

2.8 Kleine Exponenten

Frage: Ist es beim RSA-Verfahren gefährlich, einen kleinen öffentlichen Exponenten e zu wählen?

Der Exponent $e = 1$ ist völlig unbrauchbar, da dann nicht verschlüsselt wird.

Der Exponent $e = 2$ ist für RSA nicht verwendbar, da er gerade und somit nicht teilerfremd zu $\lambda(n)$ ist. Es gibt allerdings eine verwandte Chiffre, das RABIN-Verfahren, das gerade mit $e = 2$ so arbeitet. Bei diesem muss der Empfänger Quadratwurzeln mod n ziehen können, und das kann er, wenn er n faktorisieren kann (siehe später). (Er muss auch noch eine Möglichkeit haben, unter den verschiedenen Quadratwurzeln den richtigen Klartext zu erkennen.)

Der kleinste für das RSA-Verfahren prinzipiell geeignete Exponent ist $e = 3$. Hier entsteht eine Schwäche, sobald jemand die gleiche Nachricht a an *drei* verschiedene Teilnehmer A, B und C schickt. Deren öffentliche Schlüssel seien $(n_A, 3)$, $(n_B, 3)$ und $(n_C, 3)$. O. B. d. A. sind die Moduln n_A , n_B und n_C paarweise teilerfremd, sonst kann die Angreiferin mindestens zwei davon faktorisieren, also erst recht a lesen. Ansonsten hat sie (mit etwas Glück) drei Geheimtexte

$$c_A = a^3 \bmod n_A, \quad c_B = a^3 \bmod n_B, \quad c_C = a^3 \bmod n_C$$

mit $0 \leq a < n_A, n_B, n_C$, also $a^3 < n_A n_B n_C$. Mit dem chinesischen Restalgorithmus konstruiert sie daraus eine Zahl $\tilde{c} \in \mathbb{Z}$ mit

$$0 \leq \tilde{c} < n_A n_B n_C$$

und

$$\tilde{c} \equiv c_X \quad \text{für } X = A, B, C.$$

Wegen der Eindeutigkeit ist $\tilde{c} = a^3$ in \mathbb{Z} . Damit bestimmt sie $a = \sqrt[3]{\tilde{c}}$ durch Wurzelziehen in \mathbb{Z} . (Auch hier gelingt es ihr nicht, die geheimen Exponenten zu bestimmen.)

Die Verallgemeinerung dieses Angriffs auf einen beliebigen „kleinen“ gemeinsamen öffentlichen Exponenten ist offensichtlich: Wenn eine identische Nachricht an e verschiedene Teilnehmer geschickt wird, kann diese von jedem gelesen werden. So abwegig ist dieser Angriffspunkt nicht, wenn man sich etwa eine konstante „Protokollinformation“ am Beginn längerer Nachrichten vorstellt. In der Praxis wird der Exponent $e = 2^{16} + 1 = 65537$ meist als hinreichend sicher für „normale“ Anwendungen angesehen.