Attacken auf RSA

Mögliche Angriffspunkte

1. Die gleiche **Nachricht** wird an mehrere Personen mit gleichem öffentlichen Exponenten geschickt.
2. Zwei Personen verwenden den gleichen **Modulus**.

Attacke I: Low Exponent Attacke

Voraussetzungen:

- öffentlicher Exponent e ist relativ klein
- Alice verschickt die **gleiche** Nachricht an mehrere Personen

Erklärung am **Beispiel**:

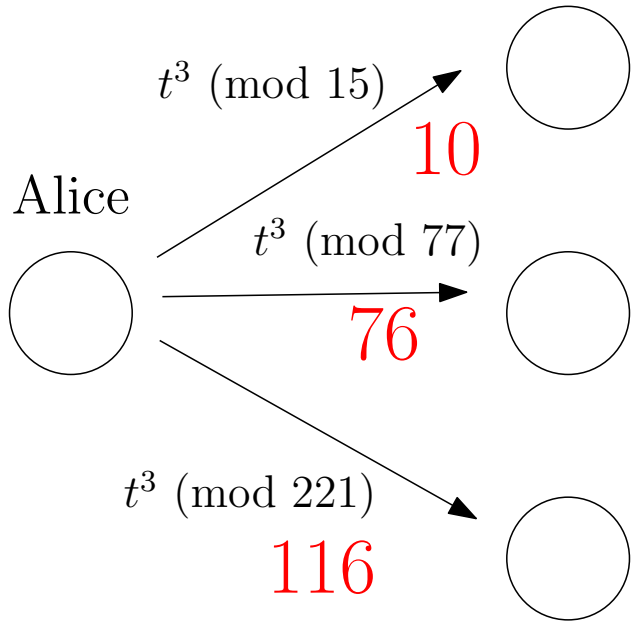
- $e = 3$
- Module der Empfänger: $m_1 = 15$, $m_2 = 77$, $m_3 = 221$
- **geheime** Nachricht $t = 10$

Attacke I: Low Exponent Attacke

Werte: $e = 3$, $m_1 = 15$, $m_2 = 77$, $m_3 = 221$, $t = 10$

geheime Berechnungen

$$10^3 = 10 \pmod{15}$$
$$10^3 = 76 \pmod{77}$$
$$10^3 = 116 \pmod{221}$$



Vorgehen

1. Bestimme mithilfe des chinesischen Restsatzes die Zahl x mit
   $$x = 10 \pmod{15}$$
   $$x = 76 \pmod{77}$$
   $$x = 116 \pmod{221}$$
2. $t := x^{1/3}$ (in den obigen Gleichungen steht x für t^3)

Bem: Die Berechnung im ersten Schritt erfolgt modulo $15 \cdot 77 \cdot 221$

Attacke I: Low Exponent Attacke

1. Bestimme mithilfe des chinesischen Restsatzes die Zahl x mit
   $$x = 10 \pmod{15}$$
   $$x = 76 \pmod{77}$$
   $$x = 116 \pmod{221}$$
2. $t := x^{1/3}$ (in den obigen Gleichungen steht x für t^3)

Berechnungsschritte

1.
   - $M_1 = 77 \cdot 221 = 17017$
   - $M_2 = 15 \cdot 221 = 3315$
   - $M_3 = 15 \cdot 77 = 1155$

   - bestimme u_1 s.d. $u_1 \cdot 17017 = 1 \pmod{15} \rightarrow \ldots \rightarrow u_1 = 13$
   - bestimme u_2 s.d. $u_2 \cdot 3315 = 1 \pmod{77} \rightarrow \ldots \rightarrow u_2 = 58$
   - bestimme u_3 s.d. $u_3 \cdot 1155 = 1 \pmod{221} \rightarrow \ldots \rightarrow u_3 = 84$

   $$\Rightarrow x = 10 \cdot (13 \cdot 17017) + 76 \cdot (58 \cdot 3315) + 116 \cdot (84 \cdot 1155) = 28079050$$
   $$= 1000 \pmod{15 \cdot 77 \cdot 221}$$
2. $t = x^{1/3} = 10$

Attacke II auf RSA – Vorüberlegungen

- $2|6$ (bedeutet: 2 teilt 6)
- Für jede beliebige Zahl a gilt: $a = 1 \pmod 6 \Rightarrow a = 1 \pmod 2$

(Begründung: $a = 1 \pmod 6 \Rightarrow a = 6 + \ldots + 6 + 1 \Rightarrow a = 1 \pmod 2$)

- **Allgemein:** Falls $r|s$, dann gilt: $a = 1 \pmod s \Rightarrow a = 1 \pmod r$

(Begründung: $a = 1 \pmod s \Rightarrow a = \underbrace{s + \ldots + s}_{=0 \pmod r} + 1 \Rightarrow a = 1 \pmod r$)

Attacke II auf RSA: Common Modulus Attacke

- **Situation:** Zwei Personen verwenden den gleichen Modulus
  - Schlüssel von Oscar (Angreifer): (e_1, m) (öffentlich), d_1 (privat)
  - Schlüssel von Alice (Opfer): (e_2, m) (öffentlich), d_2 (privat)

d_2 ↑ Oscar's Ziel

Oscars Ziel: Finde ein x, so dass ...

$x \cdot e_2 = 1 \pmod{v}$ mit $\varphi(m)|v$ $(\Rightarrow \quad x \cdot e_2 = 1 \pmod{\varphi(m)})$

Vorgehen (Bsp: $m = 91$, $e_1 = 5$, $d_1 = 29$, $e_2 = 7$)

1. $v := e_1 \cdot d_1 - 1$ (Bsp: $v = 5 \cdot 29 - 1 = 144$)
2. Fall 1: $\mathrm{ggT}(v, e_2) = 1$

   berechne x s.d. $x \cdot e_2 = 1 \pmod{v}$ (Bsp: $x \cdot 7 = 1 \pmod{144}$)
   (mit Euklid-Algo oder mod. Inversen) (Bsp: $x = 103$)
3. Fall 2: $\underbrace{\mathrm{ggT}(v, e_2)}_{g} > 1$ [Problem: unterstrichene Gl. nicht lösbar]

   $\tilde{v} := \frac{v}{g}$

   berechne x s.d. $x \cdot e_2 = 1 \pmod{\tilde{v}}$

Attacke II auf RSA: Common Modulus Attacke

Begründung, dass auch im Fall 2 der richtige Wert gefunden wird

3. Fall 2: $\underbrace{\mathrm{ggT}(v, e_2)}_{g} > 1$

   $\tilde{v} := \frac{v}{g}$

   berechne x s.d. $x \cdot e_2 = 1 \pmod{\tilde{v}}$

Bem:

- Da (e_2, m) ein öffentlicher Schlüssel ist, müssen e_2 und $\varphi(m)$ teilerfremd sein (vgl. Serie 1, Aufgabe 5a).
- $\Rightarrow$ g enthält *keinen* Teiler von $\varphi(m)$
- Beim Teilen durch g geht somit kein Teiler von $\varphi(m)$ verloren
- $\Rightarrow \varphi(m) | \tilde{v}$
  aus d. untersten Gleichung folgt automatisch $x \cdot e_2 = 1 (\mathrm{mod}\ \varphi(m))$