Wolfgang K. Seiler
Tel. 2515

A5, C201

4. Februar 2017

Modulklausur Kryptologie

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

Aufgabe 1: (*10 Punkte*)

a) Was ist der Unterschied zwischen einer Blockchiffre und einer Stromchiffre?

b) Eine gegebene Blockchiffre F arbeitet mit Klartextblöcken einer Länge von n Bit, Chiffretextblöcken einer Länge von m Bit und Schlüsseln der Länge s Bit. Mathematisch gesehen ist F eine Abbildung zwischen zwei Mengen M und N. Welche sind das?

c) Warum muß $m \geq n$ sein?

d) Welche Relation müssen m, n und s mindestens erfüllen, wenn die Blockchiffre F perfekte Sicherheit bieten soll?

e) Warum fordert Kerckhoff, daß die Sicherheit des Verfahrens nur vom Schlüssel abhängen darf?

Aufgabe 2: (*8 Punkte*)

In einem Netzwerk, das das Verfahren von ElGamal zur Verschlüsselung benutzt, seien die Primzahl p und eine natürliche Zahl a zwischen zwei und $p-1$ festgelegt. Der geheime Schlüssel von Teilnehmer A sei x, der von Teilnehmer B sei y

a) Welches sind die öffentlichen Schlüssel von A und B ?

b) Wie geht A vor, wenn er eine Nachricht $m \in \mathbb{N}$ mit $m < p$ verschlüsselt an B schicken möchte?

c) Wie kann B die Nachricht entschlüsseln?

d) In einem speziellen System habe die Primzahl p die Länge 3001 Bit. A möchte eine Nachricht von 30 000 Byte an B schicken. Wie viele Blöcke welcher Länge muß er dazu übertragen?

e) Das Verfahren von ElGamal beruht bekanntlich auf der gleichen Idee wie der Schlüsselaustausch nach Diffie und Hellman. Welche Bedingung muß erfüllt sein, daß es nicht auch durch eine *man in the middle attack* angegriffen werden kann?

Aufgabe 3: (*8 Punkte*)

a) p sei eine natürliche Zahl, und $q_1, \ldots, q_r$ seien die Primteiler von $p-1$. Zeigen Sie: Falls es eine natürliche Zahl a gibt, so daß $a^{p-1} \equiv 1 \bmod p$, aber $a^{(p-1)/q_i} \not\equiv 1 \bmod p$ für alle $i = 1, \ldots, r$, so ist p eine Primzahl.

b) Wie viele Zahlen $1 \leq a < p$ mit dieser Eigenschaft gibt es dann?

c) Umgekehrt sei p als Primzahl vorausgesetzt, und $q_1, \ldots, q_r$ seien wieder die Primteiler von $p-1$. Gibt es dann stets eine natürliche Zahl a, so daß $a^{p-1} \equiv 1 \bmod p$, aber $a^{(p-1)/q_i} \not\equiv 1 \bmod p$ für $i = 1, \ldots, r$?

• • • **Bitte wenden!** • • •

Aufgabe 4: (*7 Punkte*)

a) Zerlegen Sie die Zahl $N = 51067$ mit dem Verfahren von FERMAT in ihre Primfaktoren! Dabei soll bewiesen werden, daß die gefundenen Faktoren allesamt prim sind.

b) Welches ist der kleinste Exponent e, den man für ein RSA-Verfahren mit diesem Modul N verwenden kann?

c) Bestimmen Sie für diesen öffentlichen Exponenten einen möglichst kleinen privaten Exponenten $d \in \mathbb{N}$!

d) Der Inhaber dieses privaten Schlüssels möchte einen Hashwert $h < N$ unterschreiben. Geben Sie eine realistische obere Schranke an für die Anzahl der Multiplikationen (einschließlich Quadrierungen) modulo N, die er zur Berechnung seiner Unterschrift benötigt!

Aufgabe 5: (*7 Punkte*)

Die Zahl $a = 13579$ hat modulo $N = 37669$ die folgenden Potenzen: $a^2 \equiv 37155 \bmod N$, $a^3 \equiv 26828 \bmod N$, $a^4 \equiv 513 \bmod N$, $a^5 \equiv 34931 \bmod N$ und $a^6 \equiv 1 \bmod N$.

a) Berechnen Sie $a^{1000} \bmod N$ und $a^{-1000} \bmod N$!

b) Ist die Ordnung von a ein Teiler von $N - 1$?

c) Können Sie, nur anhand der obigen Zahlen, entscheiden, ob N eine Primzahl ist? Beweisen Sie, daß N prim ist, oder schreiben Sie N als ein nichttriviales Produkt!

Aufgabe 6: (*8 Punkte*)

a) Diskutieren Sie Aufwand und Sicherheit des folgenden Verfahrens, das aus DES eine Blockchiffre für Blöcke von 128 Bit macht: Die Blöcke werden identifiziert mit Zahlen z zwischen Null und $2^{128} - 1$, die in der Form $z = 2^{64}x + y$ geschrieben werden mit $0 \le x, y < 2^{64}$. Das Ergebnis der Verschlüsselung ist $c = 2^{64} \cdot \mathrm{DES}(x, s_1) + \mathrm{DES}(y, s_2)$, wobei s_1 und s_2 zwei verschiedene DES-Schlüssel sind.

b) Um das Verfahren aus *a)* sicherer zu machen, soll noch zusätzlich eine Permutation π aus $\mathfrak{S}_{128}$ auf die Blöcke angewendet werden, die einen Block $(b_1, \ldots, b_{128})$ transformiert in $(b_1, b_3, \ldots, b_{127}, b_2, b_4, \ldots, b_{128})$. Sollte π vor oder nach der Anwendung der beiden DES-Funktionen angewandt werden, und wie erhöht sich dadurch die Sicherheit?

c) Vergleichen Sie die Sicherheit des Verfahrens aus *a)* gegen differentielle Kryptanalyse mit der von AES!

d) Geben Sie einen Operationsmodus an, mit dem auch Nachrichten, deren Länge kein Vielfaches der Blocklänge ist, so verschlüsselt werden können, daß der Chiffretext nicht länger wird als der Klartext!

Aufgabe 7: (*8 Punkte*)

a) Die Zahl $5^{11} + 1$ ist durch 23 teilbar. Folgern Sie daraus, daß fünf eine primitive Wurzel modulo 23 ist!

b) Bestimmen Sie den diskreten Logarithmus modulo 23 von 3 zur Basis 5 nach der *baby step – giant step* Methode!

c) Das Polynom $X^3 + X + 1$ ist irreduzibel über dem Körper $\mathbb{F}_2$; der Körper $\mathbb{F}_8$ kann also realisiert werden als dreidimensionaler $\mathbb{F}_2$-Vektorraum mit Basis $1, \alpha, \alpha^2$, wobei α der Gleichung $\alpha^3 + \alpha + 1 = 0$ genügt. Stellen Sie $(\alpha + 1)^4 \in \mathbb{F}_8$ in dieser Basis dar!

Aufgabe 8: (*4 Punkte*)

a) Welche Anforderungen müssen an ein kryptographisch sicheres Hash-Verfahren gestellt werden?

b) Wie können Sie mit Hilfe von RIJNDAEL ein kryptographisch sicheres Hashverfahren definieren? Welche Bedingungen müssen dabei die Block- und die Schlüssellänge erfüllen?

Abgabe bis zum Samstag, dem 4. Februar 2017, um 10^{30} Uhr

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