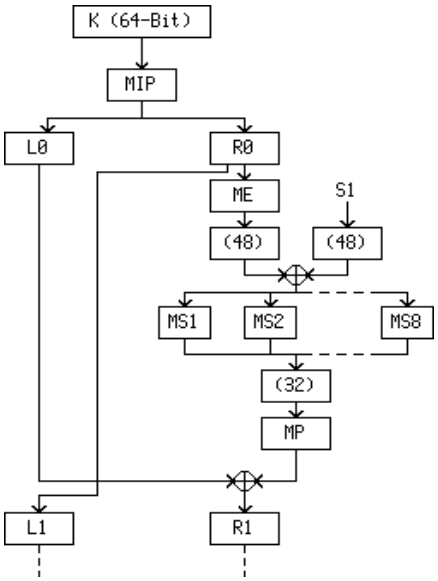
Zum DES-Verschlüsselungsverfahren (Data Encryption Standard)

Obwohl das DES-Verfahren inzwischen – vor allem wegen der geringen Schüssellänge von 56 Bit – gegen Brute Force-Angriffe nicht mehr sicher genug ist, lohnt es sich trotzdem, einen Blick darauf zu werfen, weil der DES

- die seit der Freigabe im Jahr 1977 viele Jahre international eingesetzte und bewährte Lösung bot,
- Strukturen nutzt, die auch im modernen AES-Ablauf enthalten sind (z. B. das Verschlüsseln in mehreren gleichartigen Runden oder das Vertauschen und Ersetzen der Klartextzeichen durch Permutationen und Substitutionen),
- weiterhin in der Variante des Triple-DES seinen Dienst tut.

Der DES verschlüsselt Klartextblöcke der Länge **64 Bit** und bildet dafür in jeder der 16 Runden aus dem **56 Bit** langen Hauptschlüssel 16 verschiedene Rundenschlüssel S1, S2, … , S16 jeweils der Länge **48 Bit**. Da der Ablauf in der Vorlesung durchgesprochen wurde, sind im Folgenden nur einige Angaben als Erinnerungshilfe gemacht.

Runde Nr. 1 hat diese Struktur:



MIP:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

MP:

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

ME:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

- Der Klartext durchläuft die Initialisierungs-Permutation MIP. Dabei erhält das Bit 58 den Platz 1, Bit 50 den Platz 2 usw.
- Die so vertauschten Bits werden in die 32-Bit-Blöcke L0 und R0 geteilt und dem dargestellten Ablauf gemäß weiter behandelt.
- Die Bits von R0 werden gemäß Tabelle ME vertauscht und teilweise verdoppelt: Bit 32 erhält Platz 1 usw., Bit 4 kommt auf Platz 5 **und** Platz 7, Bit 5 auf Platz 6 **und** 8 usw., es entsteht ein 48 Bit-Block.
- Der 48-Bit-Block wird mit dem ersten Teilschlüssel S1 verschlüsselt und das Ergebnis in 8 Blöcke zu je 6 Bit aufgeteilt.
- Jeder der 8 Blöcke erhält eine neue Wertzuweisung durch die entsprechende Substitutionstabelle MS1, MS2, …., MS8.

  Dabei passiert Folgendes (hier sind nur die ersten vier Tabellen angegeben):

MS1:

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

MS2:

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

MS3:

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

MS4:

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

Die 4 Zeilen erhalten die Nummern 0, 1, 2 und 3, die 16 Spalten die Nummern 0 bis 15. Hat der Block 1 z. B. das Bitmuster 110100_2 , so bestimmen die beiden äußeren Bits als Binärzahl 2_{10} die Zeilennummer, die 4 inneren Bits als 10_{10} die Spaltennummer. Dort steht die Zahl 12_{10} , die nun wegen der binär dargestellte Substitution 1100_2 als 4-Bit-Block die Operation verlässt.

- Die 4-Bit-Blöcke werden zu einem 32-Bit-Block zusammengefasst, durchlaufen die Permutation MP und addieren sich Modulo 2 (= XOR) mit dem Block L0.
- Dieser 32-Bit-Block bildet den neuen rechten Block R1 für die Runde 2, R0 stellt den neuen linken Block L1.
- Die nächsten Runden verlaufen bis auf die Behandlung mit MIP gleich, jedes mal wird allerdings mit einem anderen dazugehörigen Teilschlüssel S2, S3, …., S16 verschlüsselt.
- Nach der Runde 16 erfolgt am 64-Bit-Block die zu MIP inverse Permutation MIP

MIPI:

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

welche deren Permutation (an inzwischen ganz anderen Bits) rückgängig macht. Würde man beide Permutationen direkt hintereinander ausführen, würde wieder der eingegebene 64-Bit-Block herauskommen. Damit liegt der 64-Bit-Geheimtextblock vor.

- Die Teilschlüsselerzeugung verläuft ähnlich, wird hier aber nicht aufgeführt.
- Zur Entschlüsselung wird jeder 64-Bit-Geheimtextblock im zuvor beschriebenen Ablauf zum Klartext „verschlüsselt“ wobei nur die Reihenfolge der Teilschlüssel in S16, S15, ….., S1 umzukehren ist.

Man kann vielleicht ahnen, dass ein Angriff zur Klartextermittlung ohne Schlüssel bei diesen vielen Operationen nicht einfach sein wird (was aber eine gefühlsmäßige, sehr unbestimmte Feststellung ist und sich daher für fundierte Aussagen zur Sicherheit nicht eignet!).

Am **Beispiel** eines Null-Klartext-Blocks und eines Null-Schlüssels kann man versuchen, sich einen Eindruck zu verschaffen:

- Verschlüsselung:

```
K (ASCII):      ▪       ▪       ▪       ▪       ▪       ▪       ▪       ▪
K (BINÄR):   00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

K (perm.):   00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Teil-G:
 1           00000000 00000000 00000000 00000000 11011000 10011000 11001011 10111100
 2           11011000 10011000 11001011 10111100 11110010 00110010 11001101 11011011
 3           11110010 00110010 11001101 11011011 10101000 10111000 10101111 00101100
 4           10101000 10111000 10101111 00101100 01000001 11001111 01111100 00001110
 5           01000001 11001111 01111100 00001110 00000111 11101100 10011100 01001001
 6           00000111 11101100 10011100 01001001 10001001 11010110 11010101 00011110
 7           10001001 11010110 11010101 00011110 10010101 01101110 00001001 00101100
 8           10010101 01101110 00001001 00101100 10011010 01000010 11100110 10000111
 9           10011010 01000010 11100110 10000111 01000110 10101011 00101111 11011010
10           01000110 10101011 00101111 11011010 00000011 01001100 11110000 10000111
11           00000011 01001100 11110000 10000111 10100101 00100010 10100001 11000100
12           10100101 00100010 10100001 11000100 10111011 00101111 00010010 01001111
13           10111011 00101111 00010010 01001111 11110001 10010001 00010010 01011100
14           11110001 10010001 00010010 01011100 10101101 11000101 10101010 11000110
15           10101101 11000101 10101010 11000110 01100111 01001010 11101010 00110100
16           01100111 01001010 11101010 00110100 10100100 00110101 10000101 11010101

G:           10010101 10101000 11010111 00101000 00010011 11011010 10101001 01001101
G (ASCII):      ▪        ¨        ×        (        ▪        Ú        ▪        M
```

  Trotz des Null-Klartextblockes und desNull-Schlüssels entsteht ein von Null verschiedener Geheimtext.

- Entschlüsselung:

```
K (ASCII):      ▪        ¨        ×        (        ▪        Ú        ▪        M
K (BINÄR):   10010101 10101000 11010111 00101000 00010011 11011010 10101001 01001101

K (perm.):   10100100 00110101 10000101 11010101 01100111 01001010 11101010 00110100

Teil-G:
 1           01100111 01001010 11101010 00110100 10101101 11000101 10101010 11000110
 2           10101101 11000101 10101010 11000110 11110001 10010001 00010010 01011100
 3           11110001 10010001 00010010 01011100 10111011 00101111 00010010 01001111
 4           10111011 00101111 00010010 01001111 10100101 00100010 10100001 11000100
 5           10100101 00100010 10100001 11000100 00000011 01001100 11110000 10000111
 6           00000011 01001100 11110000 10000111 01000110 10101011 00101111 11011010
 7           01000110 10101011 00101111 11011010 10011010 01000010 11100110 10000111
 8           10011010 01000010 11100110 10000111 10010101 01101110 00001001 00101100
 9           10010101 01101110 00001001 00101100 10001001 11010110 11010101 00011110
10           10001001 11010110 11010101 00011110 00000111 11101100 10011100 01001001
11           00000111 11101100 10011100 01001001 01000001 11001111 01111100 00001110
12           01000001 11001111 01111100 00001110 10101000 10111000 10101111 00101100
13           10101000 10111000 10101111 00101100 11110010 00110010 11001101 11011011
14           11110010 00110010 11001101 11011011 11011000 10011000 11001011 10111100
15           11011000 10011000 11001011 10111100 00000000 00000000 00000000 00000000
16           00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

G:           00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
G (ASCII):      ▪        ▪        ▪        ▪        ▪        ▪        ▪        ▪
```

Die beiden wesentlichen **Schwachpunkte**:

- Die mit den 56 signifikanten Schlüsselbits zu geringe Schlüssellänge fordert beim heutigen Stand der Technik erfolgversprechende Brute Force-Angriffe heraus, die auch bereits getätigt wurden.
- Die monoalphabetische Verschlüsselung eines Klartextes mit immer demselben Schlüssel ist prinzipiell anfällig gegen Angriffe mithilfe der statistischen Kryptoanalyse, da gleiche Klartext-Blöcke immer gleiche Geheimtext-Blöcke ergeben.