Übungen zur Vorlesung Kryptographie

Blatt 6

Aufgabe 21: (RSA nutzen)
Alices öffentlicher RSA-Schlüssel ist $(N, e) = (273373, 65537)$. Wir codieren wieder Buchstaben als Zahlen so: a=0, b=1, ... z=25. Aber wir fassen diesmal je drei Buchstaben zu einem Block zusammen (Beispiel: der Text "bcd efg"wird zu 010203 040506, also $m = (m_1, m_2) = (10203, 40506)$.) Die Blöcke m_i werden dann einzeln mit RSA verschlüsselt.

(a) Sie sind Bob. Verschlüsseln Sie die Botschaft "bielefeld" an Alice.

(b) Sie sind Alice. Entschlüsseln Sie die Botschaft $(0, 149578, 35224)$. *(Das geht nur, weil die Zahlen so unrealistisch klein sind, dass Sie leicht Alices geheimen Schlüssel ermitteln können.)*

Aufgabe 22: (RSA knacken mit Taschenrechner)
Sie sind Eve. Sie kennen Alices öffentlichen Schlüssel $(N, e) = (1007, 31)$. Außerdem erfahren Sie aus dunklen Kanälen, dass $\varphi(N) = 936$.

(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) Berechnen Sie Alices geheimen Schlüssel und entschlüsseln Sie den mit den obigen Daten verschlüsselten Geheimtext $c = 358$.
(Teil (b) ist unabhängig von (a). Beide Teile können auch nur mit Stift und Papier gelöst werden.)

Aufgabe 23: (RSA knacken mit Heimtücke)
(a) Eine potenzielle Schwäche von RSA (in der Version aus der Vorlesung) ist, dass es *multiplikativ* ist, das heißt, $f(e, m_1 \cdot m_2) = f(e, m_1) \cdot f(e, m_2)$. Zeigen Sie diese Eigenschaft.

(b) Angenommen, Eve kennt einen Geheimtext $c_1 = f(e, m_1)$, den Bob an Alice schickte (aber Eve kennt nicht das m_1). Weiter angenommen, Eve kann Alice überreden, ihr einen von Eve ausgewählten Geheimtext $c_2 \neq c_1$ (mit dem privaten Schlüssel zu dem e von oben) zu einem Klartext m_2 zu entschlüsseln. Wie kann Eve die Schwäche in (a) ausnutzen, um das c_2 so heimtückisch zu wählen, dass sie damit das m_1 ermitteln kann?

(c) Wie kann das RSA aus der Vorlesung angepasst werden, um diesen Angriff zu unterbinden?

Aufgabe 24: (RSA knacken mit Wurzelziehen in $\mathbb{R}$)
Diese Aufgabe zeigt, dass es keine gute Idee ist, p sehr nah an q zu wählen. Sie also $N = pq$.

(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 $p > q > 2$.

(b) Falls p und q in etwa gleich groß sind, sind also p und q ungefähr 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. Falls nicht, setzen wir $a := a + 1$ und machen weiter.

Und nun kommt endlich die Frage zu (b): Warum ist das sinnvoll? Und wie ermitteln wir so p und q?

(c) Demonstrieren Sie das Verfahren am Beispiel $N = pq = 29486787091736557658392000 8771513215081$.

Abgabe bis Dienstag 16.5.2023 bis 23:59 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jakob Niermann janiermann+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de