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?

Lösung: In vielen Fällen weiß ein Gegner irgendetwas über den Inhalt der Nachricht oder kann es zumindest erraten. Beispiele sind Briefköpfe, Grußformeln am Ende oder standardisierte Formate wie etwa bei Transaktionen im Bankensystem.

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

Lösung: Schlecht: Sobald zusammenhängender Klartext bekannt ist mit einer Länge, die größer ist als die des Schlüsselworts, kann die ganze Nachricht entziffert werden. Auch bei weniger Klartext erhält ein Kryptanalytiker so viele Hinweise, daß dieses ohnehin unsichere Verfahren noch deutlich einfacher zu knacken ist.

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

Lösung: Der Angreifer könnte ein Entschlüsselungsgerät unbemerkt entwenden und nach der Entschlüsselung wieder unbemerkt zurückgeben.

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

Lösung: Nach Kerckhoffs Prinzip muß schon die Geheimhaltung des Schlüssels ausreichen, um die Sicherheit eines Kryptoverfahrens zu garantieren. Da es bei typischen Anwendungen der Kryptographie unrealistisch ist auf die Geheimhaltung des Verfahrens zu vertrauen, sollte man dies auch heute noch unbedingt beachten.

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

Lösung: Bei symmetrischen Kryptoverfahren vereinbaren zwei Korrespondenten einen Schlüssel, den niemand außer ihnen kennen darf. Bei asymmetrischen Kryptoverfahren wählt jeder Korrespondent ein Paar aus einem öffentlichen Schlüssel, den er allgemein bekannt macht, und einem privaten Schlüssel, den nur er kennen darf. Der öffentliche Schlüssel reicht aus, um Nachrichten zu *ver*schlüsseln; eine *Ent*schlüsselung ist aber nur bei Kenntnis des privaten Schlüssels möglich.

Symmetrische Kryptoverfahren haben den Vorteil, daß es sehr schnelle und trotzdem sichere solche Verfahren gibt; ihr Hauptnachteil ist, daß bei alleiniger Verwendung eines solchen Verfahrens irgendwie ein Schlüssel zwischen den beiden Korrespondenten vereinbart werden muß. Das kann nur bei einem persönlichen Treffen oder über einen vertrauenswürdigen Boten geschehen, was beispielsweise beim e-commerce völlig unrealistisch wäre. Außerdem braucht man in einem Netzwerk aus n Personen $\binom{n}{2} = \frac{1}{2}n(n-1)$ Schlüssel, damit jeder mit jedem sicher kommunizieren kann.

Der Hauptvorteil asymmetrischer Kryptoverfahren besteht darin, daß nach Bekanntgabe eines öffentlichen Schlüssels jedermann sicher mit dessen Inhaber kommunizieren kann. Sie haben allerdings den Nachteil, daß alle bekannten asymmetrischen Verfahren deutlich langsamer als symmetrische Verfahren mit gleichem Sicherheitsniveau sind.

In der Praxis benutzt man daher asymmetrische Verfahren oft nur zum Schlüsselaustausch für ein symmetrisches Verfahren, mit dem dann die eigentliche Kommunikation verschlüsselt wird. Diese hybride Vorgehensweise kombiniert die Vorteile beider Klassen von Verschlüsselungsverfahren.

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?

Lösung: Beim ECB-Modus werden identische Blöcke gleich verschlüsselt, so daß ein Angreifer diese identifizieren kann und dadurch zumindest etwas Information gewinnt. Bei Angriffen mit bekanntem Klartext oder auch bei Nachrichten mit bekannter Struktur, wie sie etwa im elektronischen Zahlungsverkehr üblich sind, erleichtert es zudem die Konstruktion gefälschter Nachrichten.

Bei den gängigen asymmetrischen Verfahren sind beide Probleme wegen der deutlich größeren Blocklänge (mindestens 2000 und bald mindestens 3000 bei RSA und Elgamal gegenüber 128 bei AES und 64 bei DES) deutlich kleiner, insbesondere da in der Praxis innerhalb einer Kommunikation meist nur sehr wenige asymmetrisch verschlüsselte Blöcke übertragen werden. Außerdem sorgen die bei PKCS#1 vorgeschriebenen Zufallsbits in jedem Block dafür, daß bei sachgemäßer Anwendung (d.h. neuen Zufallsbits für jeden Block und auch für jeden Empfänger) identische Blöcke zu völlig verschiedenen Verschlüsselungen führen.

Aufgabe 2: (*10 Punkte*)

a) Wie funktioniert der Schlüsselaustausch nach Diffie-Hellman?

Lösung: Zwei Korrespondenten A und B wollen über eine unsichere Leitung einen gemeinsamen Schlüssel vereinbaren. Dazu einigen sie sich (über diese Leitung) auf eine hinreichend große Primzahl p und eine Zahl a zwischen 2 und $p-2$, die modulo p eine möglichst große Ordnung hat. Dann wählt A eine geheime Zahl $x < p-1$ und schickt $u = a^x \bmod p$ an B. Dieser wählt eine geheime Zahl $y < p-1$ und schickt $v = a^y \bmod p$ an A. Der geheime Schlüssel wird nach einem zu vereinbarenden Verfahren bestimmt aus $a^{xy} \bmod p = u^y \bmod p = v^x \bmod p$, was sowohl A als auch B problemlos berechnen kann. Ein Angreifer, der nur p, a, u, v kennt, müßte aber (nach heutigem Kenntnisstand der publizierten Mathematik) daraus mindestens eine der Zahlen x oder y bestimmen, d.h. ein diskretes Logarithmenproblem lösen, was für hinreichend große p (derzeit mindestens 2000, besser 3000 Bit) mit den öffentlich bekannten Verfahren nicht praktikabel ist.

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?

Lösung: Sobald ein Gegner einen der Blöcke errät, kann er den Schlüssel berechnen und damit die gesamte Kommunikation entschlüsseln.

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

Lösung: Die wohl populärste Lösung ist das Verfahren von Elgamal: Ein Teilnehmer A wählt p, a, x wie bei Diffie-Hellman und veröffentlicht p, a und $u = a^x \bmod p$. Ein Teilnehmer B, der ihm eine Nachricht sicher übermitteln möchte, wählt für jeden Block m

eine neue Zufallszahl y und schickt das Paar aus $v = a^y \bmod p$ und $c = mu^y \bmod p$ an A. Dieser kann $u^y \equiv v^x \bmod p$ berechnen und somit m aus c rekonstruieren.

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

Lösung: Ist $p = uv$ das Produkt zweier teilerfremder Faktoren, läßt sich das diskrete Logarithmenproblem modulo p über den chinesischen Restesatz zurückführen auf die entsprechenden Probleme modulo u und v, deren Lösungen deutlich einfacher sind (und eventuell durch entsprechende Zerlegung von u und/oder v noch weiter vereinfacht werden kann).

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?

Lösung: e muß teilerfremd sein zu $p-1 = 400 = 2^4 \cdot 5^2$ und zu $q-1 = 600 = 2^3 \cdot 3 \cdot 5^2$, also zu 2, 3 und 5. Da $e = 1$ offensichtlich zu keiner Verschlüsselung führt, kommt also nur $e = 7$ in Frage.

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

Lösung: Das kleinste gemeinsame Vielfache von $p-1$ und $q-1$ ist $2^4 \cdot 3 \cdot 5^2 = 1200$. Für $e = 7$ berechnet sich der geheime Exponent durch Anwendung des erweiterten EUKLIDischen Algorithmus auf 1200 und 7:

$$\begin{aligned} 1200 : 7 = 171 \text{ Rest } 3 &\Longrightarrow 3 = 1200 - 7 \cdot 171 \\ 7 : 3 = 2 \text{ Rest } 1 &\Longrightarrow 1 = 7 - 2 \cdot (1200 - 7 \cdot 171) = 343 \cdot 7 - 2 \cdot 1200 \end{aligned}$$

Somit ist 343 ein möglicher privater Exponent.

c) Verschlüsseln Sie die der Zahl zwanzig entsprechende Nachricht!

Lösung: $N = pq = 241\,001$; die Verschlüsselung ist $20^7 \bmod N$. Bei diesem kleinen Exponenten lohnt sich kein binäres Verfahren; $20^7 = 2^7 \cdot 10^7 = 1\,280\,000\,000$ ergibt bei Division durch N den Quotienten 5 311 mit Rest 43 689; dieser Rest ist gleich der Verschlüsselung.

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

Lösung: Das hängt natürlich vom gewählten Exponenten d ab. $d = 343$ läßt sich schreiben als $2^8 + 2^6 + 2^4 + 2^2 + 2 + 1$; also ist $m^{343} = m^{256} \cdot m^{64} \cdot m^{16} \cdot m^4 \cdot m^2 \cdot m$. Zur Berechnung der $m^{2^i} \bmod N$ sind acht modulare Multiplikationen (Quadrierungen) erforderlich; für das Ergebnis muß das Produkt von sechs davon modulo N gebildet werden; dies erfordert fünf weitere modulare Multiplikationen. Insgesamt braucht man also dreizehn.

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 $\left(m^e\right)^d \equiv m \bmod N$.

Lösung: Da e teilerfremd zu allen $p_i - 1$ gewählt wurde, ist e auch teilerfremd zum kgV $\lambda(N)$; mit dem erweiterten EUKLIDischen Algorithmus lassen sich daher $d, k \in \mathbb{Z}$ finden, so daß $de - k\lambda(N)$ gleich dem ggT eins ist. Falls d negativ sein sollte, kann man durch Addition eines Vielfachen der Gleichung $\lambda(N)e - e\lambda(N) = 0$ erreichen, daß es positiv wird; dann muß k automatisch ebenfalls positiv sein.

Für jede der Primzahlen p_i ist $k\lambda(N)$ ein Vielfaches von $p_i - 1$; für ein zu p_i teilerfremdes $m \in \mathbb{Z}$ ist daher $m^{k\lambda(N)} \equiv 1 \bmod p_i$ nach dem kleinen Satz von FERMAT und damit auch $m^{ed} = m^{1+k\lambda(N)} \equiv m \bmod p_i$. Diese Kongruenz gilt auch, wenn m nicht teilerfremd zu p_i ist, denn dann sind beide Seiten durch p_i teilbar, also kongruent Null modulo p_i. Da diese Kongruenz somit für alle $m \in \mathbb{Z}$ und für alle p_i gilt, gilt sie auch modulo dem Produkt N aller p_i.

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

Lösung: Nur, wenn λ teilerfremd zu e gewählt wird; andernfalls ist $ggT(e, \lambda) > 1$, so daß man kein d mit $ed \equiv 1 \bmod \lambda$ finden kann.

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

Lösung: Bei gleicher Größenordnung von N müßten die Primzahlen p_i für $r > 2$ deutlich kleiner gewählt werden als für $n = 2$. Kleinere Faktoren lassen sich aber zumindest tendenziell leichter finden als große, so daß das Verfahren unsicherer wird.

Aufgabe 5: (*10 Punkte*)

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

Lösung: Da $11^2 = 121 > 113$, wäre 113 durch eine der Primzahlen $2, 3, 5, 7$ teilbar, falls die Zahl zusammengesetzt wäre. Als ungerade Zahl ist 113 nicht durch zwei teilbar, durch drei auch nicht, da die Quersumme 5 keine Dreierzahl ist, und wenn 113 durch fünf teilbar wäre, müßte die letzte Ziffer 0 oder 5 sein. Schließlich ist $113 : 7 = 16$ Rest 1, so daß die Zahl auch nicht durch sieben teilbar 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 $(\mathbb{Z}/113)^\times$.

Lösung: Da p prim ist, hat $(\mathbb{Z}/113)^\times$ die Ordnung $p - 1 = 112 = 2^4 \cdot 7$. Die Ordnung eines jeden Elements ist nach LAGRANGE ein Teiler davon.
Da $2^{14} \equiv 112 \equiv -1 \bmod p$, ist $2^{28} \equiv 1 \bmod p$, die Ordnung der Zwei ist also ein Teiler von 28 und kann kein Teiler von 14 sein. Falls sie kleiner als 28 ist, muß sie also ein Teiler von $28/7 = 4$ sein, aber $2^4 = 16$ ist modulo p ungleich eins. Somit hat zwei die Ordnung 28.
Die Ordnung der Drei ist ein Teiler von 112, nicht aber von 56. Falls sie kleiner als 112 wäre, müßte sie Teiler von $112/7 = 16$ sein. Da $3^8 \equiv 7 \bmod p$, ist $3^{16} \equiv 49 \bmod p$. Somit hat drei die Ordnung 112.
Für jedes $n \in \mathbb{N}$ ist $6^n \equiv 2^n \cdot 3^n \bmod p$. Falls die Ordnung von sechs kleiner als 112 ist, muß entweder 6^{56} oder 6^{16} modulo p gleich eins sein. Da 28 ein Teiler von 56 ist, ist $2^{56} \equiv 1 \bmod p$, also $6^{56} \equiv 3^{56} \equiv -1 \bmod p$.

$$6^{16} \equiv 2^{16} \cdot 3^{16} \equiv 4 \cdot 2^{14} \cdot 3^{16} \equiv 4 \cdot (-1) \cdot 49 = -196 \equiv -83 \bmod 113\,,$$

also ist beides nicht der Fall, und die Ordnung ist 112.

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

Lösung: Hier bietet sich die *baby step - giant step*-Methode an: Die Wurzel von 113 ist knapp 11; da 113 ziemlich klein ist, bieten sich elf *baby steps* an. Die ersten elf Potenzen von drei modulo 113 sind

n	1	2	3	4	5	6	7	8	9	10	11
$3^n \bmod p$	3	9	27	81	17	51	40	7	21	63	76

12 kommt in dieser Liste nicht vor; wir brauche daher noch *giant steps* und dazu zunächst 3^{-11} mod 113, also das Inverse von 76. Dies liefert der erweiterte EUKLIDische Algorithmus:

$$\begin{aligned} 113 : 76 = 1 \text{ Rest } 37 &\Longrightarrow 37 = 113 - 76 \\ 76 : 37 = 2 \text{ Rest } 2 &\Longrightarrow 2 = 76 - 2 \cdot (113 - 76) = 3 \cdot 76 - 2 \cdot 113 \\ 37 : 2 = 18 \text{ Rest } 1 &\Longrightarrow 1 = (113 - 76) - 18 \cdot (3 \cdot 76 - 2 \cdot 113) = 37 \cdot 113 - 55 \cdot 76 \end{aligned}$$

Das Inverse ist also $-55 \equiv 113 - 55 = 58$ mod 113, und für den ersten *giant step* erhalten wir $12 \cdot 3^{-11} \equiv 12 \cdot 58 \equiv 696 \equiv 18$ mod 113. Auch diese Zahl steht nicht in der Liste; wir machen weiter mit $18 \cdot 58 = 1044 \equiv 27 = 3^3$ mod 113. Also ist $12 \cdot 3^{-11 \cdot 2} \equiv 3^3$ mod 113, d.h. $12 \equiv 3^{22+3} = 3^{25}$ mod 113. Der diskrete Logarithmus ist somit 25.

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?

Lösung: Da SHA-256 nach bisherigen Erkenntnissen ein gutes Hashverfahren ist, kann man davon ausgehen, daß die Verteilung der Hashwerte zufälliger Eingaben recht nahe an einer Gleichverteilung modulo 2^{256} ist; die Sechzehnerblöcke sind entsprechend gleichverteilt modulo 2^{16}. Dasselbe gilt für ihre Summe als Vektoren aus $\mathbb{F}_2^{16}$, denn für jede Komponente gibt es bei der Summe jeweils zwei Paare von Eingabewerten, die auf Null *bzw.* eins führen. Mit etwa $2^{16} = 65\,536$ zufälligen Variationen seines Schadprogramms hat er also eine gute Chance, eines mit der gleichen Prüfsumme zu finden. Die zufälligen Variationen kann er zum Beispiel dadurch erzeugen, daß er irrelevante *dummy* Variablen einführt und diesen zufällige Werte zuweist.

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

Lösung: Nun kommt er wegen des Geburtstagsparadoxons sogar schon mit hoher Wahrscheinlichkeit zum Ziel, wenn er sowohl vom Original als auch vom Schadprogramm ungefähr $\sqrt{2^{16}} = 2^8 = 256$ zufällige Versionen erzeugt.

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?

Lösung: Die Summe sechzehn gleichverteilter Variablen ist nach dem zentralen Grenzwertsatz annähernd normalverteilt, also deutlich inhomogener. Die Summe kann nun zwar größer als 2^{16} werden, aber maximal $2^{20} - 16$, was diese Inhomogenität wohl kaum ausgleicht. Somit hat ein Angreifer wahrscheinlich schon mit deutlich weniger als 2^{16} Versuchen mit zufälligen Variationen seines Schadprogramms gute Chancen, eines mit derselben Prüfsumme zu finden.

Bei der Summe in $\mathbb{F}_{2^{16}}$ kann man wieder von einer (annähernden) Gleichverteilung ausgehen, denn wie in $\mathbb{F}_2$ ist auch hier die Summe zweier gleichverteilter Elemente gleichvberteilt. Hier ändert sich also nichts an der Sicherheit.

Aufgabe 7: *(6 Punkte)*

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

Lösung: Die S-Box von AES besteht aus der Inversenbildung gefolgt von einer affinen Transformation über $\mathbb{F}_2$. Letztere wird bei Differenzenbildung zur Multiplikation mit einer invertierbaren 8×8-Matrix über $\mathbb{F}_2$, ist also bijektiv und somit für Sicherheitsfragen irrelevant. Bleibt also die Frage, welche Werte die Differenz von $\Delta = x^{-1}$ und y^{-1} für zwei Elemente $x, y \in \mathbb{F}_{256}$ annehmen kann, wenn $d = x - y$ vorgegeben ist. Dabei muß noch berücksichtigt werden, daß für AES (im Gegensatz zur Mathematik) $0^{-1} = 0$ gilt, und natürlich ist in $\mathbb{F}_{256}$ die Subtraktion identisch mit der Addition, da $-1 = 1$ ist.

Für $d = 0$ ist $x = y$, also auch $\Delta = x^{-1} = y^{-1}$. Entsprechendes gilt natürlich bei jedem Kryptoverfahren: Bei $d = 0$ muß immer auch $\Delta = 0$ sein und umgekehrt. Das einzige Paar (d, Δ), in dem eine Null vorkommt, ist also $(0, 0)$; hier gibt es 256 Paare (x, y), die auf diese Konstellation führen.

Für $d \neq 0$ betrachten wir zunächst inur Paare (x, y) mit $x \neq 0$ und $y \neq 0$. Für diese ist $xy(x^{-1} - y^{-1}) = y - x = d$, also $\Delta = x^{-1} - y^{-1} = d/(xy)$ und $xy = d/\Delta$. Falls also $x - y = d$ und $x^{-1} - y^{-1} = \Delta$ ist, muß $xy = d/\Delta$ sein. Im Körper $\mathbb{F}_{256}$ sind x und y somit die Lösungen der quadratischen Gleichung

$$(X - x)(X - y) = X^2 - (x + y)X + xy = X^2 + dX + \frac{d}{\Delta} = 0\,,$$

d.h. das Paar (x, y) ist durch d und Δ eindeutig bestimmt.

Wenn eines der beiden Elemente x oder y verschwindet, muß das andere gleich d sein. In diesem Fall ist $\Delta = d^{-1}$; für ein solches Paar gibt es also mindestens zwei Paare (x, y) mit $x - y = d$ und $x^{-1} - y^{-1} = \Delta$.

Da für $d = 0$ auch $\Delta = 0$ sein muß, gibt es höchstens $255^2 + 1 = 65026$ mögliche Paare (d, Δ). Zu $(0, 0)$ gehören die 256 Paare (x, x). In den $255 \cdot 254 = 64770$ Fällen mit $d \neq 0$ und $\Delta \neq d^{-1}$ gibt es jeweils entweder genau zwei Paare (x, y) und (y, x) oder keines; zusammen $256 + 64770 = 65026$ Paare. Bleiben noch $256^2 - 65026 = 510$ Stück. Genauso viele Paare $(0, d)$ und $(d, 0)$ mit $d \neq 0$ gibt es, d.h. für $(d, \Delta) = (0, 0)$ gibt es 256 Paare (x, x), und für die Fälle, in denen d und damit auch Δ nicht verschwindet, gibt es jeweils zwei Paare (x, y) und (y, x), die auf dieses Paar führen. Besser kann man sich nicht vor differentieller Kryptanalyse schützen.

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

Lösung: Ja, denn alle anderen Operationen in AES sind auf Permutationen beruhende Diffusionsschritte, die mit der Differenzenbildung kompatibel sind.