Dr. Dirk Frettlöh 20.5.2026

Übungen zur Vorlesung Kryptographie

Blatt 6

Aufgabe 21: (RSA nutzen)
Alices öffentlicher Schlüssel ist $(N, e) = (91, 17)$. Es ist $N = pq = 7 \cdot 13$. Wir kodieren Buchstaben wie üblich mit a=0, b=1, ..., z=25.

(a) Sie sind Bob. Verschlüsseln Sie die Botschaft $m =$ fermat an Alice (jeden Buchstaben einzeln, Alice erhält also eine Liste von fünf Zahlen).
(b) Sie sind Alice. Entschlüsseln Sie den Geheimtext $c = (80, 76, 75, 8, 13, 41)$.

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 die mit den obigen Daten verschlüsselte Geheimbotschaft $c = 120700$. (Dieses c ist *eine* Zahl, und nicht etwa $12, 07, 00$.)

Aufgabe 23: (RSA knacken mit Euklid)
Diese Aufgabe illustriert das Beispiel "Gemeinsame Primfaktoren" im Skript. Alice_1, Alice_2 und Alice_3 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 Alice_2 und entschlüsseln Sie die Nachricht $c = 8897$ von Alice_2.

Aufgabe 24 auf Seite 2.

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 $3d \equiv 1 \bmod \varphi(N)$. 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 erfährt, dass Bob dreimal dasselbe m gesendet hat und belauscht

$$c_1 = 2247043233952, \quad c_2 = 1575736442472, quadc_3 = 793895878638.$$

(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 wurde 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 27.5.2026 bis 12:00 Uhr per Email an die Tutorin.

Lisa Henetmayr Mi 12 Uhr in S0-115 lhenetmayr+krypto@techfak.de
Lisa Henetmayr Mi 16 Uhr in U2-147 lhenetmayr+krypto@techfak.de