Fachhochschule Aargau
Nordwestschweiz

Differentielle Kryptoanalyse

Seminararbeit von Markus Brunold

Fachhochschule Aargau
Departement Technik
Studiengang I

Betreuender Dozent: Prof. Dr. Carlo U. Nicola

Windisch, 30. Mai 2002

Abstract

In this paper, I present a tutorial on differential cryptanalysis, one of the most important attacks applicable to block ciphers. I intend to show to the beginner the different steps needed to crack the well known DES block cipher. The tutorial is based on the analysis of a Feistel-cipher variant called Data Encryption Standard Algortithm (DES).

Inhaltsverzeichnis

Kapitel 1

Kryptoanalyse

1.1 Allgemein

Die Kryptoanalyse versucht aus einem Geheimtext ohne den entsprechenden Schlüssel den zugehörigen Klartext zu erstellen. Bei einem erfolgreichen Versuch kann der Klartext oder der Schlüssel gefunden werden. Die Kryptoanalyse versucht also die bestehenden Verschlüsselungsverfahren zu brechen und dabei ihre Schwachstellen aufzudecken.

1.2 Prinzip von Kerckhoff

Die moderne Kryptoanalyse basiert auf dem Prinzip von Kerckhoff (Jahr: 1883). Nach diesem Prinzip darf die Sicherheit eines Kryptosystems nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit soll nur auf der Geheimhaltung des Schlüssels basieren.

1.3 Vorgehensweise

Voraussetzung ist die Kenntnis des Geheimtextes und des Chiffrierverfahrens. Das Hauptproblem des Angreifers ist die Tatsache, dass bei den meisten Chiffriermechanismen die Zahl der möglichen Schlüssel so gross ist, dass ein Brute-Force-Angriff keinen Erfolg in angemessener Zeit bringen würde. Hilfreich dagegen ist jedoch die Tatsache, dass die meisten Benutzer (beispielsweise bei einer Passworteingabe) nicht irgendeinen Schlüssel wählen, sondern irgendeinen thematischen Begriff, Namen etc. Dadurch verringert sich die Zahl der Möglichkeiten immens; der Angreifer kann einen sogenannten Wörterbuchangriff durchführen. Es entsteht ein drastisch reduzierter Schlüsselraum.
Desweiteren werden die Einträge ins Wörterbuch auf verschiedenste Weise modifiziert, d.h. es werden Zeichen davor oder dahintergesetzt, Gross- und Kleinschreibung ist möglich, die Worte werden rückwärts geschrieben, verdoppelt

usw. Auf diese Weise ist die Erfolgsquote, zumindest was die Ermittlung von Passwörtern angeht, auch mit besten Chiffrieralgorithmen überraschend gross.

Allgemeine Angriffspunkte des Kryptoanalytikers sind:

- Wie wurde der Klartext erzeugt?
- Welche Eigenschaften hat es?
- Durchprobieren (wenn möglich) des gesamten Schlüsselraumes
- Durchsuchen eines reduzierten Schlüsselraumes (Wörterbuchangriff)
- Feste Bytefolgen bei Textverarbeitungen, bekannte Formatangaben von Datenbankfiles usw.
- negative Mustersuche
- Weitere Informationen über den Klartext ausnutzen: komprimierte Datei, ASCII-Text...
- Schwachpunkte der Implementierung nutzen: Abspeichern des Schlüssels an unsicherem Platz, Übertragen des Schlüssels im Klartext über unsicheres Netz,...

1.4 Angriffe auf Verschlüsselungsverfahren

Bei der Kryptanalyse geht es überwiegend um Methoden und Tricks, die es einem Angreifer ermöglichen, aus einem verschlüsselten Text wieder an den ursprünglichen Klartext zu gelangen. Ein Angreifer kann dabei auf verschiedene Arten vorgehen.

1.4.1 Ciphertext Only

Bei dieser Art von Angriffen steht dem Kryptanalytiker nur der Ciphertext zur Verfügung, um den Klartext zu gewinnen. Dies kann geschehen, indem der Schlüssel gefunden wird oder indem er einen Weg findet, um den Klartext auch ohne Schlüssel wiederherzustellen.

1.4.2 Known Plaintext

Bei *Known Plaintext* Angriffen steht dem Angreifer Wissen über den Klartext zur Verfügung. Dies kann z.B. daraus resultieren, dass Nachrichten immer mit einer festgelegten Einleitung beginnen oder dass der konkrete Inhalt einer Nachricht auf andere Weise dem Angreifer zur Kenntnis kommt. Dies kann ausgenutzt werden, um Informationen über den verwendeten Algorithmus und den Schlüssel zu gewinnen.

1.4.3 Chosen Plaintext Attacke

Bei *Chosen Plaintext* Angriffen hat der Kryptanalytiker zusätzlich die Möglichkeit, den Klartext, der verschlüsselt werden soll, selbst zu wählen. Dies kann geschehen, wenn der Angreifer direkten oder indirekten Zugriff auf das Verschlüsselungsgerät hat. Auf diese Weise lässt sich der Schlüssel, der verwendet wird, ermitteln.

1.4.4 Chosen Ciphertext

Ein *Chosen Ciphertext* Angriff ist das Gegenstück zum *Chosen Plaintext* Angriff. Hierbei hat der Angreifer die Möglichkeit den Ciphertext vorzugeben und aus dem resultierenden Klartext Rückschlüsse auf den Schlüssel zu ziehen.

1.4.5 Brute Force

Die einfachste Möglichkeit um einen Schlüssel zu finden und damit dann den Klartext zu entschlüsseln ist ein *Brute Force* Angriff. Dabei wird der gesamte Schlüsselraum durchsucht und jeder Schlüssel wird daraufhin untersucht, ob die Entschlüsselung einen sinnvollen Klartext ergibt.

1.4.6 Lineare Kryptoanalyse

Die Lineare Kryptanalyse ist ein *Known Plaintext* Angriff mit dem der Chiffrierschlüssel aufgedeckt werden kann. Hierbei werden die nichtlinearen Elemente des Algorithmuses durch lineare Funktionen approximiert. Mittels eines Klartext-Ciphertext-Paares lassen sich dann einige Bit des Schlüssels rekonstruieren und durch wiederholte Anwendung lässt sich schließlich der ganze Schlüssel für die Approximation des Algorithmus finden.

1.4.7 Differentielle Kryptoanalyse

Die differentielle Kryptanalyse ist eine *Chosen Plaintext* Attacke. Hierbei werden zwei Klartexte P und P' gewählt, die eine bestimmte Differenz ΔP haben. Wie diese Differenz berechnet wird, ist von dem Verschlüsseltungsalgorithmus abhängig. So ist bei DES diese Differenz über die XOR-Verknüpfung definiert.

Kapitel 2

Einführung in die DKA

Die differentielle Kryptanalyse wurde 1990 von den israelischen Mathematikern Biham und Shamir eingeführt. Sie fanden mit dieser Methode einen *Chosen Plaintext* Angriff gegen den *DES* (Data Encryption Standard).
Die differentielle Kryptoanalyse versucht aus Unterschieden im Klartext auf Unterschiede im verschlüsselten Text zu stossen, um so Rückschlüsse auf den Verschlüsselungsalgorithmus und den verwendeten Key k ziehen zu können. Das Verschlüsselungssystem muss jedoch vorliegen, da die einzelnen Schritte der Codierung analysiert werden sollen. Ist dies nicht möglich, so bleibt als Alternative die lineare Kryptoanalyse.
Die differentielle Kryptoanalyse ist seit 1990 bekannt. Erste Ansätze waren jedoch bereits 1985 erkennbar. Brisant ist jedoch, dass die Methode den Entwicklern von *DES* sehr wahrscheinlich bereits bekannt war (1974). Dies wird auch der Grund sein, warum die differentielle Kryptoanalyse nicht effizient auf den *DES* angewendet werden kann.

Kapitel 3

Systemanalyse von DES

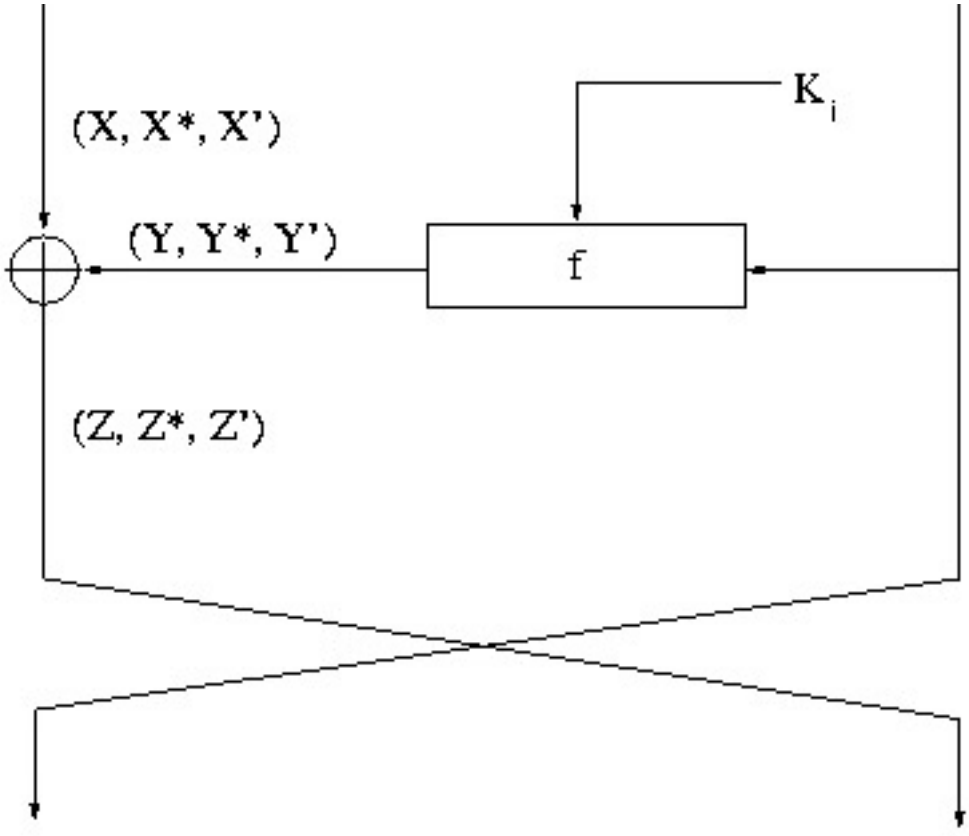
Für das folgende Beispiel wird angenommen, dass der Schlüssel immer gleich bleibt. Dieser Schlüssel kann jedoch frei gewählt werden.

3.1 Definitionen

(P, P^*)	Klartextpaar, jeweils nach der Eingangspermutation, die bei der DKA von DES keine Rolle spielt und deshalb nicht betrachtet wird.
$(P' = PxorP^*)$	"plaintext-xor", "Klartext-xor": Differenz der Klartexte P und P^*

Bei der differentiellen Kryptoanalyse werden die Differenzen mit xor berechnet.

3.2 Die äussere xor-Verknüpfung



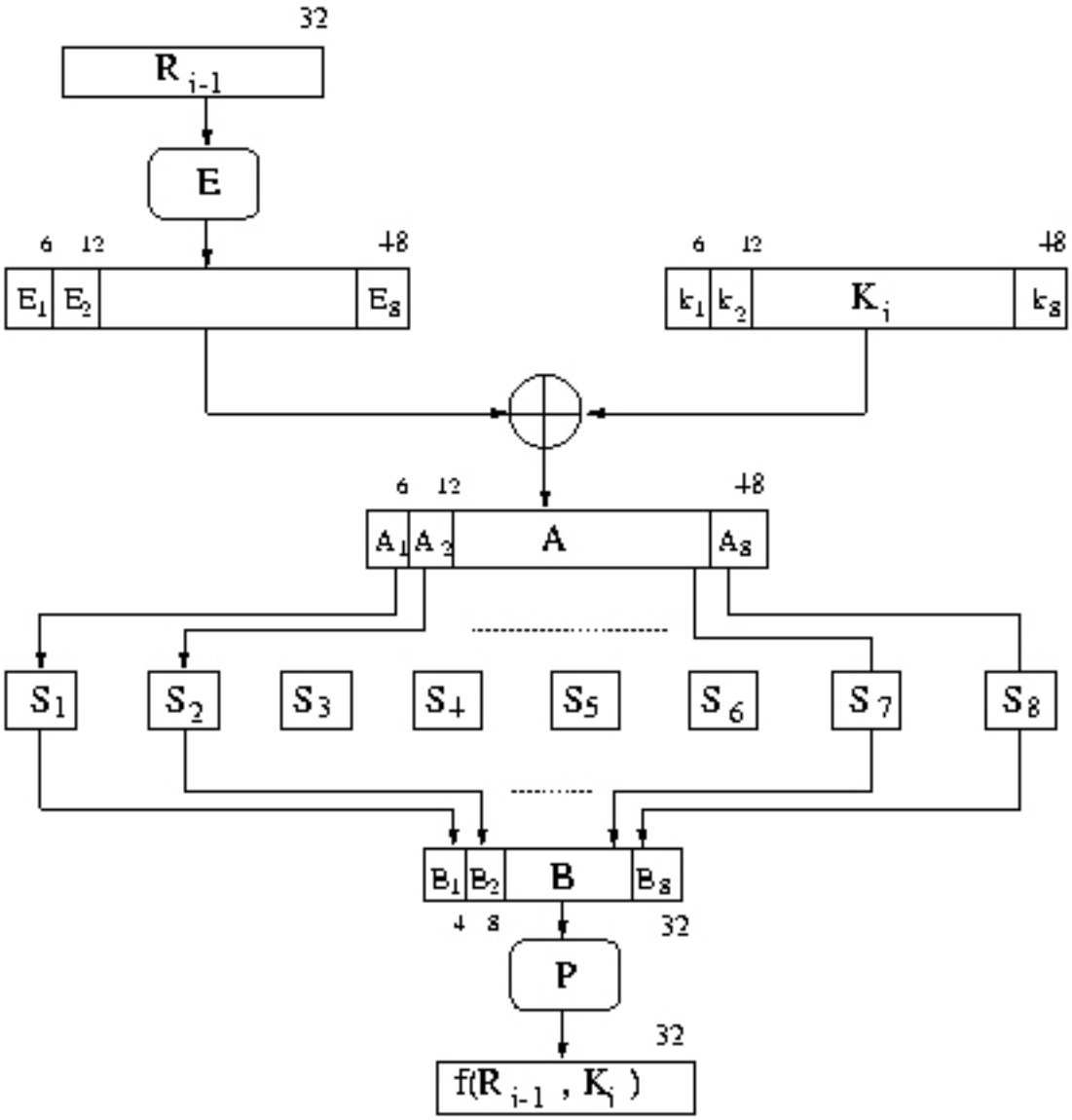
$$X' = X \oplus X^*$$

$$Y' = Y \oplus Y^*$$

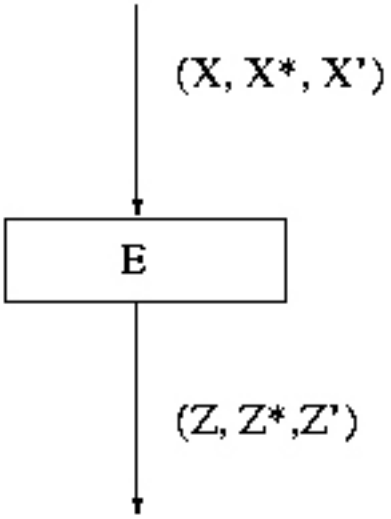
Für die resultierende Differenz gilt:

$$Z' = Z \oplus Z^* = (X \oplus Y) \oplus (X^* \oplus Y^*) = X \oplus X^* \oplus Y \oplus Y^* = X' \oplus Y'$$

3.3 Die f-Funktion



3.4 Die E-Expansion



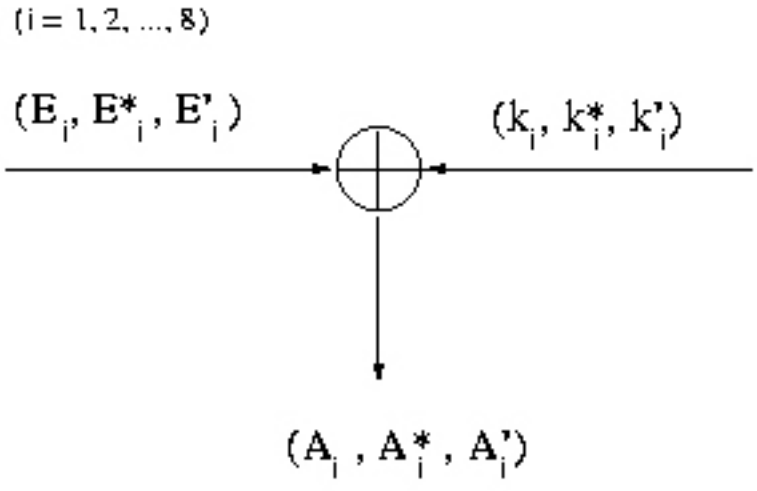
$$X' = X \oplus X^*$$

$$Z = E(X), Z^* = E(X^*)$$

Für die resultierende Differenz gilt:

$$Z' = Z \oplus Z^* = E(X) \oplus E(X^*) = E(X \oplus X^*) = E(X')$$

3.4.1 xor-Verknüpfung von expandierter Eingabe und Teilschlüssel



$$E'_i = E_i \oplus E^*_i$$

$$k_i = k^*_i$$
$$k'_i = k_i \oplus k^*_i = 0$$

$$A_i = E_i \oplus k_i$$

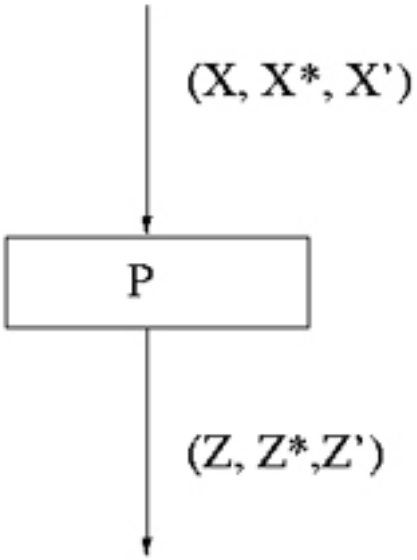
$$A^*_i = E^*_i \oplus k_i$$

Für die resultierende Differenz gilt:

$$A'_i = A_i \oplus A^*_i = E_i \oplus k_i \oplus E^*_i \oplus k_i = E_i \oplus E^*_i = E'_i$$

Das *input-xor* für die S-Boxen ist also **unabhängig vom Schlüssel**.

3.5 Die P-Permutation



Kapitel 4

Angriff auf einen Ein-Runden-DES

Das folgende Beispiel wird anhand einer DES Runde gezeigt. So könnte der Geheimschlüssel mit wenigen Klartext Geheimtextpaaren berechnet werden.

4.1 S-Box S1

Die entscheidende Rolle in der differentiellen Kryptoanalyse spielen die S-Boxen. Sie sind der einzige nicht lineare Teil des DES-Algorithmus.

S-Box S1, Spalten (0..15) und Zeilen (0..3)

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

4.2 Berechnung der Input-,Outputdifferenzen

Wir wählen zwei 6 Bit lange Inputstrings x und x^* mit fester Differenz

$$x' = x \oplus x^*$$

Wir wählen die feste Inputdifferenz von

$$x' = 110100$$

Interessant ist die Differenz des resultierenden Output zu berechnen:[1]

$$c' = S(x) \oplus S(x^*)$$

[1] $S(x)$ bedeutet S-Box angewandt auf x

Mit $x = 000000$ und x', bekommen wir $x^* = 110100$. Anwenden der S-Box auf x und x^* liefert

$$S(000000) = 14 \rightarrow 1110$$

$$S(110100) = 9 \rightarrow 1001$$

Die beiden äussersten Bits bestimmen die Zeile. Die übrigen Bits bestimmen eine Spalte in der S-Box. Im Falle $x^* = 110100$ wäre das die Zeile 2 und die Spalte 10. Aus der Tabelle der S-Box S1 kann nun die Zahl 9 ausgelesen werden. Die Output-Differenz ist dann

$$c' = 0111.$$

Die folgende Tabelle enthält für die 16 möglichen Output-Differenzen c' die zugehörigen Inputs (nur den linken Operanden x):

Output-xor	**Input x (Differenz 110100)**
0000	
0001	000011, 001111, 011110, 011111, 101010, 101011, 110111, 111011
0010	000100, 000101, 001110, 010001, 010010, 010100, 011010, 011011, 100000, 100101, 100110, 101110, 101111, 110000, 110001, 111010
0011	000001, 000010, 010101, 100001, 110101, 110110
0100	010011, 100111
0101	
0110	
0111	000000, 001000, 001101, 010111, 011000, 011101, 100011, 101001, 101100, 110100, 111001, 111100
1000	001001, 001100, 011001, 101101, 111000, 111101
1001	
1010	
1011	
1100	
1101	000110, 010000, 010110, 011100, 100010, 100100, 101000, 110010
1110	
1111	000111, 001010, 001011, 110011, 111110, 111111

Output-xor	Anzahl Input(x)
0000	0
0001	8
0010	16
0011	6
0100	2
0101	0
0110	0
0111	12
1000	6
1001	0
1010	0
1011	0
1100	0
1101	8
1110	0
1111	6

Interessant ist, dass nicht alle Output-xor gleich oft vorkommen. Einige Werte kommen sogar nicht vor. Diese Tatsache ist die Grundlage für die differentielle Kryptoanalyse auf den DES.

4.3 Known-Plain-Text Attack

Auf Basis der Inputdifferenz $x' = 110100$ wird nun einen *Known-Plaintext* Angriff durchgeführt. Ein Klartext sei $p = 000001$. Der andere Klartext ist dann notwendigerweise $p^* = p + 110100 = 110101$

4.3.1 Differenzbildung

Aus der Systemanalyse im vorangegangenen Kapitel, wissen wir, dass der Schlüssel k keinen Einfluss auf die Differenz hat:

$$x' = x \oplus x^* = p \oplus k + p^* \oplus k = p \oplus p^* = 110100$$

4.3.2 Geheimtext

Der Geheimtext sei $c' = 1101$. Aus der Tabelle kann man nun ablesen, welcher Input für diesen Output verantwortlich war. In diesem Falle muss es eine der folgenden 8 Zeichenketten sein:

Output-xor	Input x
1101	000110, 010000, 010110, 011100, 100010, 100100, 101000, 110010

Durch die *Known-Plaintext* Attacke wissen wir, dass folgender Text an der S-Box eingegeben wurde:

$$p \oplus k = 000001 \oplus k$$

Daraus folgt, dass $000001 \oplus k$ einer der 8 Zeichenketten sein muss.

4.3.3 Key k

Das Weitere ist nun einfach: Man wiederholt die *Known-Plaintext* Attacke mit unterschiedlichen Klartexten p und zwar solange, bis es nur noch eine einzige Zeichenkette gibt, die in allen resultierenden test-Mengen enthalten ist. Damit kann der gesuchte Key k ermittelt werden.

Kapitel 5

Angriff auf einen Mehr-Runden DES

Der Angriff auf den Ein-Runden-DES lässt sich notfalls auf zwei oder drei Runden ausdehnen. Für grössere Rundenzahlen kann man aber nur noch Wahrscheinlichkeitsaussagen machen. Im Folgenden wird die Vorgehensweise anhand eines zwei-Runden-DES gezeigt.

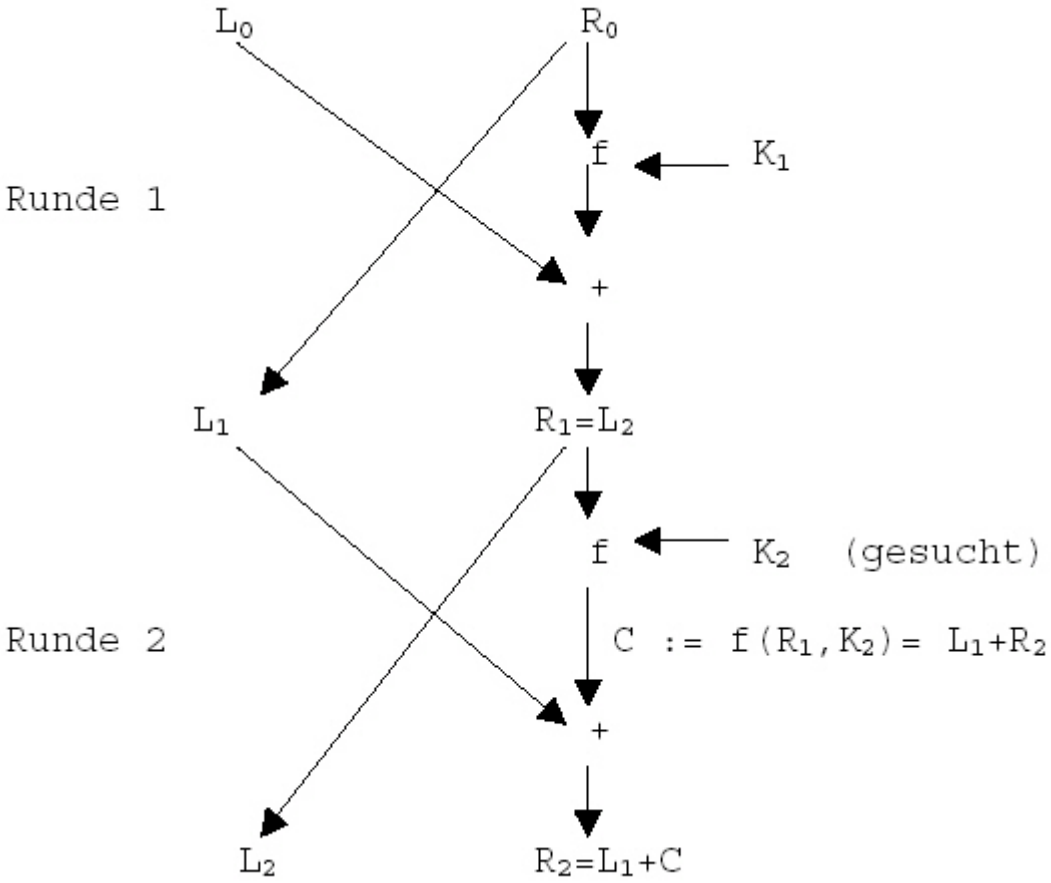
Bekannt seien zwei Klartexte

$$L_0R_0, L_0^*R_0^*$$

und die dazugehörigen Geheimtexte

$$L_2R_2, L_2^*R_2^*$$

Gesucht sind die 48 bit des letzten Rundenschlüssels K_2. Das folgende Bild zeigt die beiden Runden ausgehend von L_0R_0. (Analoges Bild für $L_0^*R_0^*$)



$R_1(= L_2)$ ist bekannt. R_1 ist im wesentlichen (d.h. abgesehen von einer Expansion) das, was nach xor mit K_2, an den 8 S-Boxen anliegt.
Analog kennt man R_1^* und damit kennt man auch R_1', d.h. man kennt Input und Inputdifferenz an den S-Boxen in Runde 2.

$C := f(R_1, K_2)$ (analog C^*) ist im wesentlichen (d.h. abgesehen von einer festen Permutation P) das, was aus den S-Boxen herauskommt. Falls man $C'(= C + C^*)$ kennen würde, so wäre man bei Runde 2 in der gleichen Situation wie beim Angriff auf den Ein-Runden-DES: Man kennt Input, Inputdifferenz und Outputdifferenz an den S-Boxen, und damit kann man mit Testmengen den Schlüssel herausbekommen. C (und analog C^*) kennt man aber nicht, da man L_1 nicht kennt. In diesem speziellen Falle ist $L1$ sehr wohl bekannt ($L_1 = R_0$). Aber das liegt daran, dass wir nur zwei Runden haben, und davon wollen wir keinen Gebrauch machen.

Die Idee beim probabilistischen Angriff ist: Man wähle die Inputdifferenz $L_0'R_0'$ in Runde 1 so, dass man die Outputdifferenz $L_1'R_1'$ mit hoher Wahrscheinlichkeit kennt.

5.1 Ein-Runden Charakteristik

Im vorangegangen Fall liefert die folgende Charakteristik das gewünschte Resultat mit der Wahrscheinlichkeit $p = 14/64$

$L'_0 = 00000000_{16}$	$R'_0 = 60000000_{16}$
$L'_1 = 60000000_{16}$	$R'_1 = 00808200_{16}$

Wenn der Input mit der in der oberen Zeile angegebenen Differenz in die Runde hineingeht, so resultiert am Ende der Runde mit der angegebenen Wahrscheinlichkeit die in der unteren Zeile notierte Outputdifferenz.

Mit der gleichen Wahrscheinlichkeit kennt man dann in Runde 2 die aus den S-Boxen herauskommende Outputdifferenz:

$$C' = L_1 + R_2 + L_1^* + R_2^* = L'_1 + R_2 + R_2^*$$

5.1.1 Erläuterungen zur Charakteristik

Gegeben sei

$$R'_0 = 60000000_{16}$$

binär wäre das

0110 0000 0000 0000 0000 0000 0000 0000

Die Expansion liefert die an den S-Boxen anliegenden Inputdifferenzen:

S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
001100	000000	000000	000000	000000	000000	000000	000000

Die Outputdifferenz der S-Boxen 2 bis 8 sind dann null. An der ersten S-Box liegt 001100 als Inputdifferenz an. Berechnete man die zu dieser Differenz gehörende Input-Output- Tabelle, so ist zu erkennen, dass die Outputdifferenz 1110 sehr häufig, nämlich in 14 (von 64) Fällen vorkommt.
Konsequenz: Die Outputdifferenz der S-Boxen ist

1110 0000 0000 0000 0000 0000 0000 0000

mit Wahrscheinlichkeit $p = 14/64$. Die letzte Aktion der Runde ist die Permutation P. Die bringt die ersten drei Bits an die Positionen 9,17 und 23:

0000 0000 1000 0000 1000 0010 0000 0000

Hexadezimal ist das

$$R'_1 = 00808200_{16}$$

5.2 Know-Plain-Text Attacke

Die Attacke läuft wie folgt ab:

- Man wählt zufällige Paare mit der Inputdifferenz $L'_0R'_0$
- Man bestimmt die Testmengen wie oben beschrieben und macht sich eine Streichliste der vorgeschlagenen Schlüssel.

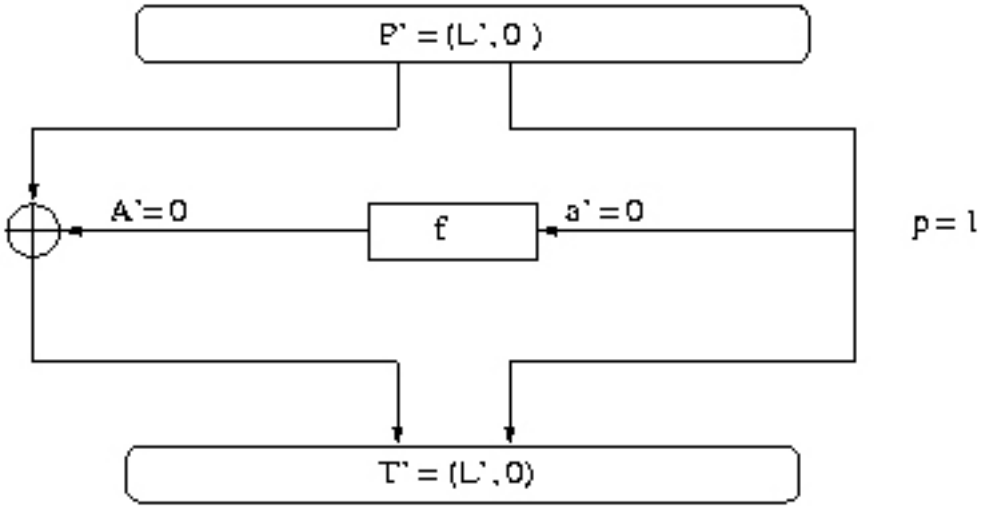
Mit Wahrscheinlichkeit $p = 14/64$ hat man *richtige Paare* bezüglich der Charakteristik gewählt mit der Folge, dass in diesen Fällen der richtige Schlüssel in den berechneten Testmengen stets dabei ist. Mit der Restwahrscheinlichkeit werden Testmengen und Schlüssel völlig zufällig erscheinen.
Insgesamt wird der richtige Schlüssel häufiger vorgeschlagen als die übrigen. Der am häufigsten vorgeschlagene Schlüssel ist in diesem Beispiel K_2.

Kapitel 6

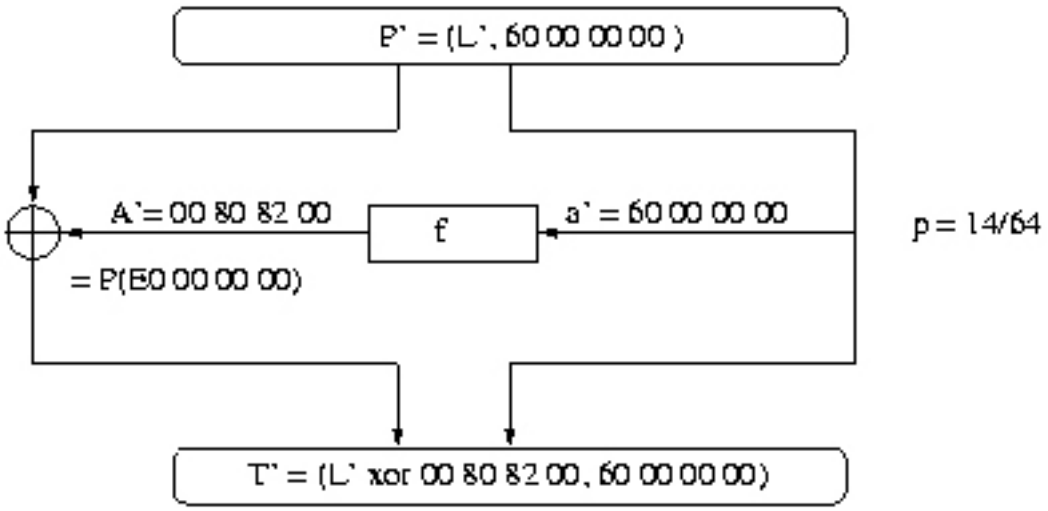
Charakteristiken

Eine Charakteristik beschreibt schrittweise die auftretenden Differenzen von Runde zu Runde. Einer Charakteristik kann eine Wahrscheinlichkeit zugeordnet werden. Dabei geht man normalerweise davon aus, dass die Rundenschlüssel $k[i]$ zufällig und voneinander unabhängig sind. Bekannt ist auch der Begriff des Differentials, der sich aus vielen Charakteristiken zusammensetzen kann. Ein Differential wird durch die Eingabe- und die Ausgabedifferenz beschrieben, ohne Betrachtung der Zwischenwerte.

6.1 Ein-Runden Charakteristik



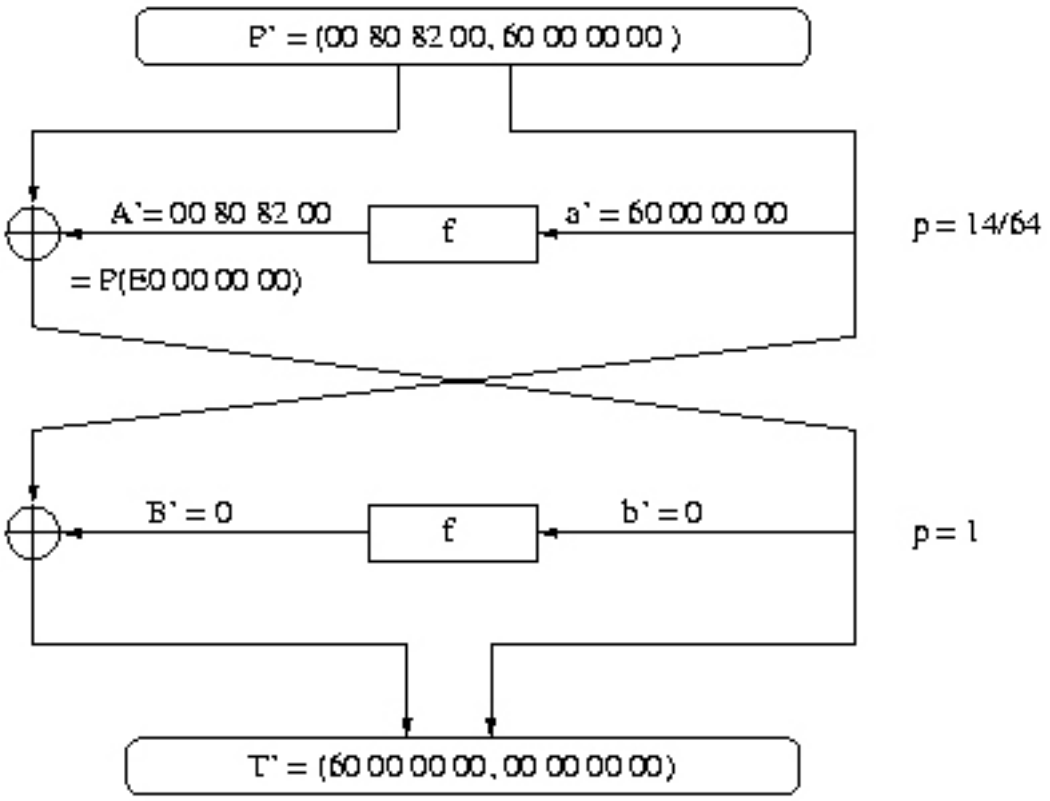
Diese Charakteristik ist die einzige mit $p > 1/4$. [2]



$$p = 14/64$$

Es gibt zwei Möglichkeiten von Ein-Runden Charakteristiken. Im ersten Fall werden die Klartexte so gewählt, dass die Outputdiffernz gleich wie die Inputdifferenz bleibt. Das heisst, die Charakteristik kommt mit der Wahrscheinlichkeit 1 durch das System. Im zweiten Fall ist die bereits bekannte variante der Tabellenbildung bei die gewünschte Charakteristik mit der Wahrscheinlichkeit $p = 14/64$ durch das System kommt.

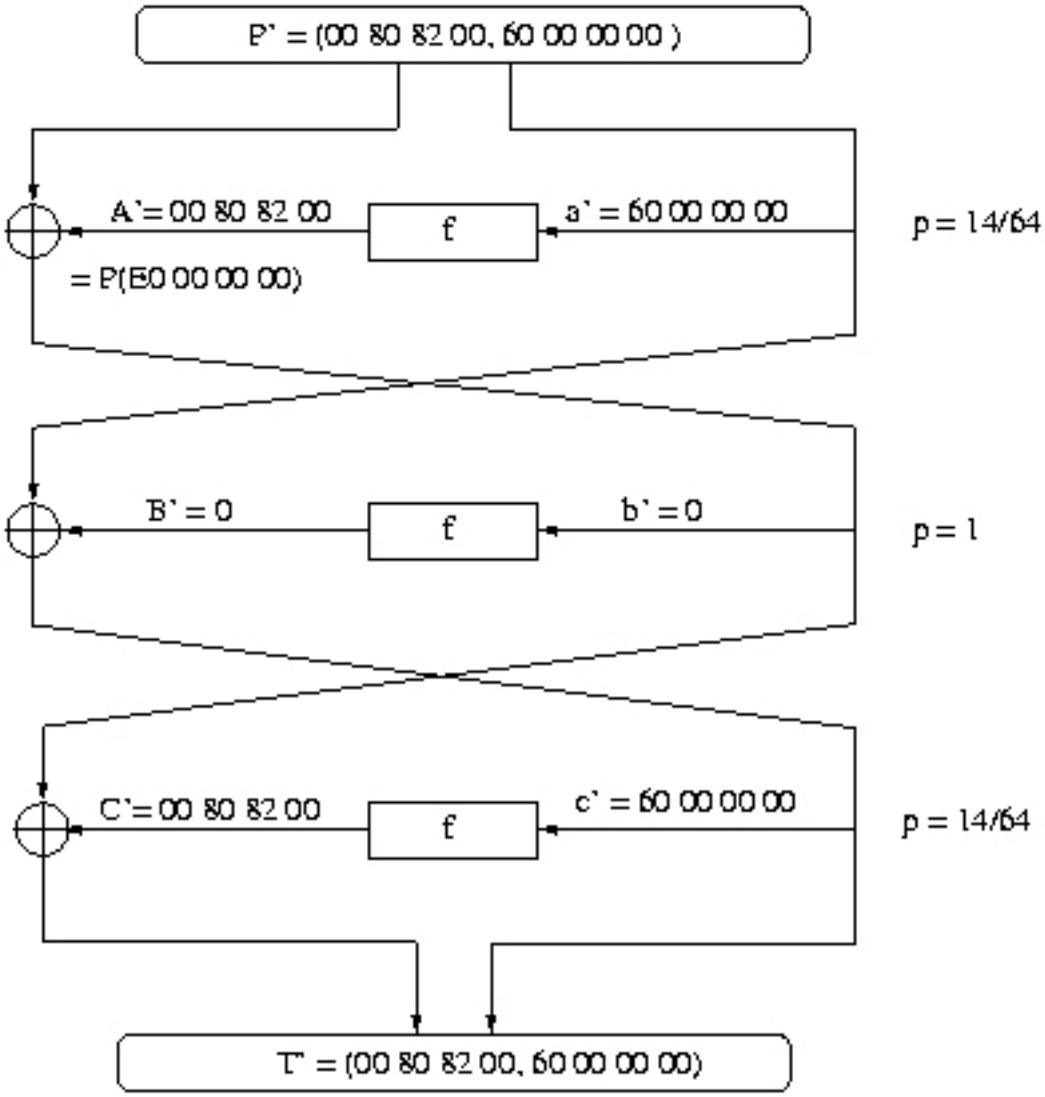
6.2 Zwei-Runden Charakteristik



$$p = 14/64$$

Diese Zwei-Runden-Charakteristik ist offensichtlich eine Kombination der beiden Ein-Runden-Charakteristiken. Die Wahrscheinlichkeit der Charakteristik ergibt sich bei den Voraussetzungen als Produkt der Wahrscheinlichkeiten der Ein-Runden-Charakteristiken.

6.3 Drei-Runden Charakteristik



$$p = (14/64)^2$$

6.4 Wahrscheinlichkeit

Eine n-Runden Charakteristik ist gleich aufgebaut wie die bereits erwähnten. Entscheidend ist, dass die Differenz mit einer bestimmen Wahrscheinlichkeit durch das System durchkommt. Die Wahrscheinlichkeiten der einzelnen Schritte

werden mitgenommen. Für eine ungerade Anzahl von Runden lässt sich die Wahrscheinlichkeit wie folgt ausdrücken:

$$p(r) = p^{(r-1)/2}$$

Anzahl Runden r	Wahrscheinlichkeit
3	$1/2^{7.9}$
5	$1/2^{15.7}$
7	$1/2^{23.6}$
9	$1/2^{31.5}$
11	$1/2^{39.4}$
13	$1/2^{47.2}$
15	$1/2^{55.1}$
17	$1/2^{63}$

Entscheidend ist, dass man bei 15 Runden schon mehr als 2^{55} geeignete Differenzen braucht, um die Charakteristik auch nur ein mal durchzubekommen.

6.4.1 Biham und Shamir

Für die 16 Runden des *DES* benötigt man laut Biham und Shamir 2^{60} ausgewählte Klartexte um den Schlüssel k herauszufindenen.

Runden	# ausgewählte Klartexte bei unabhängigen Schlüsseln	# ausgewählte Klartexte bei abhängigen Schlüssel
4	16	8
6	256	256
8	2^{16}	2^{14}
16	2^{60}	2^{47}

Kapitel 7

Fazit

Biham und Shamir zeigen mit der differentiellen Kryptoanalyse einen weiteren Ansatzpunkt, um Verschlüsselungsverfahren zu testen. Im Falle des DES zeigt sich, dass dieser dem Verfahren stand halten kann. Die Effizienz der DKA ist hier sehr schlecht. Um nach den 16 Runden des DES Algorithmus des Schlüssel k herauszubekommen, bräuchte es mit dem DKA Verfahren rund 2^{60} ausgewählte Klartexte. Somit wäre der Aufwand sogar noch grösser als mit einer einfachen *Brute-Force* Attacke, da der Schlüssel des DES nur 56 bit lang ist. Das bedeutet, dass der DES gegen die DKA sicher ist.

In der Praxis wird dieses Verfahren wohl nicht angewandt werden. Es ist jedoch eine interessante Grundlage, um ein Verschlüsselungsverfahren auf seine Sicherheit zu testen. Die differentielle Kryptoanalyse lässt sich nicht nur auf den DES anwenden. Auch für andere Algorithmen wird die DKA benutzt, um die Sicherheit der jeweiligen Verfahren zu testen.

Teil I

Anhang

Literaturverzeichnis

[1] **Heys, Howard M.** *Linear and Differential Cryptoanalysis.* Electrical and Computer Engineering Faculty of Engineering and Applied Science, Memorial University of Newfoundland St. John's, NF, Canada

[2] **Gerold, Anton** *Neue Methoden der Kryptanalyse*
http://home.in.tum.de/~gerold/aktvorl20012002/dka.html
Stand 05.05.2002 18

[3] **Lipmaa, Helger** *Differential cryptanalysis*
http://www.tcs.hut.fi/~helger/crypto/link/block/dc.html
Stand 05.05.2002

[4] **NEC Research Institute** *On Matsui's Linear Cryptanalysis (1994)*
http://citeseer.nj.nec.com/biham94matsuis.html
Stand 05.05.2002

[5] **Bandouch, Jan** *Shared Key Kryptographie (DES, IDEA) und PGP)*
http://wwwbrauer.in.tum.de/seminare/web/WS0001/vortrag09.html#des
Stand 05.05.2002

[6] **Lucks, Stefan** *Vorlesung: Kryptographie (WS 1998/99)*
http://th.informatik.uni-mannheim.de/People/Lucks/Vorl/vorl.html
Stand 05.05.2002