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?

Lösung: Bei einer Blockchiffre wird die zu verschlüsselnde Nachricht in Blöcke einer festen Länge zerlegt, und der Chiffrieralgorithmus transformiert jeden dieser Blöcke (praktisch immer in Abhängigkeit von einem Schlüssel) in einen Chiffreblock.
Bei einer Stromchiffre wird jedes einzelne Klartextzeichen oder -bit sofort in Chiffre umgewandelt nach einem Algorithmus, der außer diesem Zeichen auch noch Schlüsselinformation und gegebenenfalls innere Zustände benutzt.

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?

Lösung: Klartextblöcke der Länge n Bit entsprechen Elementen von $\mathbb{F}_2^n$, Chiffreblöcke der Länge m solchen von $\mathbb{F}_2^m$, und die Schlüssel liegen in $\mathbb{F}_2^s$. Somit ist $M = \mathbb{F}_2^s \times \mathbb{F}_2^n$ und $N = \mathbb{F}_2^n$, d.h. F ist eine Abbildung $\mathbb{F}_2^s \times \mathbb{F}_2^n \to \mathbb{F}_2^m$, die jedem Paar aus einem Schlüssel s und einem Klartextblock x einen Chiffreblock $F(s,x)$ zuordnet.

c) Warum muß $m \geq n$ sein?

Lösung: Damit die Nachricht entschlüsselt werden kann, muß für jeden festen Schlüssel $s \in \mathbb{F}_2^s$ die Abbildung $\mathbb{F}_2^n \to \mathbb{F}_2^m$, die den Klartextblock x auf $F(s,x)$ abbildet, injektiv sein, d.h. die Anzahl 2^m möglicher Chiffretexte muß mindestens so groß sein wie die Anzahl 2^n möglicher Klartexte.

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

Lösung: Nach Shannon ist perfekte Sicherheit höchstens dann möglich, wenn die Anzahl möglicher Schlüssel mindestens gleich der Anzahl möglicher Klartexte ist; für eine Nachricht aus k Blöcken der Länge n muß also $s \geq k \cdot n$ sein.

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

Lösung: Bei jedem Verfahren, das über einen längeren Zeitraum und/oder von einem größeren Personenkreis benutzt wird, muß man damit rechnen, daß es dem Gegner eventuell bekannt wird. Danach kann nur ein häufig wechselnder Schlüssel für Sicherheit sorgen.

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 ?

Lösung: Für A ist es $u = a^x \bmod p$, für B entsprechend $v = a^y \bmod p$.

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

Lösung: Er wählt eine Zufallszahl k mit $1 < k < p-1$, berechnet die beiden Zahlen $r = a^k \bmod p$ und $s = v^k m \bmod p$ und schickt dann das Paar (r, s) an B.
Bemerkung: Die meisten haben an Stelle von k den geheimen Schlüssel von A genommen und $v^x m$ entweder für sich oder zusammen mit u übertragen. Das wäre nur dann sicher, wenn während der gesamten Gültigkeitsdauer der beiden Schlüssel nur ein einziger Nachrichtenblock übertragen wird, was wohl kaum realistisch sein dürfte. Ansonsten ist das Verfahren extrem unsicher gegenüber Angriffen mit bekanntem Klartext: Wenn der Angreifer nur einen Nachrichtenblock kennt oder errät, kann er aus m und $v^{-x}m$ die Zahl $v^x = u^y$ berechnen und kann damit jede vergangene oder künftige Nachricht von A an B oder auch B an A entschlüsseln.

c) Wie kann B die Nachricht entschlüsseln?

Lösung: $v^k \equiv \left(a^y\right)^k \equiv a^{yk} \equiv \left(a^k\right)^y \equiv r^y \bmod p$. Somit kann B aus r und s die Nachricht m mit seinem geheimen Schlüssel y entschlüsseln als $m \equiv r^{-y}s \bmod p$.

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?

Lösung: Modulo einer Primzahl mit 3001 Bit können Blöcke der Länge 3000 Bit als Restklassen modulo p dargestellt werden. Für 30 000 Byte gleich 240 000 Bit werden also 80 Blöcke benötigt. Da für jeden Klartextblock zwei Chiffretextblöcke berechnet werden, überträgt er 160 Blöcke der Länge 3001 Bit. (Nicht jede Restklasse modulo p kann als 3000-Bit-Zahl dargestellt werden; nur die Umkehrung gilt.)

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?

Lösung: A muß sicher sein, daß v wirklich der öffentliche Schlüssel von B ist, d.h. er muß v entweder persönlich von B oder von einem vertrauenswürdigen Boten erhalten haben, oder aber v muß von einer vertrauenswürdigen Agentur zertifiziert sein.

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.

Lösung: Da $a^{p-1} \equiv 1 \bmod p$, ist die Ordnung n von a in $\left(\mathbb{Z}/p\right)^\times$ ein Teiler von $p-1$. Sie ist somit ein Produkt von Potenzen der q_i, wobei der Exponent jeweils höchstens gleich dem in der Primzerlegung von $p-1$ ist. Wäre der Exponenten eines q_i echt kleiner, so wäre n ein Teiler von $(p-1)/q_i$; mit a^n wäre daher auch $a^{(p-1)/q_i} \equiv 1 \bmod p$. Da dies nach

Voraussetzung ausgeschlossen ist, muß $n = p - 1$ sein. Damit enthält $(\mathbb{Z}/p)^\times$ mindestens die $p-1$ verschiedenen Potenzen von a; da es nicht mehr Elemente enthalten kann, ist also $(\mathbb{Z}/p)^\times = \mathbb{Z}/p \setminus \{0\}$. Somit ist jede Zahl u zwischen eins und $p-1$ invertierbar modulo p, also teilerfremd zu p. Für $u \neq 1$ heißt dies insbesondere, daß sie kein Teiler von p sein kann, d.h. p hat keinen echten Teiler und ist somit prim.

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

Lösung: Ist a eine primitive Wurzel und $b = a^r \bmod p$, so sind die Potenzen von b modulo p die Zahlen $a^{ri} \bmod p$. Falls r invertierbar modulo $p-1$ ist, durchläuft mit i auch $ri \bmod p-1$ alle Zahlen zwischen eins und $p-1$; andernfalls ist $t = \mathrm{ggT}(r, p-1) > 1$, und nur Vielfache von t treten auf. Somit ist die Anzahl der natürlichen Zahlen $r < p$, für die a^r eine primitive Wurzel ist, gleich der Anzahl der zu $p-1$ teilerfremden Zahlen zwischen eins und $p-1$, also gleich $\varphi(p-1)$, wobei φ die Eulersche φ-Funktion bezeichnet.

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 $i = 1, \ldots, r$?

Lösung: Ist p prim, so ist $\mathbb{Z}/p$ ein endlicher Körper. Da die multiplikative Gruppe eines endlichen Körpers zyklisch ist, gibt es dort Elemente der Ordnung $p-1$. Für jedes solche Element a und jeden Primteiler q von $p-1$ ist $(p-1)/q$ echt kleiner als $p-1$, also ist $a^{(p-1)/q} \not\equiv 1 \bmod p$.

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.

Lösung: Da eine Quadratzahl als letzte Ziffer eine 0, 1, 4, 5, 6 oder 9 haben muß, sind N und $N + 1^2$ keine Quadratzahlen. $N + 2^2 = 51071$ kann trotz der Eins am Ende auch keine sein, da sonst vor der Eins eine gerade Zahl stehen müßte. $N + 3^2 = 51076 = 226^2$, also ist

$$N = 226^2 - 3^2 = (226 - 3)(226 + 3) = 223 \cdot 229 \,.$$

Da $16^2 = 256$ größer ist als jeder der beiden Faktoren, muß es, falls einer der beiden nicht prim ist, einen Primteiler kleiner 16 geben. Zwei kommt nicht in Frage, da beide Zahlen ungerade sind, drei nicht wegen der Quersummen sieben und dreizehn, fünf nicht wegen der Endziffern. Wäre eine der beiden Zahlen durch sieben teilbar, so wegen $210 = 7 \cdot 30$ auch ihre Differenz mit 210, also 13 *bzw.* 19; das ist offensichtlich nicht der Fall. $220 = 20 \cdot 11$ ist durch elf teilbar, drei und neun aber nicht, also ist auch elf kein Teiler. Schließlich ist $223 : 13 = 17$ Rest zwei und damit $223 \equiv 2 \bmod 13$ und $229 \equiv 8 \bmod 13$, so daß auch dreizehn keine der beiden Zahlen teilt.

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

Lösung: Der Exponent e muß teilerfremd sein sowohl zu $223 - 1 = 222 = 2 \cdot 3 \cdot 37$ als auch zu $229 - 1 = 228 = 2^2 \cdot 3 \cdot 19$, darf also durch keine der vier Primzahlen $2, 3, 19$ und 37 teilbar sein. Die kleinste solche Zahl ist $e = 5$.

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

Lösung: Ein solches d läßt sich beispielsweise konstruieren, indem man den erweiterten Euklidischen Algorithmus anwendet auf e und das kleinste gemeinsame Vielfache von

222 und 228, also auf $r = 2^2 \cdot 3 \cdot 19 \cdot 37 = 8436$.

$$8436 : 5 = 1687 \quad \text{Rest } 1 \Longrightarrow 1 = 8436 - 1687 \cdot 5\,.$$

Da wir ein positives d wollen, addieren wir noch 8436 und erhalten $d = 8436 - 1687 = 6749$.

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!

Lösung: Zum Unterschreiben wird mit dem privaten Exponenten d potenziert; wegen $2^{12} = 4096 < 6749 < 8192 = 2^{13}$ hat dieser dreizehn Bit. Über zwölf Quadrierungen können die zweite bis 2^{12}-te Potenz berechnet werden, und durch höchstens zwölf Multiplikationen erhalten wir daraus die d-te Potenz. Somit ist 24 eine realistische obere Schranke.
Wenn wir eine schärfere Schranke wollen, müssen wir d im Zweiersystem darstellen:

$$6749 = 2^{12} + 2^{11} + 2^9 + 2^6 + 2^4 + 2^3 + 2^2 + 1$$

hat acht Binärziffern eins, also werden zusätzlich zu den zwölf Quadrierungen noch sieben weitere Multiplikationen 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 $a^{-1000} \bmod N$!

Lösung: Wie die Zahlen aus der Aufgabenstellung zeigen, hat a modulo N die Ordnung sechs; $a^r \bmod N$ hängt also nur ab von $r \bmod 6$. Da $1000 \equiv 4 \bmod 6$, ist

$$a^{1000} \equiv a^4 \equiv 513 \bmod N\,.$$

a^{-1000} ist invers zu $a^{1000} \equiv a^4 \bmod N$; wegen $a^6 \equiv 1 \bmod N$ ist also

$$a^{-1000} \equiv a^2 \equiv 37155 \bmod\ .$$

Bemerkung: Wer nicht gesehen hat, daß a^n nur von $n \bmod 6$ abhängt, kann $a^{1000} \bmod N$ natürlich auch nach dem allgemeinen Algorithmus berechnen, indem er durch fortgesetztes Quadrieren zunächst die Potenzen $a^2, a^4, \ldots, a^{512}$ modulo N berechnet und daraus, entsprechend der Binärziffern von 1000, das Ergebnis als Produkt einiger dieser Zahlen. Was aber *nicht* geht, auch wenn rund die Hälfte aller Klausurteilnehmer so gerechnet haben, ist ein Ansatz, der 1000 zum Beispiel als das Produkt $2 \cdot 4 \cdot 5 \cdot 5 \cdot 5$ darstellt und daraus folgert, daß $a^{1000} \equiv a^2 \cdot a^4 \cdot a^5 \cdot a^5 \cdot a^5 \bmod N$ sei. Nach den aus der Schule bekannten Rechenregeln für Potenzen ist $a^n \cdot a^m = a^{n+m}$, so daß rechts $a^{2+4+5+5+5} = a^{21}$ steht. $a^{nm} = \left(a^n\right)^m$.

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

Lösung: Die Ordnung von a ist sechs. Da $N - 1 = 37668$ gerade ist und Quersumme dreißig hat, ist $N - 1$ durch sechs teilbar.

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!

Lösung: $\left(a^3\right)^2 = a^6 \equiv 1 \bmod 1$, d.h. $a^3 \equiv 26828 \bmod N$ hat modulo N das Quadrat eins, ist aber weder $+1$ noch -1. Wäre N prim, so wäre $\mathbb{Z}/N$ ein Körper und das Polynom

X^2-1 hätte nur die beiden Nullstellen ± 1. Da es hier mit a^3 noch mindestens eine weitere Nullstelle gibt, kann N keine Primzahl sein.

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.

Lösung: Der Verschlüsselungsaufwand ist praktisch identisch zu dem mit einfachem DES, denn de facto wird jeder 128-Bit-Block in zwei 64-Bit-Blöcke zerteilt, von denen der erste mit s_1 und der zweite mit s_2 verschlüsselt wird. Die Sicherheit ist auch nicht viel größer als die von DES: Durch systematisches Durchprobieren aller 2^{56} Möglichkeiten für s_1 findet man einen Schlüssel, der für die (oder einige) 64-Bit-Blöcke an den ungeraden Positionen sinnvolle Textfragmente liefert, und entsprechend erhält man s_2 mit denen an geraden Positionen.

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?

Lösung: Falls die Permutation erst hinterher angewandt wird, kann sie ein Angreifer problemlos rückgängig machen, so daß sie keinerlei Effekt auf die Sicherheit hat. Wendet man sie vorher an, liefern die DES-Entschlüsselungen der 64-Bit-Teilblöcke keinen Klartext mehr, sondern Blöcke, bei denen die ungeraden Bits zu einem, die geraden Bits zu einem anderen Klartext gehören. Das ist zwar immer noch sehr speziell, aber immerhin etwas sicherer als vorher.

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

Lösung: Die Sicherheit gegen differentielle Kryptanalyse entspricht genau der von DES, d.h. sie ist ziemlich gut, aber nicht perfekt. Bei AES ist sie perfekt, also besser.

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!

Lösung: Dafür läßt sich jeder Operationsmodus verwenden, der die Chiffre nur zur Erzeugung eines Schlüsselstroms verwendet, der dann auf den Klartext addiert wird. Unter den standardisierten Modi sind das *Cipher Feedback* (CFB), *Output Feedback* (OFB) und *Counter Mode* (CTR).

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!

Lösung: Wir müssen zeigen, daß fünf modulo 23 die Ordnung 22 hat. Falls nicht, hat es eine der Ordnungen eins, zwei oder elf. Eins ist es offensichtlich nicht, zwei auch nicht, denn $5^2 = 25 \equiv 2 \bmod 23$, und elf kommt nicht in Frage, denn wegen der Teilbarkeit von $5^{11}+1$ durch 23 ist $5^{11} \equiv -1 \bmod 23$. Somit muß die Ordnung 22 sein, d.h. die Fünf ist eine primitive Wurzel modulo 23.

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

Lösung: Die nächste Quadratzahl nach 23 ist 25; wir arbeiten daher mit $m = 5$. Die *baby steps* sind (alle Rechnungen modulo 23)

$$5^1 = 5, \quad 5^2 = 2, \quad 5^3 = 10, \quad 5^4 = 5 \quad \text{und} \quad 5^5 = 20\,.$$

Für die *giant steps* brauchen wir die Zahlen $3 \cdot 5^{-5k}$ mod 23.
5^{-5} mod 23 ist das Inverse zu $5^5 \equiv 20 \bmod 23$; berechnen wir also zunächst dieses mit dem erweiterten EUKLIDischen Algorithmus:

$$23 : 20 = 1 \quad \text{Rest } 3, \quad 20 : 3 = 6 \quad \text{Rest } 2 \quad \text{und} \quad 3 : 2 = 1 \quad \text{Rest } 1\,.$$

Somit ist $1 = 3 - 2 = 3 - (20 - 6 \cdot 3) = 7 \cdot 3 - 20 = 7 \cdot (23 - 20) - 20 = 7 \cdot 23 - 8 \cdot 20$, also ist $-8 \equiv 15 \bmod 23$ das Inverse von 20 modulo 23.
Damit ist $3{\cdot}5^{-5} \equiv 3{\cdot}15 \equiv -1 \bmod 23$, $3{\cdot}5^{-10} = (3{\cdot}5^{-5}){\cdot}5^{-5} \equiv (-1){\cdot}15 = -15 \equiv 8 \bmod 23$ und $3 \cdot 5^{-15} = (3 \cdot 5^{-10}) \cdot 5^{-5} \equiv 8 \cdot 15 \equiv 5 \bmod 23$. Also ist

$$3 \cdot 5^{-15} \equiv 5^1 \bmod 23 \Longrightarrow 3 \equiv 5^{16} \bmod 23\,.$$

Der diskrete Logarithmus modulo 23 von drei zur Basis fünf ist also 16.

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!

Lösung: Über $\mathbb{F}_2$ ist $(a + b)^2 = a^2 + b^2$, also ist

$$(\alpha + 1)^4 = \left((\alpha + 1)^2\right)^2 = \left(\alpha^2 + 1\right)^2 = \alpha^4 + 1\,.$$

Wegen $\alpha^3 = \alpha + 1$ ist $\alpha^4 = \alpha^2 + \alpha$, also $(\alpha + 1)^4 = \alpha^4 + 1 = \alpha^2 + \alpha + 1$.

Aufgabe 8: *(4 Punkte)*

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

Lösung: Erstens muß sich der Hashwert leicht auch dem Ausgangstext berechnen lassen. Zweitens darf es nicht mit realistischem Aufwand möglich sein, zu einem gegebenen Hashwert einen Text zu konstruieren, der darauf führt. Drittens schließlich darf es nicht einmal mit realistischem Aufwand möglich sein, zwei verschiedene Texte zu konstruieren, die auf den gleichen Hashwert führen.

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

Lösung: Wie jede Blockchiffre liefert auch RIJNDAEL ein Hashverfahren, wenn man etwa Cipher Block Chaining verwendet und die Verschlüsselung des letzten Blocks als Hashwert wählt. Wegen des Geburtstagsparadoxons hat man allerdings bei Blocklänge $2n$ nur ein Sicherheitsniveau von n Bit; will man also das heute anzustrebende Sicherheitsniveau von 128 Bit erreichen, darf man nicht mit 128-Bit-Blöcken wie bei AES arbeiten, sondern braucht die (nicht als AES standardisierte) RIJNDAEL-Variante mit Blocklänge 256. Die Schlüssellänge hat für die Sicherheit des Hashverfahrens keine Bedeutung, da der Schlüssel hier ohnehin als Teil des Algorithmus veröffentlicht wird.