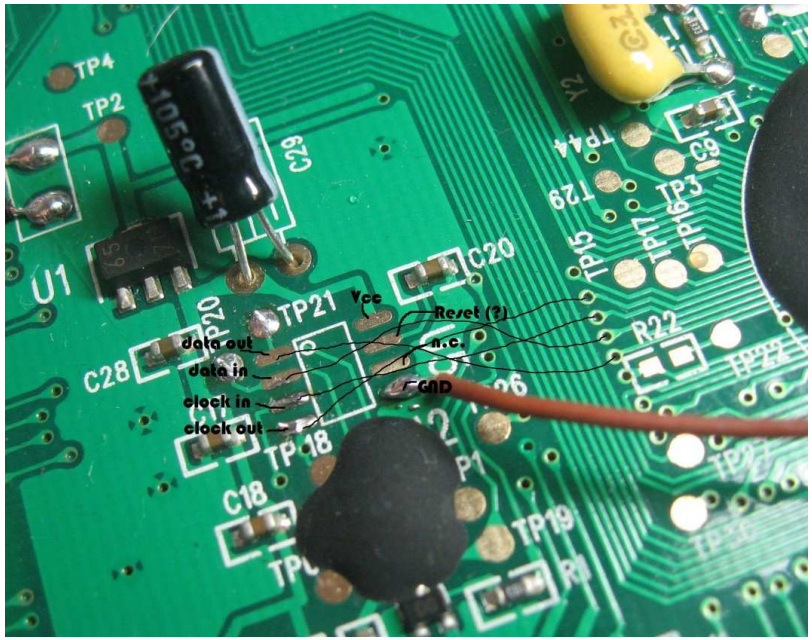
Crypto Algorithmus



Open now !

Beschreibung und Ablauf in der Übersicht

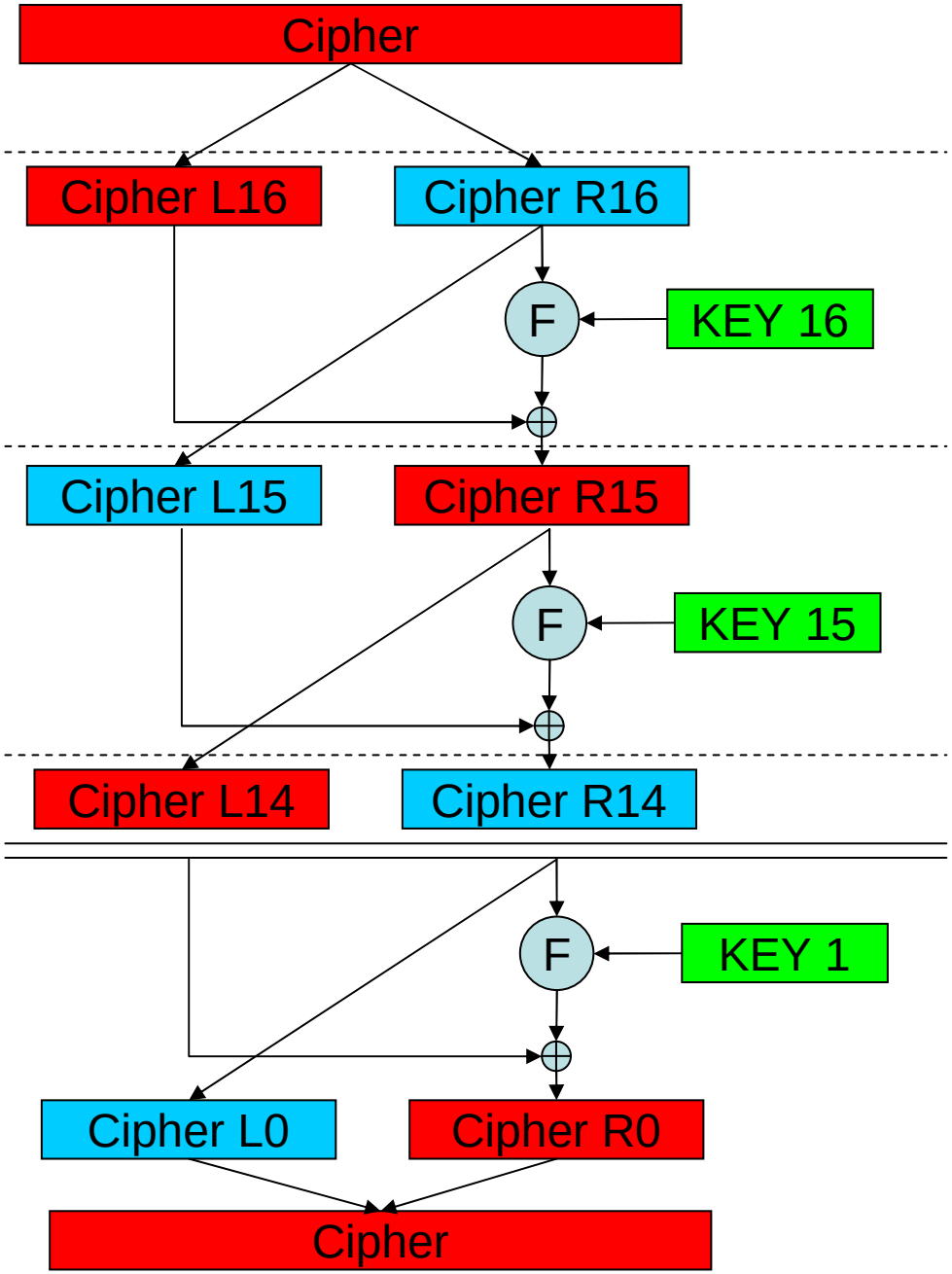
- Es werden 82 Bit eingelesen, Bit 0 und 7 werden verworfen
- Die ersten 40 Bit sind der Cipher, die zweiten 40 Bit die Zeit
- Bei dem Algorithmus handelt sich um einen DES, der auf 40 Bit angepasst wurde. Normal sind es 56 Bit
- Entsprechend gibt es 5 S-Boxen anstelle der üblichen 8
- Eingangs-, Schluß- sowie Schlüssel-permutation entfallen
- Der Schlüssel ist der angehängte Zeitstempel
- Ein gültiges Plain wird an dem Wert 0x2501 erkannt
- 2 Bit aus Plain konnte ich noch nicht zuordnen
- Es sieht so aus, als ob es keine Redundanz Informationen gibt
- Der PIC führt den Algorithmus 41 mal aus, wobei fortlaufend ein Bit der Cipher Daten gekippt wird. Ein „Fehlerkorrektur“ findet aber nicht statt (obwohl es mit diesem Mechanismus möglich wäre)
- Der Code aus den ersten 64 Worte des PIC sind zur Berechnung des Plain nicht nötig

Schlüssel Erzeugung und „ *f* “

- Der Schlüssel (die 40 Bit Zeit) werden in zwei Teile zu je 20 Bit geteilt
- Zu Begin jeder Runde werden die beiden 20-Bit Zeiten jeweils nach rechts geschoben. Dabei wird das unten heraus fallende Bit oben wieder eingeschoben
- In den Runden 16, 8, 7 und 3 zwei mal, in den restlichen Runden ein mal (insgesamt 20 mal). Es wird mit Runde 16 begonnen. Ähnlich wird auch beim DES vorgegangen
- Aus den 40 Zeit Bits werden von festen Positionen 30 Bit entnommen (Equivalent zur **Kompressions-Permutation** oder **Schlüsselauwahl** des DES) ⇨Ki (Rundenschlüssel)
- R der Cipher Daten durchläuft eine **Expansions Permutation** (20 Bit -> 30 Bit)
- Expandiertes R und Ki werden nun **XOR** verküpft (DES konform)
- Mit den 5 **S-Boxen** werden aus den 5 mal 6 Bit wieder 5 mal 4 Bit (= 20 Bit) gemacht
- Es folgt die **P-Box Permutation** (Verwürfelung)
- Die so gewonnenen 20 Bit werden XOR mit L der Cipher Daten verknüpft (L‘)
- Abschließend wird L‘ zu R und R zu L der nächsten Runde

Zusammenfassung

- Beim DES wird normalerweise nur der Schlüssel geheim gehalten, der Algorithmus, die S-Boxen und die Permutationen sind bekannt
- Bei Meteotime-Algorithmus ist es genau umgekehrt: der Schlüssel wird öffentlich übertragen, der Algorithmus, die S-Boxen und die Permutationen werden geheim gehalten
- Es gibt extra Design Regel für die S-Boxen
- Da S-Boxen und Permutationen wurden anscheinend neu gemacht. Dadurch, dass diese nicht bekannt sind (und somit kein Aussenstehender „drüber geschaut“ hat) besteht die Möglichkeit, dass dort Schwächen sind
- In wie fern die Sicherheit durch Veröffentlichung S-Boxen oder der Permutationsmechanismen gefärdet wird, kann ich nicht abschätzen



Cypher

Runde 16

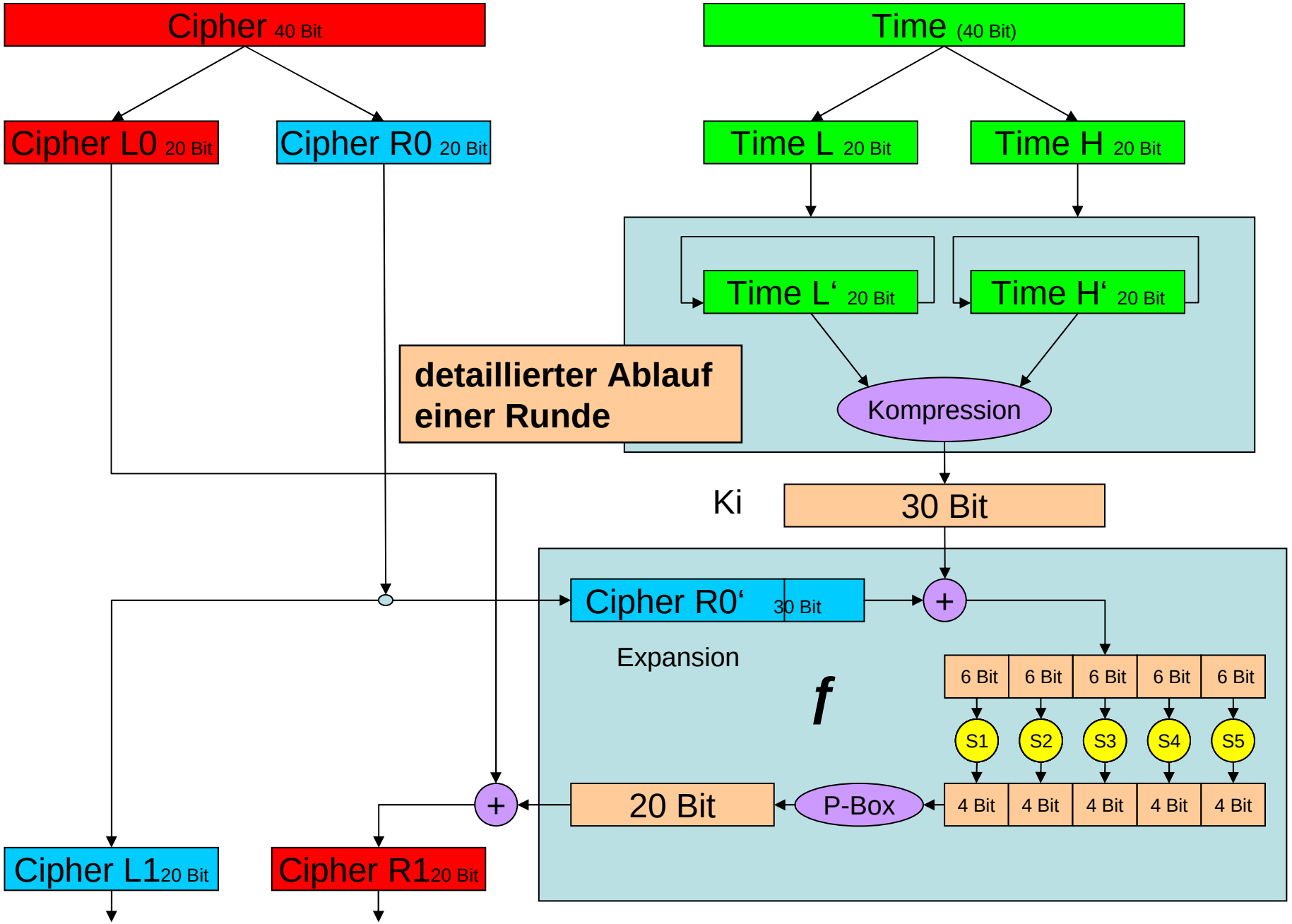
Runde 15

Runde 1

Plain

Grundsätzlicher Ablauf des DES

(ohne Eingangs- und Schluss-permutation)


Cipher 40 Bit
Time (40 Bit)
Cipher L0 20 Bit
Cipher R0 20 Bit
Time L 20 Bit
Time H 20 Bit
Time L‘ 20 Bit
Time H‘ 20 Bit
detaillierter Ablauf einer Runde
Kompression
Ki
30 Bit
Cipher R0‘ 30 Bit
+
Expansion
f
6 Bit
6 Bit
6 Bit
6 Bit
6 Bit
S1
S2
S3
S4
S5
+
20 Bit
P-Box
4 Bit
4 Bit
4 Bit
4 Bit
4 Bit
Cipher L1 20 Bit
Cipher R1 20 Bit

…und danke für den Fisch…