

Übungen zur Vorlesung Kryptographie

Blatt 6

Aufgabe 21: (RSA nutzen)

Alices öffentlicher Schlüssel ist $(N, e) = (91, 11)$. Es ist $N = pq = 7 \cdot 13$. Wir kodieren Buchstaben wie üblich mit $a=0, b=1, \dots, z=25$.

(a) Sie sind Bob. Verschlüsseln Sie die Botschaft $m = \text{arminia}$ an Alice (jeden Buchstaben einzeln, Alice erhält also eine Liste von 7 Zahlen).

(b) Sie sind Alice. Entschlüsseln Sie den Geheimtext $c = (61, 14, 75, 24, 38, 41, 13, 61)$.

Aufgabe 22: (RSA knacken mit Whistleblower)

Sie sind Eve. Sie kennen Alices öffentlichen Schlüssel $(N, e) = (212171, 31)$. Außerdem erfahren Sie aus dunklen Kanälen, dass $\varphi(N) = 211200$.

(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 $c = 12735$.

Aufgabe 23: (RSA knacken mit Euklid)

Diese Aufgabe illustriert das Beispiel "Gemeinsame Primfaktoren" im Skript. Alice₁, Alice₂ und Alice₃ haben die öffentlichen Schlüssel

$$(e_1, N_1) = (13, 9379), \quad (e_2, N_2) = (17, 9797), \quad (e_3, N_3) = (19, 9991).$$

Finden Sie einen gemeinsamen Primfaktor von zwei dieser N_i . Finden Sie damit den geheimen Schlüssel von Alice₂ und entschlüsseln Sie die Nachricht $c = 8099$ von Alice₂.

Aufgabe 24: (RSA knacken mit Chinesen)

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

$$N_1 = 1234698768539, \quad N_2 = 1234698768731, \quad N_3 = 1234709880589.$$

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

$$c_1 = 1227388885583, \quad c_2 = 2987984480, \quad c_3 = 795997958345.$$

- (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 Montag 23.5.2022 bis 14 Uhr per Email an Ihren Tutor.

Bitte auf jeder Abgabe das Tutorium angeben. Bitte die Abgaben so nennen: *techfakaccount-blm.pdf*, also z.B. *dfrettloeh-bl6.pdf*, oder *dfrettloeh+mnebel-bl6.pdf*.

Jan-Philipp Brünger	jbruenger@techfak.de
Simon Hahm	shahm+krypto@techfak.de
Tim Lakämper	tlakaemper+krypto@techfak.de