Berechne $half(y)$ für gegebenes $y = e_K(x)$, wobei $half(y) = 0$ falls $0 \leq x < n/2$ und $half(y) = 1$ falls $n/2 < x \leq n - 1$

Sicherheit von RSA gegen $half(y)$

- ▶ RSA gibt keine Informationen zur effizienten Berechnung von $half(y)$ preis, wenn die Verschlüsselung insgesamt sicher ist
- ▶ Beweis über Problemreduktion von RSA-Entschlüsselung auf Berechnung von $half(y)$

$$\text{RSA_DECRYPT} \leq_p \text{HALF}(y)$$

- ▶ D.h. Berechnung von $half(y)$ ist nicht einfacher als totale Entschlüsselung