Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 18.12.2015
Abgabe: Mo. 11.01.2016 bis 14:00 (D3 Kasten)/14:45 Uhr (Fürstenallee)

Einführung in Kryptographie

WS 2015/2016

Heimübungszettel 5

AUFGABE 1 (6 Punkte)**:**
Sei $N = pq$ ein RSA-Modul.

a) Zeigen Sie, dass aus $\varphi(N)$ die Faktorisierung von N effizient berechnet werden kann.
Tipp: Versuchen Sie eine quadratische Gleichung aufzustellen.

b) Faktorisieren Sie $N = 309641$ mit $\varphi(N) = 308484$ basierend auf dem Ergebnis aus a).

AUFGABE 2 (5 Punkte)**:**
Sei $N = pq$ ein RSA-Modul.

a) Sie wählen ein $m \in \mathbb{Z}_N$ zufällig gleichverteilt. Wie groß ist die Wahrscheinlichkeit, dass $m \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$ gilt?

b) Sei $m \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$, $m \neq 0$ und e der öffentliche Exponent. Zeigen Sie, dass dann aus c mit $c \equiv m^e \mod N$ die Faktorisierung von N effizient berechnet werden kann.

c) Sie wählen ein $m \in \mathbb{Z}_N$ zufällig gleichverteilt. Wie groß ist die Wahrscheinlichkeit, dass m beide Bedingungen $m \equiv 1 \mod p$ und $m \not\equiv 1 \mod q$ gleichzeitig erfüllt?

AUFGABE 3 (4 Punkte)**:**
Betrachten Sie das Elgamal-Kryptosystem. Seien die Schlüssel $sk = (p, g, a)$ und $pk = (p, g, h)$ fest. Zu einem Klartext $m \in \mathbb{Z}_p$ bezeichne dann $C(m) \subseteq \mathbb{Z}_p^* \times \mathbb{Z}_p$ die Menge aller möglichen Chiffretexte der Nachricht m. Zeigen Sie, dass für alle $m_1, m_2 \in \mathbb{Z}_p$ mit $m_1 \neq m_2$ gilt:

$$C(m_1) \cap C(m_2) = \emptyset.$$

AUFGABE 4 (6 Punkte)**:**
Zeigen Sie: Das Elgamal-Kryptosystem ist nicht sicher gegen *Chosen-Ciphertext-Angriffe (CCA)*. Beschreiben Sie dazu einen effizienten CCA-Angreifer, der jeden gegebenen Chiffretext $c = (c_1, c_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p$ entschlüsseln kann, wobei nur eine Entschlüsselungsanfrage für $c' \in \mathbb{Z}_p^* \times \mathbb{Z}_p, c' \neq c$ ausgeführt wird.

AUFGABE 5 (6 Punkte)**:**
Betrachten Sie das *Diffie-Hellman-Problem* (DH) aus der Vorlesung. Zeigen Sie, dass die Elgamal-Entschlüsselung eines Chiffretextes ohne Kenntnis des zugehörigen privaten Schüssels äquivalent zur Lösung des Diffie-Hellman-Problem ist. Gehen Sie dazu in zwei Schritten vor:

a) Gegeben sei ein Elgamal Angreifer $\mathcal{A}$, der bei Eingabe von (pk, c) das Element m ausgibt. Dabei sei $m \in \mathbb{Z}_p$, $pk = (p, g, h)$ ein beliebiger öffentlicher Elgamal Schlüssel und $c \in \mathbb{Z}_p^* \times \mathbb{Z}_p$ die Verschlüsselung einer beliebigen Nachricht m unter dem Schlüssel pk. Geben Sie eine polynomielle Reduktion des DH Problems auf $\mathcal{A}$ an.

b) Gegeben sei ein Algorithmus $\mathcal{B}$, der bei Eingabe einer beliebigen Primzahl p, eines beliebigen Generators $g \in \mathbb{Z}_p^*$ und der Elemente $g^a, g^b \in \mathbb{Z}_p^*$ für alle $a, b \in \mathbb{Z}$ das Element $g^{ab} \in \mathbb{Z}_p^*$ ausgibt. Konstruieren Sie einen Angreifer, der $\mathcal{B}$ benutzt und in polynomieller Zeit Elgamal verschlüsselte Nachrichten ohne Kenntniss des geheimen Schlüssels entschlüsseln kann.