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?

Lösung: Die Angriffe gegen klassische monoalphabetische Substitutionen nutzen die Häufigkeitsverteilungen der Buchstaben und Buchstabenpaare im Chiffretext aus. Bei einem Alphabet aus 2^{128} Blöcken ist es, wenn wir davon ausgehen, daß 2^{128} Rechenoperationen jenseits der Möglichkeiten unserer Gegner liegen, nicht möglich, entsprechende Statistiken aufzustellen.

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?

Lösung: Es hat höchstens dann einen Vorteil, wenn man ein existentes Programm oder Hardwaremodul zur Berechnung von AES mit Schlüssellänge 128 weiter benutzen will, hat aber den Nachteil eines erheblich größeren Rechenaufwands 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!

Lösung: Bei diesem Angriff muß er zu einem bekannten Paar aus Klartext x und Chiffretext y alle 2^{128} möglichen Werte von $\mathrm{AES}_{k_2}(x)$ sowie alle 2^{128} möglichen Werte von $\mathrm{AES}_{k_1}^{-1}(y)$ berechnen und nach einem Wert suchen, der in beiden Listen vorkommt. Dazu muß eine der Listen gespeichert werden, er braucht also auch noch Speicherplatz für 2^{128} Blöcke der Länge 128 Bit oder 16 Byte. Insgesamt braucht er also mindestens 2^{132} Byte Speicherplatz; das sind 2^{122} Kilobyte, 2^{112} Megabyte, 2^{102} Gigabyte, 2^{92} Terabyte, also jedenfalls sehr viel. Bei DES reichen 2^{56} Blöcke von je acht Byte, also $2^{16} = 65536$ Terabyte, was zwar auch viel ist, aber mit hinreichend großen Speicherbänken wohl bereits heute realisiert werden kann.

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

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

Verwenden Sie zum Beweis nur den kleinen Satz von FERMAT!

Lösung: Nach dem kleinen Satz von FERMAT ist $a^{p-1} \equiv 1 \bmod p$ für alle zu p teilerfremden Zahlen $a \in \mathbb{Z}$. Damit ist für diese a auch $a^{m(p-1)} \equiv 1^m = 1 \bmod p$ für alle ganzen Zahlen m und somit $a^{m(p-1)+1} \equiv a \bmod p$. Letztere Beziehung gilt bei positivem Exponenten auch, wenn a ein Vielfaches von p ist, denn dann sind beide Seiten kongruent Null modulo p. Somit ist

$$a^{m(p-1)+1} \equiv a \bmod p \quad \text{für alle } a \in \mathbb{Z} \text{ und } m \in \mathbb{N}_0.$$

Entsprechend folgt, daß

$$a^{n(q-1)+1} \equiv a \bmod q \quad \text{für alle } a \in \mathbb{Z} \text{ und } n \in \mathbb{N}_0.$$

Für den privaten Exponenten d gibt es eine natürliche Zahl k, so daß $de-k(p-1)(q-1) = 1$ ist, d.h.

$$de = k(p-1)(q-1) + 1\,.$$

Nach den beiden obigen Gleichungen mit $m = k(q-1)$ und $n = k(p-1)$ folgt, daß $a^{de} \equiv a \bmod p$ und $a^{de} \equiv a \bmod q$ für alle $a \in \mathbb{Z}$. Da p und q zwei verschiedene Primzahlen sind, ist dann auch $a^{de} \equiv a \bmod N = pq$.

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?

Lösung: In diesem Fall würde der gleiche Ansatz wie bei *a)* zeigen, daß für alle $a \in \mathbb{Z}$ gilt $a^{k(p-1)(q-1)(r-1)+1} \equiv a \bmod N$; somit müßte man ein e nehmen, das teilerfremd ist zu $(p-1)(q-1)(r-1)$, und dann via EUKLID ein d finden, so daß für ein geeignetes $k \in \mathbb{N}$ gilt $de - k(p-1)(q-1)(r-1) = 1$.

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

Lösung: Ein kleiner Vorteil bestünde darin, daß man kleinere Primzahlen suchen müßte; allerdings bräuchte man natürlich drei statt zwei. Ein großer Nachteil wäre, daß N kleinere Faktoren hätte, so daß der Aufwand zur Faktorisierung von N kleiner würde.

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

Lösung: Wegen $de - k(p-1)(q-1)(r-1) = 1$ ist

$$\frac{k}{d} \approx \frac{e}{(p-1)(q-1)(r-1)} \approx \frac{e}{pqr} = \frac{e}{N}\,;$$

für kleine Werte von d ist also der Bruch e/N recht gut approximiert durch den Bruch k/d, der einen viel kleineren Nenner hat. Falls die Approximation hinreichend gut ist ($\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$), muß k/d eine Konvergente der Kettenbruchentwicklung von e/N sein. Man berechnet daher nacheinander diese Konvergenten und probiert durch Testen mit einer zufälligen Basis a, ob der Nenner als privater Exponent d in Frage kommt, ob also $a^{de} \equiv a \bmod N$ ist.

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 $a \in \mathbb{Z}$!

Lösung: Ein solches d läßt sich beispielsweise konstruieren, indem man den erweiterten EUKLIDischen Algorithmus anwendet auf e und $\varphi(N) = (p-1)(q-1) = 66 \cdot 126 = 8316$:

$$\begin{aligned} 8316 : 17 = 489 \quad \text{Rest } 3 &\Longrightarrow 3 = 8316 - 489 \cdot 17 \\ 17 : 3 = 5 \quad \text{Rest } 2 &\Longrightarrow 2 = 17 - 5 \cdot 3 = 2446 \cdot 17 - 5 \cdot 8316 \\ 3 : 2 = 1 \quad \text{Rest } 1 &\Longrightarrow 1 = 3 - 2 = 6 \cdot 8316 - 2935 \cdot 17 \end{aligned}$$

Dies liefert ein negatives d; um ein positives zu bekommen, müssen wir noch $\varphi(N)$ addieren und erhalten $d = 8316 - 2935 = 5381$.

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

Lösung: Statt mit $\varphi(N) = (p-1)(q-1)$ hätten wir auch mit dem kgV der beiden Zahlen $p-1 = 66 = 2 \cdot 3 \cdot 11$ und $q-1126 = 2 \cdot 3^2 \cdot 7$ arbeiten können, also mit $2 \cdot 3^2 \cdot 7 \cdot 11 = 1386$. Dann hätten wir ein positives $d \leq 1386 \leq 1500$ gefunden.

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?

Lösung: Wir suchen positive ganze Zahlen d und k, für die $1 = de - k\varphi(N)$ ist. Da wir hierzu beliebige Vielfache der Gleichung $\varphi(N) \cdot e - e\varphi(N) = 0$ addieren können, kann dabei $1 \leq k < e$ erreicht werden. Für jedes Lösungspaar (d, k) ist

$$d = \frac{1 + k\varphi(N)}{e} = \frac{1 + k(p-1)(q-1)}{e};$$

wenn für k nur wenige Werte in Frage kommen, kann man durchprobieren, für welchen davon dieser Ausdruck ganzzahlig ist

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 $\varphi(N) = (p-1)(q-1)$!

Lösung: $1 = de - k\varphi(N)$ läßt sich auch auflösen zu

$$\varphi(N) = \frac{de - 1}{k} = \frac{21\,535\,400}{k}$$

mit $1 \leq k < 3$. Da $\varphi(N) < N$ ist, kommt nur $k = 2$ in Frage, d.h. $\varphi(N) = 10\,767\,700$.

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

Lösung: $\varphi(N) = (p-1)(q-1) = pq - p - q + 1 = N + 1 - (p+q) = 10\,767\,700$; daher ist $p + q = 10\,774\,633 + 1 - 10\,767\,700 = 6\,934$. Somit ist

$$p + q = 6\,934 \quad \text{und} \quad p \cdot q = 10\,774\,633;$$

p und q sind daher die Lösungen der quadratischen Gleichung $x^2 - 6\,934x + 10\,774\,633$. Jede Methode zur Lösung einer quadratischen Gleichung führt auf die beiden Nullstellen $p = 2351$ und $q = 4583$.

Aufgabe 5: (*10 Punkte*)

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

Lösung: Das geht am schnellsten durch Probieren: In $\mathbb{F}_{19}$ ist

$$\begin{gathered} 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16, \quad 2^5 = 32 = 13, \quad 2^6 = 26 = 7, \\ 2^7 = 14, \quad 2^8 = 28 = 9, \quad 2^9 = 18 = -1, \quad 2^{10} = -2, \quad 2^{11} = -4, \\ 2^{12} = -8, \quad 2^{13} = -16 = 3, \quad 2^{14} = 6, \quad 2^{15} = 12, \quad 2^{16} = 24 = 5\,; \end{gathered}$$

der gesuchte Logarithmus ist also sechszehn.

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

Lösung: Nach dem chinesischen Restesatz läßt sich die Berechnung eines diskreten Logarithmus modulo einem Produkt teilerfremder Zahlen zurückführen auf die beiden einfacheren Probleme der Berechnung der entsprechenden Logarithmen modulo der Faktoren. Nach dem Verfahren von Pohlig und Hellman läßt sich die Berechnung eines diskreten Logarithmus modulo einer Primzahlpotenz zurückführen auf Berechnungen modulo der Basis. Daher kann der Logarithmus modulo einer zusammengesetzten Zahl immer einfacher berechnet werden als der modulo einer Primzahl gleicher Größenordnung.

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

Lösung: Die multiplikative Gruppe von $\mathbb{F}_p^\times$ hat die Ordnung $p - 1$; falls $p - 1 = 2q$ ist mit einer Primzahl q, kann die Ordnung eines Elements also nur $1, 2, q$ oder $2q$ sein. Um zu testen, ob ein Element $g \in \mathbb{F}_p^\times$ primitive Wurzel ist (was für Kryptoverfahren auf der Basis diskreter Logarithmen stets nützlich ist), muß daher nur überprüft werden, ob g, g^2 und g^q alle drei von Eins verschieden sind. Auch wenn man sich die Berechnung von g^q ersparen will, kann man schon aus der Ungleichung $g^2 \neq 1$ schließen, daß g mindestens die Ordnung q hat, was für kryptographische Anwendungen diskreter Logarithmen meist ausreicht.

d) Wie funktioniert das Verschlüsselungsverfahren von ElGamal?

Lösung: Der Empfänger einer Nachricht wählt eine Primzahl p (nach derzeitigen Sicherheitsstandards mindestens 2048 Bit) sowie eine Zahl $a \in \mathbb{F}_p^\times$ mit möglichst hoher Ordnung; außerdem wählt er einen geheimen Schlüssel x und berechnet a^x in $\mathbb{F}_p$. Er veröffentlicht p, a und y.
Zu jedem Nachrichtenblock m an ihn wählt der Sender eine Zufallszahl c und schickt die beiden Zahlen $u = a^c \bmod p$ und $v = y^c m \bmod p$ an den Empfänger. Dieser kann

$$y^c = \left(a^x\right)^c = a^{cx} = u^x$$

und damit auch das Inverse davon bestimmen, so daß er m aus v berechnen kann.

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

Lösung: Er weiß dann einerseits, welche Klartextblöcke gleich sein (das werden im Allgemeinen nur wenige sein, wenn überhaupt), und er kann die Quotienten m_i/m_j der Nachrichtenblöcke ermitteln. Sofern er nur einen Block errät (womit man immer rechnen muß), kennt er also die gesamte Nachricht.

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.

Lösung: In $\mathbb{F}_p$ ist $y^2 = a^{(p+1)/2} = x^{p+1} = x^p \cdot x = x^2 = a$ nach dem kleinen Satz von FERMAT.

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

Lösung: In $\mathbb{F}_p$ ist $y^2 = a^{(p+1)/2}$, also $y^4 = a^{p+1} = a^2$. Somit $y^2 = \pm a$. Da der Fall $y^2 = a$ ausgeschlossen ist, muß $y^2 = -a$ sein.

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

Lösung: Die beiden offensichtlichen Lösungen sind $x \equiv \pm 1 \bmod N$. In $\mathbb{F}_{67}$ und in $\mathbb{F}_{127}$ hat die Gleichung $x^2 = 1$ nur die beiden Lösungen $x = \pm 1$; Lösungen modulo N bekommen wir auch, wenn wir x finden mit $x \equiv 1 \bmod 67$ und $x \equiv -1 \bmod 127$ oder umgekehrt. Diese liefert uns der chinesische Restesatz, für dessen Anwendung wir zunächst die Eins aus 67 und 127 kombinieren müssen:

$$\begin{aligned}
127 : 67 = 1 \quad \text{Rest } 60 &\Longrightarrow 60 = 127 - 67 \\
67 : 60 = 1 \quad \text{Rest } 7 &\Longrightarrow 7 = 2 \cdot 67 - 127 \\
60 : 7 = 8 \quad \text{Rest } 4 &\Longrightarrow 4 = 60 - 8 \cdot 7 = 9 \cdot 127 - 17 \cdot 67 \\
7 : 4 = 1 \quad \text{Rest } 3 &\Longrightarrow 3 = 7 - 4 = 19 \cdot 67 - 10 \cdot 127 \\
4 : 3 = 1 \quad \text{Rest } 1 &\Longrightarrow 1 = 4 - 3 = 19 \cdot 127 - 36 \cdot 67
\end{aligned}$$

Also ist $1 + 36 \cdot 67 = 19 \cdot 127 = 2413 \equiv \begin{cases} 1 & \bmod 67 \\ 0 & \bmod 127 \end{cases}$
und $1 - 19 \cdot 127 = -36 \cdot 67 = -2412 \equiv \begin{cases} 0 & \bmod 67 \\ 1 & \bmod 127 \end{cases}$, wobei wir das letztere Element von $\mathbb{Z}/N$ auch als 6097 schreiben können.
Die Zahl $x = 2413 \cdot 1 - 2412 \cdot (-1) = 4825$ ist somit kongruent eins modulo 67 und kongruent -1 modulo 127; ihr Quadrat ist kongruent eins modulo beider Primzahlen und damit modulo N. Entsprechend ist auch ihr Negatives eine Quadratwurzel der Eins. Somit ist $x^2 \equiv 1 \bmod N$ genau dann, wenn $x \equiv \pm 1 \bmod N$ oder $x \equiv \pm 4825 \bmod N$.

Aufgabe 7: (*6 Punkte*)

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

Lösung: Er kann zum einen feststellen, wann zwei Chiffreblöcke zu gleichem Klartext gehören, zum andern kann er möglicherweise Blöcke umstellen, ohne daß dies vom Empfänger bemerkt wird.

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?

Lösung: Das funktioniert beim Cipher Block Chaining, da dort jeder Chiffreblock von allen vorangegangenen Klartextblöcken abhängt. Um 128 Bit Sicherheitsniveau zu erreichen, muß man hier allerdings mit einer Blocklänge von mindestens 256 Bit arbeiten. Die Schlüssellänge ist gleichgültig, da der Schlüssel beim Hashen keine Geheimhaltungsfunktion hat, sondern zur Überprüfung des Hashwerts ohnehin bekannt gemacht werden muß.

Aufgabe 8: *(8 Punkte)*

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

Lösung: Dazu muß zunächst das multiplikative Inverse von 17 bestimmt werden, d.h. wir müssen den ggT 1 von 17 und 1021 als Linearkoombination dieser beiden Zahlen darstellen.

$$1021 : 17 = 60 \quad \text{Rest } 1 \Longrightarrow 1 = 1021 - 60 \cdot 17 .$$

Somit ist $17^{-1} = -60$ in $\mathbb{F}_{1021}$. Multiplizieren wir die Gleichung damit, erhalten wir

$$x = -60 \cdot 17x = -60 \cdot 50 = -3000 = 63 .$$

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

Lösung: $2^{10} = 1024$ ist in $\mathbb{F}_{1021}$ gleich drei; somit ist $2^{50} = 3^5 = 243$.

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

Lösung: $\mathbb{F}_{23}^{\times}$ hat 22 Elemente; die Ordnung eines Elements ist nach LAGRANGE ein Teiler davon, also $1, 2, 11$ oder 22. Eins ist sie nicht und, da $2^2 = 4$ ist, auch nicht zwei. $2^{11} = 2048$ und $2048 : 23 = 89$ Rest 1. Also hat die Zwei Ordnung elf.