Wolfgang K. Seiler
Tel. 2515

B6,26, A4.18

19. Dezember 2019

Modulklausur Kryptologie

• • • **Schreiben Sie bitte auf jedes Blatt Ihren Namen!** • • •
• • • **Die Aufgaben müssen *nicht* in der angegebenen Reihenfolge** • • •
• • • **bearbeitet werden; konzentrieren sie sich zunächst** • • •
• • • **auf das, womit sie schnell Punkte holen können!** • • •

Aufgabe 1: (*8 Punkte*)

a) Warum muß ein gutes Verschlüsselungsverfahren auch gegen Angriffe mit bekanntem Klartext sicher sein?

b) Wie sieht es beim Vigenère-Verfahren mit dieser Sicherheit aus?

c) Wie könnte ein Angriff mit frei wählbarem Chiffretext auf ein Kryptoverfahren ablaufen?

d) Was besagt Kerckhoffs Prinzip, und warum sollte man es beachten?

e) Worin unterscheiden sich symmetrische und asymmetrische Kryptoverfahren, und was sind ihre jeweiligen Vor- und Nachteile?

f) Warum sollten symmetrische Blockchiffren wie AES oder DES nie im ECB-Modus verwendet werden, während es für asymmetrische Blockchiffren wie RSA mit PKCS#1 keine entsprechende Empfehlung gibt?

Aufgabe 2: (*10 Punkte*)

a) Wie funktioniert der Schlüsselaustausch nach Diffie-Hellman?

b) Man könnte den so vereinbarten Schüssel direkt benutzen, indem man die zu übermittelnde Nachricht in Blöcke zerlegt, deren numerische Entsprechungen kleiner sind als die beim Schlüsselaustausch benutzte Primzahl p, und diese Blöcke dann modulo p mit dem vereinbarten Schlüssel multiplizieren. Welches zusätzliche Sicherheitsproblem tritt dabei auf?

c) Wie kann man die Idee des Schlüsselaustauschs nach Diffie-Hellman so modifizieren, daß ein sicheres asymmetrisches Kryptosystem entsteht?

d) Das Verfahren von Diffie und Hellman würde auch funktionieren, wenn p keine Primzahl wäre. Warum wählt man trotzdem eine Primzahl?

Aufgabe 3: (*10 Punkte*)

a) Ein Demo-RSA-System benutzt die beiden Primzahlen $p = 401$ und $q = 601$. Welche einstelligen Zahlen e kommen als öffentliche Exponenten in Frage?

b) Bestimmen Sie für einen dieser Exponenten einen passenden privaten Exponenten!

c) Verschlüsseln Sie die der Zahl zwanzig entsprechende Nachricht!

d) Wie viele modulare Multiplikationen brauchen Sie, um die Nachricht 123456 zu unterschreiben?

• • • **Bitte wenden!** • • •

Aufgabe 4: (*8 Punkte*)

a) Für eine r-Primzahlen-Variante von RSA könnte man als Modul N das Produkt von r paarweise verschiedenen großen Primzahlen $p_1, \ldots, p_r$ nehmen und dazu einen Exponenten e wählen, der teilerfremd ist zu jeder der r Zahlen $p_i - 1$ für $i = 1, \ldots, r$. Zeigen Sie: Ist $\lambda(N)$ das kgV der $p_i - 1$, so gibt es $d, k \in \mathbb{N}$ mit $ed - k\lambda(N) = 1$, und für alle $m \in \mathbb{Z}$ ist $\left(m^e\right)^d \equiv m \bmod N$.

b) Könnte man statt mit $\lambda(N)$ auch mit einem beliebigen gemeinsamen Vielfachen der $p_i - 1$ arbeiten?

c) Warum verwendet man in der Kryptographie nur die Version mit $r = 2$?

Aufgabe 5: (*10 Punkte*)

a) Zeigen Sie, daß $p = 113$ eine Primzahl ist!

b) Modulo $p = 113$ gelten die Kongruenzen $3^8 \equiv 7 \bmod p$ und $2^{14} \equiv 3^{56} \equiv 112 \bmod p$ (die Sie *nicht* nachrechnen müssen). Bestimmen Sie die Ordnungen der Elemente zwei, drei und sechs in $(\mathbb{Z}/113)^\times$.

c) Bestimmen Sie den diskreten Logarithmus modulo p von zwölf zur Basis drei!

Aufgabe 6: (*8 Punkte*)

Ein Softwarehersteller schützt seine über das Internet vertriebenen Programme mit einem Hashcode. Damit dieser bequem von seiner Webseite abgeschrieben werden kann, berechnet er zwar jeweils den SHA-256-Hashwert, teilt diesen dann aber auf in sechzehn Blöcke à sechzehn Bit, und addiert diese sechzehn Zahlen als Vektoren aus $\mathbb{F}_2^{16}$ zur Prüfsumme.

a) Wie groß ist der zu erwartende Aufwand für einen externen Gegner, der eine verfälschte Version des Programms in Umlauf bringen will, die zur gleichen Prüfsumme führt, und wie würde er vorgehen?

b) Was ändert sich, wenn der für das Programm und seine Veröffentlichung zuständige Mitarbeiter zusätzlich noch eine verfälschte Version in Umlauf bringen will?

c) Was ändert sich jeweils, wenn die sechzehn Blöcke nicht als $\mathbb{F}_2^{16}$-Vektoren, sondern als ganze Zahlen oder als Zweiervektoren über $\mathbb{F}_{256}$ addiert werden?

Aufgabe 7: (*6 Punkte*)

a) Zeigen Sie, daß die S-Box von AES resistent ist gegen differentielle Kryptanalyse!

b) Folgt daraus auch, daß AES als ganzes dagegen resistent ist?