

Vorbemerkung: Die Bits werden einheitlich wie folgt dargestellt:

Bit 0 = Index 1; Bit 1 = Index 2; Bit 4 = Index 5.

Das Schieben der Register erfolgt von Index: 1 nach 5.

Die Schritte entsprechen den kommenden Additionsreihen (Wurmfolgen) aus der Komplizierungseinheit.

Chiffrieren:

- Schritt 1 ... 5
Register SRV2 und SRV3 nicht im Rekursionsbetrieb!
Schieben der ersten Additionsbit (Wurmreihe) in das Register SRV2
Inhalt des SRV2 = $a_5; a_4; \dots a_1$.
Füllen des Registers SRV3 mit 11111
- Schritt 6
Rekursiver Durchlauf des Inhaltes des SRV2 und SRV3 (siehe Tabelle 1, s.u.)
Ist zu Anfang SRV2 = 00000 oder 11111 nicht taktet, weiter mit Schritt 7 ... 11,
ansonsten durchtaktet bis SRV2 = 11111 ist;
Beispiel: Bitfolge 10101 im SRV2 (dez. 21 = Pos.14)
jetzt schieben bis SRV2 = 11111 ist. Also von Pos.14 bis Pos.1.
Das sind 18 Takte, das wird in X zwischengespeichert.
 X = Anzahl der Taktung im Schritt 6 (hier im Bsp.: $X = 18$)
SRV3 ist durch das gleichzeitige Schieben im Rekursionsbetrieb ein
Symmetriewert $a_5^*; a_4^*; a_3^*; a_2^*; a_1^*$ gebildet.
Hier im Beispiel ist aus SRV3 = 11111 nun 00001 (dez. 1 = Pos.19) geworden.
Das Bit a_6 der Wurmreihe wird nicht genutzt!
- Schritt 7 ... 11
Register SRV2 und SRV3 nicht im Rekursionsbetrieb!
Schieben des Inhaltes des Registers SRV3 in das Register SRV2
Inhalt SRV2 = $a_5^*; a_4^*; a_3^*; a_2^*; a_1^*$
SRV3 wird jetzt mit Klartextbit k_1 XOR Additionsbit $a_7; \dots k_5$ XOR a_{11} ;
gefüllt.
Inhalt SRV3 = $k_5 \otimes a_{11}; k_4 \otimes a_{10}; k_3 \otimes a_9; k_2 \otimes a_8; k_1 \otimes a_7$.
oder auch als Zwischeneinheit benannt: $SRV3 = Z_5; \dots Z_1$.
- Schritt 12
keine Aktivitäten. a_{12} wird nicht genutzt.
- Schritt 13
Wie Schritt 6 nur mit den jetzt geladenen Symmetriewerten.
Rekursiver Durchlauf des Inhaltes des SRV2 und SRV3 (siehe Tabelle 1)
Ist SRV2 = 11111 keine Taktung, 00000 kann nicht vorkommen siehe Tabelle 1.
Hier ist jetzt nicht X sonder Y die Zählvariable.
Die Z im SRV3 wird mitgetaktet.
Das Ergebnis im SRV3 ist dann der verschlüsselte Klartext $G_5; \dots G_1$.
Bei SRV2 = 11111 ist $G_n = Z_n$.
 a_{13} wird nicht genutzt.
- Schritt 14 gehe zu Schritt 1 ...; a_{14} entspricht dann a_1 .

Die mathematische Darstellung des Chiffrierens lautet: $G_j = (K_j \text{ xor } B_j) * M^r_j$

<i>Bit 1</i>	<i>Bit 2</i>	<i>Bit 3</i>	<i>Bit 4</i>	<i>Bit 5</i>	<i>Rekursionsbit aus Bit 3 XOR Bit 5</i>	<i>Hex.</i>	<i>Dez.</i>	<i>Pos.</i>
0	0	0	0	0	0	0	0	0
1	1	1	1	1	0	1F	31	1
0	1	1	1	1	0	1E	30	2
0	0	1	1	1	0	1C	28	3
0	0	0	1	1	1	18	24	4
1	0	0	0	1	1	11	17	5
1	1	0	0	0	0	03	3	6
0	1	1	0	0	1	06	6	7
1	0	1	1	0	1	0D	13	8
1	1	0	1	1	1	1B	27	9
1	1	1	0	1	0	17	23	10
0	1	1	1	0	1	0E	14	11
1	0	1	1	1	0	1D	29	12
0	1	0	1	1	1	1A	26	13
1	0	1	0	1	0	15	21	14
0	1	0	1	0	0	0A	10	15
0	0	1	0	1	0	14	20	16
0	0	0	1	0	0	08	8	17
0	0	0	0	1	1	10	16	18
1	0	0	0	0	0	01	1	19
0	1	0	0	0	0	02	2	20
0	0	1	0	0	1	04	4	21
1	0	0	1	0	0	09	9	22
0	1	0	0	1	1	12	18	23
1	0	1	0	0	1	05	5	24
1	1	0	1	0	0	0B	11	25
0	1	1	0	1	0	16	22	26
0	0	1	1	0	1	0C	12	27
1	0	0	1	1	1	19	25	28
1	1	0	0	1	1	13	19	29
1	1	1	0	0	1	07	7	30
1	1	1	1	0	1	0F	15	31
1	1	1	1	1	Pos. 1	1F	1	Pos.1

Besonderheit



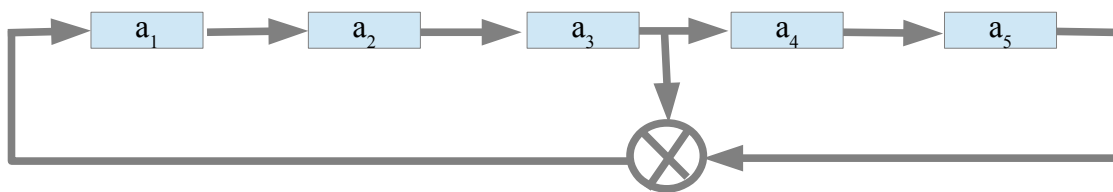
Tabelle 1: Rekursionsregister SRV2 und 3.

Dechiffrieren:

- Schritt 1 ... 5
Register SRV2 und SRV3 nicht im Rekursionsbetrieb!
Schieben der ersten Additionsbit (Wurmreihe) in das Register SRV2
Inhalt des SRV2 = $a_5; a_4; \dots a_1$. / Gebildet aus der Synchronfolge der Komplizierungseinheit.
Füllen des Registers SRV3 mit dem empfangenen Chiffirat, $G_5; \dots G_1$.
- Schritt 6
rekursiver Durchlauf des Inhaltes des SRV2 und SRV3 (siehe Tabelle 1, s.o.)
Ist zu Anfang SRV2 = 00000 oder 11111 nicht takten, weiter mit Schritt 7 ... 11,
ansonsten durchtakten bis SRV2 = 11111 ist;
Beispiel: Bitfolge 10101 im SRV2 (dez. 21 $\equiv$ Pos.14)
jetzt schieben bis SRV2 = 11111 ist. Also von Pos.14 bis Pos.1.
Das sind 18 Takte, das wird in X zwischengespeichert.
 X = Anzahl der Taktung im Schritt 6 (hier im Bsp.: $X = 18$)
SRV3 ist durch das gleichzeitige Schieben im Rekursionsbetrieb der
Zwischenwert $Z_5; Z_4; Z_3; Z_2; Z_1$ gebildet.
 a_6 wird nicht genutzt.
- Schritt 7 ... 11
Register SRV3 nicht im Rekursionsbetrieb!
Inhalt SRV2 ist hier nicht mehr relevant, hat jetzt immer den Inhalt 11111
SRV3 wird jetzt Z_n ausgelesen dann mit $Z_1 \text{ XOR } a_7; \dots Z_5 \text{ XOR } a_{11}$;
gefüllt.
Inhalt SRV3 = $Z_5 \otimes a_{11}; Z_4 \otimes a_{10}; Z_3 \otimes a_9; Z_2 \otimes a_8; Z_1 \otimes a_7$.
Bzw. der Klartext: SRV3 = $k_5; \dots k_1$.
- Schritt 12
keine aktivitäten. a_{12} wird nicht genutzt.
- Schritt 13
keine aktivitäten. a_{13} wird nicht genutzt.
- Gehe zu Schritt 1 ...; a_{14} entspricht dann a_1 .

Die mathematische Darstellung des Dechiffrierens lautet: $K_j = (G_j * B_j) \text{ xor } M^{r_j}$

Das Rekursionsregister SRV2 und SRV3:



$$a_1 = a_3 \text{ XOR } a_5$$

Die Matrix lautet:

$$M = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$