5. Übungsblatt
Kryptographie und Mediensicherheit (SoSe 2016)

Bauhaus-Universität Weimar, Professur für Mediensicherheit
Prof. Dr. Stefan Lucks, Jakob Wenzel
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching`
Abgabe: Bis zum 20.06.2015, 13:30 Uhr zu Beginn der Übung oder per E-Mail an `jakob.wenzel(at)uni-weimar.de`.
Lösungen sind bevorzugt in LaTeX zu verfassen. Ein Template finden Sie auf der Übungsseite der Veranstaltung. **Denken Sie daran, stets nachvollziehbare Lösungswege mit anzugeben. Für Lösungen, deren Herkunft nicht nachvollziehbar ist, werden 0 Punkte vergeben**.

Aufgabe 1 – Kleiner RSA-Modulus (4 Punkte)
Alice, Bob und Charlie haben als öffentlichen RSA-Exponenten $e = 5$ gewählt. Ihre öffentlichen RSA-Moduli n_A, n_B und n_C seien paarweise teilerfremd. Eve möchte eine Nachricht m jeweils an Alice, Bob und Charlie schicken und verschlüsselt m wie folgt:

$$\begin{aligned} c_A &\equiv m^5 \bmod n_A \quad \text{mit} \quad c_A = 189 \text{ und } n_A = 299, \\ c_B &\equiv m^5 \bmod n_B \quad \text{mit} \quad c_B = 197 \text{ und } n_B = 323, \\ c_C &\equiv m^5 \bmod n_C \quad \text{mit} \quad c_C = 275 \text{ und } n_C = 319. \end{aligned}$$

Zeigen Sie, dass jeder mit Kenntnis von c_A, c_B, und c_C die Nachricht m entschlüsseln kann. (*Hinweis:* Wiederholen Sie den chinesischen Restsatz).

Aufgabe 2 – Schwächen von RSA (2+4 Punkte)

a) Seien n_A und n_B verschiedene RSA-Moduli von Alice bzw. Bob. Angenommen, n_A und n_B teilen sich den Primfaktor p. Zeigen Sie, dass jeder mit diesem Wissen n_A und n_B effizient faktorisieren kann.

b) In der Firma ROTI.26 Inc. wird ein neuer IT-Security-Manager eingestellt, welcher die PKI (Public Key Infrastructure) signifikant optimieren soll, um den Verwaltungsaufwand zu minimieren und im Zweifelsfall Mitarbeiter überwachen/überführen zu können. Deshalb werden folgende Maßnahmen getroffen:

- Die Firma erstellt alle Schlüsselpaare (e_i, d_i) mit dem selben RSA-Modulus n.
- Jeder Mitarbeiter bekommt ein Schlüsselpaar (e_i, d_i) ausgehändigt, wobei gilt: alle Paare (e_i, d_i) und (e_j, d_j) sind verschieden und $\text{ggT}(e_i, e_j) = 1$, $\forall i, j$. Letzteres wird umgesetzt, da so der Auswahlprozess für neue öffentliche Exponenten beschleunigt wird.

Angenommen der CEO der Firma sendet die gleiche Nachricht m an zwei verschiedene Projektleiter. Eve überwacht das Netzwerk und fängt die dazugehörigen Chiffretext c_1 und c_2 ab. Zeigen Sie, dass Eve, ohne Kenntnis der geheimen Schlüssel, die Nachricht m wiederherstellen kann.

Aufgabe 3 – Gruppentheorie (2+2 Punkte)
Lösen Sie die beiden folgenden Aufgaben mit Argumenten aus der Gruppentheorie.

a) Um eine Implementierung des Diffie-Hellmann Schlüsselaustausches zu vereinfachen, soll die additive Gruppe $(\mathbb{Z}_p, +)$ anstelle der multiplikativen Gruppe $(\mathbb{Z}_p^*, \cdot)$ genutzt werden. Ist dieser Schritt sinnvoll in Bezug auf die Sicherheit des Diffie-Hellman Schlüsselaustausches? Begründen Sie ihre Antwort.

b) Betrachten Sie das ElGamal-Verschlüsselungsschema aus der Vorlesung (Kapitel 5.4 Folie 178 ff.). Wie wird die Sicherheit von der ElGamal-Verschlüsselung beeinflusst, wenn der Wert für g kein erzeugendes Element der Gruppe $\mathbb{Z}_p$ ist? Warum ist beispielsweise die Wahl $g = 1$ keine gute Entscheidung? Begründen Sie ihre Antwort.

Aufgabe 4 – Diffie-Hellman-Protokoll (2+2(+1) Punkte)
Alice und Bob wollen mittels Diffie-Hellman einen Schlüssel aushandeln. Sie wählen eine große Primzahl p und einen Generator $g \in \mathbb{Z}_p^*$. Alice wählt zufällig ein geheimes $a \in \mathbb{Z}_p^*$ und Bob ein geheimes $b \in \mathbb{Z}_p^*$. Alice schickt Bob ihren öffentlichen Schlüssel (A, g, p) mit $A = g^a \bmod p$ und Bob antwortet mit $B = g^b \bmod p$:

a) Berechnen Sie beispielhaft einmal für $g = 11$ und $p = 991$ sowie einmal für $g = 11$ und $p = 983$ die jeweils durchschnittliche Ordnung $ord(\langle g^{ab} \rangle)$ über alle $a, b \in \{1, \ldots, p-1\}$, z. B. mit einem kleinen Python-Skript (*Hinweis:* Es gilt $ord(\langle g^i \rangle) = \frac{ord(\langle g \rangle)}{ggT(ord(\langle g \rangle), i)}$).

b) Wir betrachten zwei Methoden um p zu wählen: (1) $p-1$ besitzt viele kleine Primteiler: $p-1 = q_1 \cdot q_2 \cdot q_3 \cdot \ldots$ und (2) $p-1 = m \cdot q$, für kleines m und eine große Primzahl q. Erläutern Sie: Welche Wahlmethode für p bietet höhere Sicherheit für den auszuhandelnden Schlüssel und was heißt höhere Sicherheit hier?

c) **Bonus (+1 Punkt):** Angenommen, $p - 1 = m \cdot q$ für kleines m und q prim. Alice wählt (absichtlich oder zufällig) $a = q$. Wie beeinflusst dieser Umstand die Sicherheit des ausgehandelten Schlüssels?

Aufgabe 5 – (Bonus) Fehlerhafte Implementierung von RSA (+4 Punkte)
Alice und Bob wollen RSA nutzen, um einen geheimen Schlüssel K zu übertragen. Dazu wählt Alice einen 64-bit-Schlüssel K und kodiert und verschlüsselt ihn mit Bobs öffentlichem RSA-Schlüssel (n, e) zu $Y \leftarrow (0 \ldots 0 \,\|\, K)^e \bmod n$. Anschließend sendet sie Y an Bob. Bob berechnet $K' = Y^d \bmod n$. Eve hört Y mit und möchte K rausfinden.

Angenommen, Bob antwortet Alice mit "success" wenn $K' < 2^k$ ist und mit "fail" wenn $K' \geq 2^k$ ist. Beschreiben Sie einen Algorithmus, der Bob als Orakel nutzt um so effizient wie möglich den Schlüssel K wiederherstellen kann.
(Zum Verständnis können Sie dazu Kapitel 5 aus [1] lesen.)

Literatur

[1] Kühn, Ulrich. "Side-channel attacks on textbook RSA and ElGamal encryption." Public Key Cryptography—PKC 2003. Springer Berlin Heidelberg, 2002. 324-336.