

Übungen zur Vorlesung Kryptographie

Blatt 6

Aufgabe 21: (RSA nutzen)

Alices öffentlicher Schlüssel ist $(N, e) = (551, 31)$. Es ist $N = pq = 19 \cdot 29$.

- (a) Sie sind Bob. Verschlüsseln Sie die Botschaft $m = 422$ an Alice.
- (b) Sie sind Alice. Entschlüsseln Sie den Geheimtext $c = 370$.

Aufgabe 22: (RSA knacken I)

Sie sind Eve. Sie kennen Alices öffentlichen Schlüssel $(N, e) = (168149075693, 31)$. Außerdem erfahren Sie aus dunklen Kanälen, dass $\varphi(N) = 168148245408$.

- (a) Berechnen Sie nach dem Verfahren aus Bemerkung 5.1 im Skript die Primfaktoren p und q von N . *(Andere Methoden würden hier funktionieren, weil die Werte so klein sind, gelten aber nicht als Lösung.)*
- (b) Entschlüsseln Sie den mit den obigen Daten verschlüsselten Geheimtext $c = 1409463781$.

Aufgabe 23: (RSA knacken II)

Diese Aufgabe demonstriert: Ist die Nachricht m nicht teilerfremd zu N (also $\text{ggT}(m, N) \neq 1$), dann ist m lesbar.

- (a) Zeigen Sie dazu erstens: $\text{ggT}(N, c)$ 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 $N = 899 = 29 \cdot 31$, $e = 17$, $c = 527$. Was ist in diesem Fall der Wert von m ?

Aufgabe 24: (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 $3d \equiv 1 \pmod{\varphi(N)}$. Angenommen, die Nutzer Alice₁, Alice₂ und Alice₃ haben als N jeweils

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

Bob sendet nun dieselbe Nachricht m an Alice₁, Alice₂ und Alice₃; also $c_i \equiv m^3 \pmod{N_i}$. Eve erfährt, dass Bob dreimal dasselbe m gesendet hat und belauscht

$$c_1 = 2700017742623, \quad c_2 = 4349505357688, \quad c_3 = 1082033621441.$$

- (a) Beschreiben Sie, wie Eve den Wert von m bestimmen kann, ohne das d zu kennen. *(Tipp: chinesischer Restsatz, sowie der Abschnitt „Kleine m “ im Skript auf Seite 22).*
- (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?

Abgabe bis Mittwoch 20.5.2020 bis 14 Uhr per Email an den Tutor.

Philipp Braukmann pbraukmann@techfak.de
Jonas Friemel jfriemel+krypto@techfak.de