Wolfgang K. Seiler
Tel. 2515

A5, C201

4. Juni 2013

Modulklausur Kryptologie I

• • • **Schreiben Sie bitte auf jedes Blatt Ihren Namen!** • • •

Aufgabe 1: (*6 Punkte*)

a) AES kann aufgefaßt werden als eine monoalphabetische Substitution auf dem Alphabet bestehend aus allen Bitfolgen der Länge 128. Warum ist das Verfahren trotzdem sicher gegen die Art von Angriffen, mit denen sich die monoalphabetischen Verschlüsselungen vergangener Jahrhunderte so einfach knacken lassen?

b) In wenigen Jahrzehnten werden Computer so leistungsfähig sein, daß sie AES mit 128 Bit-Schlüsseln genauso einfach knacken können wie heute DES. Wer dann noch AES benutzen will, könnte versucht sein, nach Art von Triple-DES einen Triple-AES zu definieren: Er wählt zwei AES-Schlüssel $k_1, k_2 \in \mathbb{F}_2^{128}$ und verschlüsselt einen 128-Bit-Block $x \in \mathbb{F}_2^{128}$ als $\mathrm{AES}_{k_1}\Big(\mathrm{AES}_{k_2}^{-1}\big(\mathrm{AES}_{k_1}(x)\big)\Big)$. Welche Vor- und/oder Nachteile hat dies gegenüber AES mit Schlüssellänge 256?

c) Angenommen, ein Gegner hat einen so schnellen Computer, daß er AES mit 128 Bit in akzeptabler Zeit durch systematisches Durchprobieren aller Schlüssel knacken kann. Welche weiteren technischen Möglichkeiten bräuchte er, damit er auch eine doppelte AES-Verschlüsselung der Form $x \mapsto \mathrm{AES}_{k_1}\big(\mathrm{AES}_{k_2}(x)\big)$ nach Art des bekannten Angriffs auf Doppel-DES knacken könnte? Beschreiben Sie seine Strategie!

Aufgabe 2: (*10 Punkte*)

a) Warum gilt bei RSA mit Modul N, öffentlichem Exponenten e und privatem Exponenten d für *alle* ganzen Zahlen a die Kongruenz

$$\big(a^e\big)^d \equiv a \bmod N\,?$$

Verwenden Sie zum Beweis nur den kleinen Satz von Fermat!

b) Wie müßte man RSA modifizieren, wenn man modulo dem Produkt $N = pqr$ von drei verschiedenen Primzahlen arbeiten würde? Welche Bedingung müßte dann der öffentliche Exponent e erfüllen, und wie würde man diesen privaten Exponenten d aus e berechnen?

c) Welche Vor- und/oder Nachteile hätte das so modifizierte RSA-Verfahren gegenüber dem üblichen?

d) Wie läßt sich das modifizierte RSA-Verfahren bei kleinem privaten Exponenten angreifen?

Aufgabe 3: (*6 Punkte*)

a) Bestimmen Sie für das RSA-System mit Modul $N = 8509 = 67 \cdot 127$ und $e = 17$ eine natürliche Zahl d, so daß $(a^e)^d \equiv a \bmod N$ für alle $a \in \mathbb{Z}$!

b) Zeigen Sie, daß *a)* auch eine Lösung $d \leq 1500$ hat!

• • • **Bitte wenden!** • • •

Aufgabe 4: (*6 Punkte*)

a) Wie läßt sich bei RSA mit einem kleinen öffentlichen Exponenten e wie $e = 3$ oder $e = 5$ der private Exponent d ohne EUKLIDischen Algorithmus aus e und den Primzahlen p, q berechnen?

b) Ein RSA-System mit Modul $N = p \cdot q = 10\,774\,633$ verwendet den öffentlichen Exponenten drei und privaten Exponenten $d = 7\,178\,467$. Berechnen Sie $\varphi(N) = (p-1)(q-1)$!

c) Bestimmen Sie die Primzahlen p und q! Falls Sie ohne Taschenrechner arbeiten, genügt es, wenn Sie eine Formel für p und q angeben.

Aufgabe 5: (*10 Punkte*)

a) Berechnen Sie den diskreten Logarithmus modulo 19 von 5 zur Basis 2!

b) Diskrete Logarithmen lassen sich modulo einer beliebigen natürlichen Zahl definieren. Warum verwendet man in der Kryptographie nur Primzahlen?

c) Welchen Vorteil hat es, wenn diese Primzahl von der Form $2q + 1$ ist mit einer weiteren Primzahl q?

d) Wie funktioniert das Verschlüsselungsverfahren von ELGAMAL?

e) Welche Angriffsmöglichkeiten hat ein Gegner, wenn der Sender einer Nachricht für jeden Block dieselbe Zufallszahl wählt?

Aufgabe 6: (*8 Punkte*)

a) Zeigen Sie: Ist $p \equiv 3 \bmod 4$ eine Primzahl und gibt es zu $a \in \mathbb{Z}$ eine ganze Zahl x mit $x^2 \equiv a \bmod p$, so ist auch $y = a^{(p+1)/4}$ eine Lösung dieser Kongruenz.

b) Zeigen Sie, daß $y^2 \equiv -a \bmod p$ ist, falls die Kongruenz $x^2 \equiv a \bmod p$ keine Lösung hat!

c) Bestimmen Sie für $N = 8509 = 67 \cdot 127$ alle $x \in \mathbb{Z}$, die die Kongruenz $x^2 \equiv 1 \bmod N$ erfüllen!

Aufgabe 7: (*6 Punkte*)

a) Welche Möglichkeiten hat ein Gegner, wenn er im ECB-Modus verschlüsselten Chiffretext abfängt?

b) Bei welchem Operationsmodus von Rijndael läßt sich der Chiffreblock zum letzten Block der Nachricht als Hashwert verwenden? Welche Schlüssel- und welche Blocklängen muß man mindestens verwenden, damit dieser Hashwert kryptographisch sicher ist?

Aufgabe 8: (*8 Punkte*)

a) Lösen Sie im Körper F_{1021} die Gleichung $17x = 50$!

b) Berechnen Sie dort das Element 2^{50} !

c) Welche Ordnung hat die Zwei im Körper $\mathbb{F}_{23}$?

Abgabe bis zum Dienstag, dem 4. Juni 2013, um 18^{00} Uhr

• • • **Steht Ihr Name auf jedem Blatt?** • • •