Zusammenfassung des Vortrags

DEAL

vorgetragen im Rahmen des Seminars: „Analyse kryptographischer Algorithmen“

unter Leitung von Prof. Köbler und M. Schwan

am 29. Mai 2002

von

Ingo Bendel

1. Einleitung

Der kryptographische Algorithmus DEAL, dessen Buchstaben die Abkürzung für „Data Encryption Algorithm with Larger blocks“ ist, wurde im Februar 1998 von Lars Knudsen entwickelt, in [3] veröffentlicht, und im August 1998 von Richard Outerbridge dem National Institut of Standards and Technology (NIST) als Kandidat für den Advanced Encryption Standard (AES) vorgeschlagen.[7]
DEAL konnte jedoch die 2. Runde des Auswahlverfahrens schon nicht erreichen, und wurde somit nicht zum AES erhoben.

Bei diesem Algorithmus handelt es sich um eine Feistel-Chiffre mit einer 128 Bit Blockgröße, die den „Data Encryption Standard“(DES) in der Rundenfunktion verwendet. Für den DEAL kann zwischen drei verschieden großen Schlüssellängen gewählt werden, nämlich 128 Bit, 192 Bit und 256 Bit. Entsprechend wird der DEAL dann als DEAL-128, DEAL-192 bzw. DEAL-256 bezeichnet. Für die ersten beiden werden von Knudsen sechs Runden für den DEAL-256 acht Runden empfohlen.

2. DES

2.1. Historie

Im Mai 1973 wurde vom National Bureau of Standards(NBS) erstmals eine Ausschreibung für einen normungsfähigen, kryptographischen Algorithmus veranstaltet. Trotz großem Interesse gab es jedoch keine Einsendungen und erst 1974 auf einen zweiten Anlauf hin, reichte ein Entwicklerteam von IBM eine Weiterentwicklung der Lucifer-Chiffre ein.

1975 wurde nach Analyse durch die NSA eine leicht überarbeitete Version veröffentlicht und als Standard vorgeschlagen um im November 1977 dann als Bundesstandard vom NBS genormt zu werden. Die offizielle Bezeichnung lautete „Data Encryption Standard“, kurz DES, und wurde im Federal Information Processing Standard(FIPS) PUB 46 beschrieben.
1981 wurde der DES auch vom American National Standard Institut(ANSI) unter der Bezeichnung Data Encryption Algorithm(DEA) standardisiert.
In den Jahren nach 1977 folgten dann weitere Normungen durch das NBS welche Betriebsmodi des DES sowie Richtlinien für den Gebrauch und die Implementierung enthielten. DES war damit der erste in seiner Spezifikation vollständig veröffentlichte und durch die NSA begutachtete kryptographische Algorithmus. Er wurde für „ausreichend sicher“ für die normale Geheimhaltung befunden, allerdings nicht bei der Verschlüsselung von streng geheimen Informationen.
Der Standard galt erst einmal für 5 Jahre, und sollte dann auf Aktualität und Sicherheit hin überprüft werden. Dies führte zu einer Bestätigung des DES als Standard in den Jahren 1982, 1987,1992 und 1997, so daß er es auf 25 Jahre Regierungsstandard gebracht hat.
Im Jahr 2002 wird er nun durch den „Advanced Encryption Standard“(AES) abgelöst.

2.2. DES

Beim DES handelt es sich um eine Blockchiffre mit Feistel-Netzwerk, welche Daten in Blöcken von 64 Bit in 16 Runden verschlüsselt. DES ist damit ein symmetrischer Algorithmus: Ver- und Entschlüsselung benutzten den gleichen Algorithmus und den gleichen Schlüssel.

Die Schlüssellänge beträgt 64 Bit jedoch ist die effektive Schlüssellänge nur 56 Bit, da jedes achte Bit (jeweils die niederwertigsten Bits der einzelnen Bytes) einer Paritätsprüfung dienen, und bei der Ver- und Entschlüsselung ignoriert werden. Die gesamte Sicherheit des Verfahrens beruht auf dem Schlüssel, da ja die Spezifikation wie oben erwähnt vollständig veröffentlicht wurde.
Bis heute wurde kein praktisch verwertbarer Angriffspunkt für Attacken beim DES gefunden. Dennoch gilt er heute nicht mehr als sicher, da ein Brute-Force-Angriff auf die 2^{55} Schlüssel im technisch Möglichen liegt. 1993 entwickelte Michael Wiener eine Maschine, dessen Herstellungskosten er auf eine Million US-Dollar schätzte und die in der Lage ist mittels Brute-Force-Attacke den Schlüssel in 3.5 Stunden ausfindig zu machen.[1]
Gerüchteweise ist die NSA sogar in der Lage mittels spezieller Algorithmen, welche es ermöglichen Teillösungen für den möglichen Schlüssel auszuschließen, den DES in 3 bis 15 Minuten zu knacken, wobei die Kosten solcher Maschinen in größerer Stückzahl um 50000 US-Dollar liegen.[2]

Aus Zeitgründen und der Tatsache, das der DES in der Vorlesung „Kryptologie I“ von Prof. Köbler detailliert vorgestellt wird, verzichte ich hier auf nähere technische Darstellung, möchte aber, auf eine Weiterentwicklung des DES, den Triple-DES, eingehen.

Der unzureichenden Schlüssellänge kann man naiv durch wiederholte Verschlüsselung mit dem gleichen Algorithmus und verschiedenen Schlüsseln begegnen.

$$C = DES_{K'}(DES_K(P))$$

Dies würde allerdings den effektiven Schlüssel nur dann vergrößern und damit mehr vor einem Brute-Force-Angriff schützen, wenn der Algorithmus frei von der „Gruppeneigenschaft“ ist. Dies ist genau dann der Fall, wenn eine Verschlüsselung mit Schlüssel K und anschließende Verschlüsselung mit dem Schlüssel K‘ nicht zum gleichen Chiffretext führt wie eine einzige Verschlüsselung mit einem Schlüssel K^*. Denn dann muß wieder nur ein Schlüssel nämlich K^* angegriffen werden, und die effektive Schlüssellänge bleibt unverändert.
Für den DES konnte allerdings nachgewiesen werden, das er die „Gruppeneigenschaft“ nicht besitzt, d.h. es gilt:

$$DES_{K^*} \neq DES_{K'}(DES_K(P))$$

3. Triple-DES

Auf diesen Tatsachen aufbauend entwickelte Tuchman 1979 den Triple-DES-Algorithmus. Dieser erhält zwei Schlüssel K und K‘, die zusammen eine effektive Schlüssellänge von 112 Bit besitzen und somit gegen Brute-Force-Angriffe erheblich besser gerüstet sind als der DES.

$$C = DES_K\left(DES_{K'}^{-1}\left(DES_{K''}(P)\right)\right) \quad K = K''$$

In der ersten DES-Verschlüsselung wird der Schlüssel K‘‘ auf den Klartext P angewandt, das Ergebnis wird mit dem Schlüssel K‘ dann entschlüsselt, um dann mit dem Schlüssel K der gleich dem K‘‘ ist, wieder verschlüsselt zu werden. Ist der Schlüssel K auch gleich dem Schlüssel K‘ so führt der Algorithmus nur die einfache DES-Verschlüsselung durch.
Der Triple-DES kann in sieben verschiedenen Modi verwendet werden, unter denen sich auch die 4 Standardmodi befinden. Es ist offensichtlich, dass der Algorithmus bei dreimaliger Anwendung des DES auch mindestens dreimal so langsam ist, da eine Parallelisierung ausgeschlossen ist. In einigen Quellen habe ich auch die Möglichkeit gefunden, die Schlüssellänge auf effektive 168 Bit „aufzubohren“, indem die Schlüssel K und K‘‘ ungleich sind, also drei echt verschiedene Schlüssel verwendet werden. Das entspricht aber glaube ich nicht dem genormten Standard von Triple-DES.
Es gibt bis heute kein rationales Argument, das gegen die Sicherheit von Triple-DES spricht.

4. DEAL

Wie schon erwähnt handelt es sich beim DEAL um eine 128 Bit Feistel-Chiffre welche den DES in der Rundenfunktion verwendet, und die Schlüssel der Länge 128 Bit, 192 Bit und 256 Bit akzeptiert.
DEAL kann in allen drei Schlüsselversionen in den vier Standardmodi:

ECB (electronic code book),
CBC (cipher block chaining),
OFB (output feedback)
CFB (cipher feedback)

benutzt werden. Im Unterschied zum DES werden beim DEAL alle Schlüsselbits genutzt, d.h. es gibt keine Parity-Check-Bits! Deswegen ist die effektive Schlüssellänge auch gleich der des Schlüssels.

4.1. DEAL im ECB-Modus

Notation:
$C = E_B(A)$ DES-Verschlüsselung eines 64 Bit Klartextblocks A mit Schlüssel B
$Y = EA_Z(X)$ DEAL-Verschlüsselung eines 128 Bit Klartextblocks X mit dem Schlüssel Z

Der Klartext P wird zerlegt in 128 Bit große Blöcke P_i : $P = P_1, P_2,..., P_n$

Schlüsselgenerierungsalgorithmus nimmt den Schlüssel K und liefert r-viele Rundenschlüssel RK_i wobei i = 1,..,r und r∈ {6,8} ist.

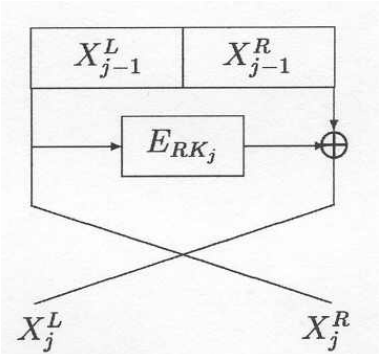
X^L und X^R bezeichnen die linke bzw. rechte Hälfte von Block X und sind jeweils 64 Bit lang.

Die Verschlüsselung des Klartexts P_i (abgekürzt als $EA_K(P_i)$) geschieht wie folgt:

Setze $X_0^L = P_i^L, X_0^R = P_i^R$
und berechne für j = 1,..,r:

$$X_j^L = E_{RK_j}\left(X_{j-1}^L\right) \oplus X_{j-1}^R$$
$$X_j^R = X_{j-1}^L$$

Setze $C_i = X_r^L \parallel X_r^R$



Für DEAL-128 und DEAL-192 wie auch schon erwähnt r = 6 Runden empfohlen, für DEAL-256 reichen sie jedoch nicht aus, deshalb sollte r = 8 Runden durchgeführt werden.
Der DEAL-256 ist aufgrund der Performance nur bei sehr starker Verschlüsselungen empfehlenswert.
Das Vertauschen der beiden Chiffretexthälften in der letzten Runde von DEAL wird nicht wie beim DES weggelassen! Das hat jedoch keinen Einfluß auf die Sicherheit der Blockchiffre im ECB-Modus.

4.2. DEAL im CBC-Modus

CBC-Modus bedeutet, dass jeder Klartextblock mit dem nächsten Block vor der Verschlüsselung XOR-verknüpft wird.

Seien	$P_1,P_2,...,P_n$	die 128-bit Klartextblöcke
und	$C_1,C_2,...,C_n$	die korrespondierenden Chiffretextblöcke
	C_0	ist ein initialer Wert

$$C_i = EA_K\left(C_{i-1} \oplus P_i\right)$$

4.3. Der Schlüsselgenerator des DEAL

Als Eingabe erhält der Schlüsselgenerator s-viele Teilschlüsseln $K_1,...,K_s = K$ für s = 2,3,4 des vom Benutzer eingegebenen Schlüssels K, wobei jeder K_i 64 Bit breit ist und als Ausgabe werden r-viele DES Schlüssel RK_i für r = 6,8 geliefert.
Die Verschlüsselung unter Verwendung des DES im CBC-Modus mit einem festen DES-Schlüssel K_* und dem initialem Wert auf Null gesetzt. K_* = 0x0123456789abcdef
Die resultierenden Chiffretextblöcke sind die Rundenschlüssel RK_i welche nur als DES-Schlüssel verwendet werden, d.h. die Paritätsbits von RK_i werden in der i-ten Runde nicht zur Verschlüsselung genutzt.

Für den DEAL-128 werden die 6 Rundenschlüssel wie folgt definiert:

$$
\begin{aligned}
RK_1 &= E_{K_*}(K_1), \\
RK_2 &= E_{K_*}(K_2 \oplus RK_1), \\
RK_3 &= E_{K_*}(K_1 \oplus \langle 1 \rangle \oplus RK_2), \\
RK_4 &= E_{K_*}(K_2 \oplus \langle 2 \rangle \oplus RK_3), \\
RK_5 &= E_{K_*}(K_1 \oplus \langle 4 \rangle \oplus RK_4), \\
RK_6 &= E_{K_*}(K_2 \oplus \langle 8 \rangle \oplus RK_5).
\end{aligned}
$$

wobei $\langle i \rangle$ ein 64-bit Zeichenkette ist, in der nur das (i-1)te Bit gesetzt ist und alle anderen Bits ungesetzt, also Null sind.
$\langle 1 \rangle$ wird bspw. hexadezimal durch „0x8000000000000000“ repräsentiert.

Für den DEAL-192:

$$
\begin{aligned}
RK_1 &= E_{K_*}(K_1), \\
RK_2 &= E_{K_*}(K_2 \oplus RK_1), \\
RK_3 &= E_{K_*}(K_3 \oplus RK_2), \\
RK_4 &= E_{K_*}(K_1 \oplus \langle 1 \rangle \oplus RK_3), \\
RK_5 &= E_{K_*}(K_2 \oplus \langle 2 \rangle \oplus RK_4), \\
RK_6 &= E_{K_*}(K_3 \oplus \langle 4 \rangle \oplus RK_5).
\end{aligned}
$$

Dies erfordert 6 DES-Verschlüsselungen mit dem festem DES-Schlüssel K_*, wobei die Rundenschlüssel jeweils nur einmal berechnet werden müssen, wenn sie jeweils gespeichert werden.

Für den DEAL-256:

$$
\begin{aligned}
RK_1 &= E_{K_*}(K_1), \\
RK_2 &= E_{K_*}(K_2 \oplus RK_1), \\
RK_3 &= E_{K_*}(K_3 \oplus RK_2), \\
RK_4 &= E_{K_*}(K_4 \oplus RK_3), \\
RK_5 &= E_{K_*}(K_1 \oplus \langle 1 \rangle \oplus RK_4), \\
RK_6 &= E_{K_*}(K_2 \oplus \langle 2 \rangle \oplus RK_5), \\
RK_7 &= E_{K_*}(K_3 \oplus \langle 4 \rangle \oplus RK_6), \\
RK_8 &= E_{K_*}(K_4 \oplus \langle 8 \rangle \oplus RK_7).
\end{aligned}
$$

Hier werden 8 DES Verschlüsselungen mit festem Schlüssel benötigt.

Als Entwurfskriterien hat Knudsen Folgendes für den Schlüsselgenerator formuliert:

- Die Rundenschlüssel sollen von vielen Bits des Schlüssels K abhängen, aber ohne viel Aufwand zu machen.
- Jeder der s aufeinanderfolgenden Rundenschlüssel soll eine Entropie(=Informationsgehalt) von 56*s Bits haben.
- Es sollen keine halbschwachen oder schwachen Schlüssel und nicht die „Komplementäreigenschaft“ vorliegen.

„Komplementäreigenschaft“: Sei x‘ das Komplement von x, dann gilt:
$E_K(P) = C$
$E_{K'}(P') = C'$
das bedeutet, dass Komplemente von Schlüsseln und Klartext zum Komplement des Chiffretexts führen, wie z.B. beim DES.

Der Offset $\langle i \rangle$ wurde eingeführt um schwache, halbschwache Schlüssel und die „Komplementäreigenschaft“ zu verhindern. Ohne ihn würden z.B. für den DEAL-128 die Schlüssel $K_1 = K_2 = D_{K^*}(0)$ 6 Rundenschlüssel alle mit den Werten Null generieren, genauso wie beim DES.

4.4. Sicherheit des DEAL

- L. Knudsen:

Ein *brute-force* Angriff ist auf Grund der Schlüssellänge in allen drei Fällen offensichtlich nicht durchführbar. Eine *matching-chiffretext* Attacke benötigt als Voraussetzung 2^{64} Chiffretextblöcke für einen Erfolg.

Für den DEAL-192/256 würde eine einfache *meet-in-the-middle* Attacke die Schlüssel in einer Zeit von $(2^{56})^3 = 2^{168}$ bzw. $(2^{56})^4 = 2^{224}$ Verschlüsselungen unabhängig von der Schlüsselgenerierung finden. Dazu werden noch 2^{173} Bytes Speicher und 3 Klartexte benötigt. Damit wäre diese Attacke schneller als ein brute-force Angriff, ist durch ihre Speicheranforderungen aber gänzlich unrealistisch, auch wenn Trade-off-Methoden bekannt sind, um Platz auf Kosten von länger Laufzeit zu sparen.

Für den DEAL-128 und DEAL-192 benötigt die allgemeine Attacke auf eine 6-Runden-Feistel-Chiffre (*chosen-plaintext* Attacke) über 2^{121} DES-Verschlüsselungen und über 2^{70} gewählte Klartexte. Auf Grund der benötigten Anzahl gewählter Klartexte ist aber auch dieser Angriff undurchführbar.
Als kleine Abschätzung: $2^{70} = (2^{10})^7 \approx (10^3)^7 = 10^{21}$ = 1 Trilliarde Klar-Chiffretextpaare

Erst wenn ein Angreifer 2^{64} Paare von Klar-und Chiffretexten bekommen würde, wird eine solche Attacke realistisch, d.h.: 2^{64} Paare *2 * 128 Bit = 2^{72} Bit Speicher erforderlich, das sind rund 1 Mrd($2^{30} \approx 10^9$) * 2^{40} (= 1 TB) => rund 1 Mrd TerraByte, also viel zu viel.

- S. Lucks:

Lucks beschreibt in [4] eine *chosen-chiffertext* Attacke auf den DEAL-192, die einen Trade-off zwischen der Anzahl der Chiffretexte, Speicheranforderungen und der Zeit für die Berechnung erlaubt.

Parameter	Gewählte Chiffretexte	Verschlüsselungen	Speicher
p	2^{32+p}	$8*2^{191-2p}$	2^{39+p} Bit

mit $p \in \{0.5, 1, 8, 16, 24\}$

Die geringsten Speicheranforderungen ergeben sich bei:
2^{33} gewählte Chiffretexte, 2^{192} DES-Verschlüsselungen, 2^{40} Bits Speicher

Die kleinste Anzahl Verschlüsselungen bei:
2^{56} gewählte Chiffretexte, 2^{146} DES-Verschlüsselungen, 2^{63} Bits Speicher

Die DEAL Schlüsselgeneration basiert auf einer langsamen aber starken Verschlüsselung, sprich dem DES, jedoch hängt der Rundenschlüssel RK_1 noch nicht von allen Schlüsseln K_i ab, genauso wie RK_2 nicht beim DEAL-192/256, und der RK_3 beim DEAL-256.

Ist ein Teil des Schlüssels K bekannt, hängt die Sicherheit des DEAL davon ab, welchen Teil des Schlüssels es betrifft. Die Sicherheit des DEAL-192 Schlüssels liegt, wenn 64-Bit bekannt sind noch über der des DEAL-128, wenn dies z.B. gerade der K_3 ist. Wenn der Angreifer jedoch K_1 kennt, muß er nur noch einen 128 Bit Schlüssel in 5 statt 6 Runden wie beim DEAL-128 angreifen, da der RK_1 ja nur mit dem K_1 gebildet wird.

Diese Probleme können gelöst werden, indem eine weitere Verschlüsselung für den DEAL-128, zwei weitere für den DEAL-192 und drei weitere für den DEAL-256 hinzugefügt werden. Dies geschieht nach dem gleichen Prinzip, auf dem alle DEAL Schlüsselgenerationen beruhen.
Für den DEAL-128 werden dann nur die $RK_2,...,RK_7$ als Rundenschlüssel verwendet, wobei RK_7 wie folgt berechnet wird:

$$RK_7 = E_{K_*}\left(K_1 \oplus \langle 5 \rangle \oplus RK_6\right)$$

und $\langle 5 \rangle$ wieder eine Konstante verschieden von $000..0, \langle 1 \rangle \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle$ ist.
Entsprechend wird für den DEAL-192 und den DEAL-256 vorgegangen.

Es ist festzuhalten, dass die zusätzlichen Verschlüsselungsoperationen nur einen zusätzlichen Aufwand zwischen 1/6 und 3/8 der Zeit des originalen Schlüsselgenerators bedeuten, also eine akzeptable Verlangsamung für die Modifikation.

- J. Kelsey und B. Schneier

In [5] wird die Schwäche des Schlüsselgenerationsalgorithmus demonstriert, die sowohl zu äquivalenten Schlüsseln, als auch zu einer Anfälligkeit für related-key Attacken führt.

Ein Verschlüsselungsalgorithmus besitzt *äquivalente Schlüssel* wenn für zwei oder mehr Schlüssel K, K‘ gilt: $K \neq K' \wedge E_K(X) = E_{K'}(X)$ für alle Klartexte X.

Für den DEAL-128 wird ein Algorithmus angegeben, der mit einem Aufwand von 2^{64} DES-Verschlüsselungen Paare von äquivalenten Schlüsseln findet. Ein davon verschiedener, angegebener Algorithmus bestimmt mit nur 6 bzw. 8 DES-Verschlüsselungen für den DEAL-192 und DEAL-256 jeweils eine Menge von 256 äquivalenten Schlüsseln.

Des weiteren ist eine *related-key* Attacke auf den DEAL-192 angegeben, welche unter Verwendung von 2^{33} verwandten Schlüsseln, sowie drei gewählten und mit jedem dieser Schlüssel verschlüsselten Klartexte, bei $3*2^{45}$ Bytes Speicher 2^{137} DES-Verschlüsselungen oder bei $3*2^{69}$ Bytes Speicher 2^{113} DES-Verschlüsselungen benötigt. Sie ist bei diesem Aufwand allerdings nur von theoretischen Interesse.

Abschließend kann man sagen, dass keine mit heutigen Mitteln realisierbare Attacke auf den DEAL bekannt ist.

R. Outerbridge merkte in [7] jedoch zu bedenken an, dass der DEAL auf dem DES basiert, und damit mögliche Einbrüche in den DES auch Einbrüche in den DEAL erlauben würde.

4.5. Performance

Die Ver- und Entschlüsselungsgeschwindigkeit bei den Schlüssellängen sind verschieden. Der DEAL-128 und -192 sind fast so schnell(bzw. langsam) wie der Triple-DES, welcher dreimal langsamer als der DES ist. Der DEAL-256 ist um 33% langsamer als der DEAL-128.
Die Performancetests in [6] auf 32 Bit und 64 Bit CPUs sowie bei Hash-Funktionen lassen sich mit folgendem Zitat ausreichend zusammenfassen: „... DEAL is a straw-man algorithm that provides a worst-case performance benchmark for AES...“

Bei der Smart-Card-Performance schnitt der DEAL, der mit 50 Bytes RAM Anforderungen zu den wenigen, für eine Smart-Card-Implementation geeigneten Algorithmen gehörte (< 64 Bytes RAM), genauso schlecht ab, und war ähnlich „schnell“ wie der Triple-DES. Dies liegt vor allem an der DEAL-Schlüsselberechnung, die ja den langsamen DES verwendet.

4.6. Zukunftsaussichten

DEAL hat den Vorteil, dass der verwendete DES schon ausreichend studiert und deployed wurde. Deshalb wird er in Zukunft Verbreitung in der Realen Welt finden, denn die breite Verfügbarkeit von DES-Hard- und software ermöglicht eine einfache und billige Implementierung in vielen verschiedenen Umgebungen.

4.7. Literatur

[1] B. Schneier: *Angewandte Kryptographie*, Addison-Wesley, 1996

[2] R. Wobst: *Abenteuer Kryptologie*, Addison-Wesley, 1998

[3] L. Knudsen: *DEAL- A 128-bit Block Cipher*, AES-Proposal, Juni 1998
http://www.ii.uib.no/~larsr/papers/deal.pdf

[4] S. Lucks: *On the Security of the 128-Bit Block Cipher DEAL*, 1999
http://th.informatik.uni-mannheim.de/m/lucks/papers/deal.ps.gz

[5] J. Kelsey, B. Schneier: *Key-Schedule Cryptoanalysis of DEAL*,
http://www.counterpane.com/deal.pdf

[6] B.Schneier, J. Kelsey, u.a.: *Performance Comparison of the AES Submissions*, Feb. 1999
http://www.counterpane.com/aes-performance.pdf

[7] R. Outerbridge: *AES Candidate DEAL*, Präsentationsfolien, 1998
http://csrc.nist.gov/encryption/aes/round1/conf1/deal-slides.pdf