Dr. Dirk Frettlöh 22.5.2019

Übungen zur Vorlesung Kryptographie

Blatt 7

Aufgabe 25: (RSA nutzen)
Es sei $N = pq = 899$, also $p = 29$, $q = 31$. Der öffentliche Schlüssel ist $e = 31$.

(a) Verschlüsseln Sie die Nachricht $m = 712$.
(b) Berechnen Sie d (das geht, weil wir ja die Primfaktoren von N kennen), und entschlüsseln Sie die Nachricht $c = 631$.

Aufgabe 26: (RSA knacken I)
Diese Aufgabe demonstriert: Ist die Nachricht m nicht teilerfremd zu N, dann ist m lesbar.

(a) Zeigen Sie dazu erstens: $\mathrm{ggT}(N, c)$ liefert einen der beiden Primfaktoren von N. Beschreiben Sie dann, wie man daraus effizient den anderen Primfaktor von N, dann $\varphi(N)$ und schließlich d berechnet.

(b) Demonstrieren Sie dann die Methode am Zahlenbeispiel $N = 899 = 29 \cdot 31$, $e = 17$, $c = 651$.

Aufgabe 27: (RSA knacken II)
Diese Aufgabe zeigt, dass es keine gute Idee ist, p sehr nah an q zu wählen.

(a) Zeigen Sie, dass $N = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$ und dass $\frac{p+q}{2} \in \mathbb{N}$ für Primzahlen $p > q > 2$.

Falls p und q in etwa gleich groß sind, sind also p und q ungefahr so groß wie $\sqrt{N}$. Damit ist auch $A := \frac{p+q}{2}$ in etwa gleich $\sqrt{N}$, und $B := \frac{p-q}{2}$ ist klein dagegen. Wegen (a) ist $N = A^2 - B^2$, also $B^2 = A^2 - N$.

Also probieren wir $a = \lceil \sqrt{N} \rceil$ und testen, ob $a^2 - N$ eine Quadratzahl ist. Falls ja, so sind (mit $b = \sqrt{a^2 - N}$) die Zahlen $a - b$ und $a + b$ Teiler von N.

(b) Warum?

Falls nicht, setzen wir $a := a + 1$ und machen weiter.

(c) Demonstrieren Sie das Verfahren am Beispiel $N = pq = 23360947609$.

Aufgabe 28: (RSA knacken III)
Zunächst spricht nichts gegen kleine öffentliche Teilschlüssel e. Außer falls viele Nutzer dasselbe e nutzen. Wir betrachten folgendes Szenario: In einem Onlinebankingsystem benutzen alle Nutzer dasselbe $e = 3$. Also wählt jeder Nutzer ein $N = pq$, so dass $\text{ggT}(\varphi(N), 3) = 1$ und ein d mit $3d \equiv 1 \bmod \varphi(N)$. Angenommen, die Nutzer Alice_1, Alice_2 und Alice_3 haben als N jeweils

$$N_1 = 5000746010773, \quad N_2 = 5000692010527, \quad N_3 = 5000296004107.$$

Bob sendet nun dieselbe Nachricht m an Alice_1, Alice_2 und Alice_3; also $c_i \equiv m^3 \bmod N_i$. Eve belauscht

$$c_1 = 1549725913504, \quad c_2 = 2886199297672, \quad c_3 = 2972130153144.$$

(a) Beschreiben Sie, wie Eve den Wert von m bestimmen kann, ohne das e zu kennen. *(Tipp: chinesischer Restsatz).*

(b) Berechnen sie m nach der Methode aus (a)

(c) In manchen realen Onlinebankingsystemen wird für alle Nutzer derselbe öffentliche Teilschlüssel $e = 2^{16} + 1$ benutzt. Wieviele verschlüsselte Texte mit dem gleichen Klartext m muss Eve nun abfangen, um m zu berechnen?

(d) Wie kann die RSA-Verschlüsselung angepasst werden, um diesen Angriff zu verhindern?

Falls Sie Programmcode abgeben, bitte (1) auch erklären, wie Sie vorgingen, (2) auch das Ergebnis aufschreiben, und (3) bitte den Code selbst (kein Foto) an den Tutor schicken.

Abgabe: Mittwoch 29.5.2019 bis 14 Uhr in Postfach 2183 in V3, oder per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben! (Di oder Do)

Dienstag	Philipp Braukmann	pbraukmann@techfak.uni-bielefeld.de
Donnerstag	Oliver Tautz	otautz@techfak.uni-bielefeld.de