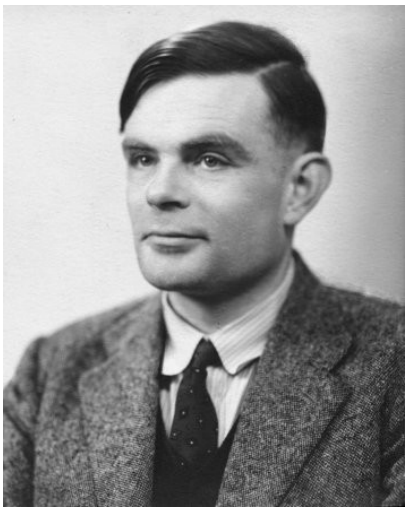


Alan Mathison Turing

(1912–1954) Englischer Mathematiker, Logiker, Kryptologe und einer der ersten Computerkonstrukteure. Turing studierte 1931–1935 Mathematik am King's College in Cambridge, promovierte 1938 in Princeton (USA) und unterrichtete danach am King's College. Im 2. Weltkrieg leistete er seinen Dienst in der geheimen Nachrichtenentschlüsselungsabteilung des britischen Außenministeriums in Bletchley Park, nördlich von London. Seine außergewöhnlichen Erfolge bei der Entschlüsselung der deutschen Geheimnachrichten, die mithilfe des Chiffriergeräts „Enigma" verschlüsselt wurden, werden nach langjähriger Geheimhaltung durch den britischen Staat inzwischen als kriegsentscheidend, insbesondere was den U-Boot-Krieg im Atlantik betraf, eingestuft. Bereits bei seiner Tätigkeit im Geheimdienst wurden speziell entworfene Spezialrechner, basierend auf Relaistechnik, eingesetzt. Später war Turing beim Bau der ersten Großrechenanlage (genannt ACE) in England beteiligt. Diese Arbeiten basierten auf seinen theoretischen Überlegungen zur Berechenbarkeitstheorie. In seiner berühmtesten Arbeit „On computable numbers, with an application to the Entscheidungsproblem" (1937) stellt er das Konzept der „Turingmaschine" vor und zeigt auch die Nicht-Berechenbarkeit bestimmmter Probleme. Später schrieb er umfangreiche Programme für diese ersten Computer und befasste sich mit weiter gehenden Fragen, wie und ob Computer Schachspielen und ganz allgemein denken können (der nach ihm benannte „Turing-Test" soll dies feststellen können). Nach 1950 konzentrierten sich seine Interessen auf philosophische Fragen der Kybernetik und mathematische Aspekte der theoretischen Biologie.

Turing's Homosexualität wurde den Behörden nach dem Krieg offenbar. Da dies in England als Straftat galt, musste er sich unter Androhung von Gefängnis einer Hormonbehandlung unterziehen lassen. Vermutlich ist dies der Grund für seinen Selbstmord (mit Zyankali vergifteter Apfel) im Jahr 1954. Das bewegte Leben von Turing und seine Eigenarten waren Anlass für Romane und sogar Theaterstücke („Breaking the Code", uraufgeführt in London, 1986).

Autokey-Verschlüsselung (Variante von Vigenère)

Variante 1: $Chiffre_i$ als $Schlüssel_{i+1}$ verwenden

```
  MORGE NFRUE HANGR EIFEN
+ DEATH PSRZL CXITP JXVZG
---------------------------
  PSRZL CXITP JXVZG NFADT
```

Sei a_i, k, c_i i-ter Klartext-, Schlüssel, i-ter Chiffretext-Block.

In Formeln: $c_0 = a_0 \oplus k$

↑ ziffernweise Addition, mod 26

$$c_i = a_i \oplus c_{i-1} \qquad (i = 1, 2, \ldots)$$

Kryptoanalyse:

$$a_i = c_i \ominus c_{i-1} \qquad (i = 1, 2, \ldots)$$

```
  PSRZL CXITP JXVZG NFADT
-   ?   PSRZL CXITP JXVZG
---------------------------
  ?     NFRUE HANGR EIFEN
```

Autokey-Variante 2: $Klartext_i$ als $Schlüssel_{i+1}$ verwenden.

MORGE NFRUE HANGR EIFEN
+ DEATH ↘ MORGE ↘ NFRUE ↘ HANGR

PSRZL ZTIAI UFEAV LISKE

in Formeln: $c_0 = a_0 \oplus k$

$c_i = a_i \oplus a_{i-1} \qquad (i = 1,2,\dots)$

Dechiffrierung, bei Kenntnis des Schlüssels (von links nach rechts):

$a_0 = c_0 \ominus k$

$a_i = c_i \ominus a_{i-1} \qquad (i = 1,2,\dots)$

Ohne Kenntnis des Schlüssels (Kryptoanalyse):
Zunächst dieselben Formeln verwenden mit $k=0$, ergibt sog. Pseudoklartext $a_0' a_1' a_2' \dots$

$a_0' = c_0 \ominus 0 = c_0$

$a_i' = c_i \ominus a_{i-1}'$

Für Pseudoklartext, im Vergleich zum korrekten Klartext gilt: $a_0 = a_0' \oplus k$

$a_1 = c_1 \ominus a_0 = c_1 \ominus c_0 = c_1 \ominus a_0 \ominus k$

$= a_1' \ominus k$

Und so geht es weiter:

$$a_2 = a_2' \oplus k$$
$$a_3 = a_3' \ominus k$$
$$a_4 = a_4' \oplus k$$
$$a_5 = a_5' \ominus k$$
$$\vdots$$

Das bedeutet, der Pseudoklartext $a_0' a_1' a_2' \ldots$ ist eine Vigenère-Verschlüsselung des Klartexts $a_0 a_1 a_2 \ldots$ mit dem Schlüssel $(k, \ominus k)$

Also: Schlüssel hat nun doppelte Länge, dafür aber symmetrische Struktur.

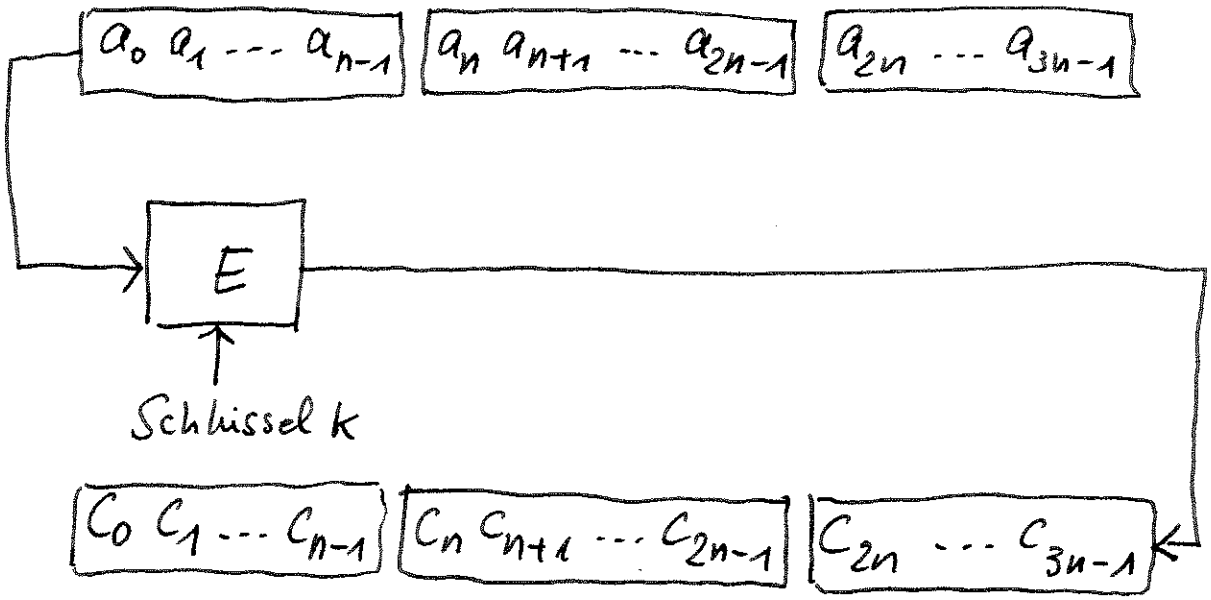
Bsp: Aus DEATH wird $\underbrace{\text{DEATH}}_{k}\,\underbrace{\text{XWAHT}}_{\ominus k}$

Also kann man die Autokey-Variante 2 ebenfalls mit den Methoden der Vigenère-Kryptoanalyse „knacken".

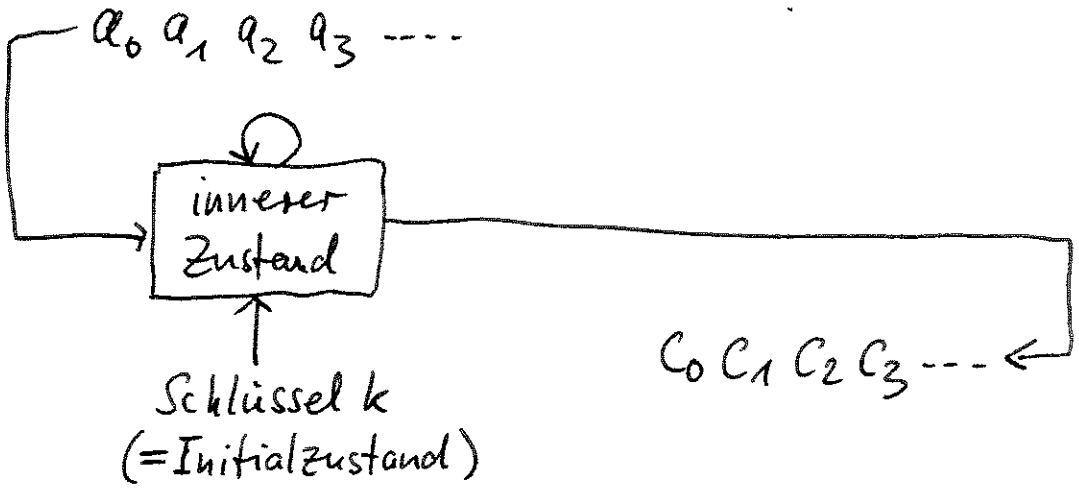
Klassische Kryptosysteme können bei größerer Schlüssellänge durchaus sicher sein.

Polyalphabetische Chiffrierung verwenden.

- Blockweise chiffrieren:



- Stromchiffre

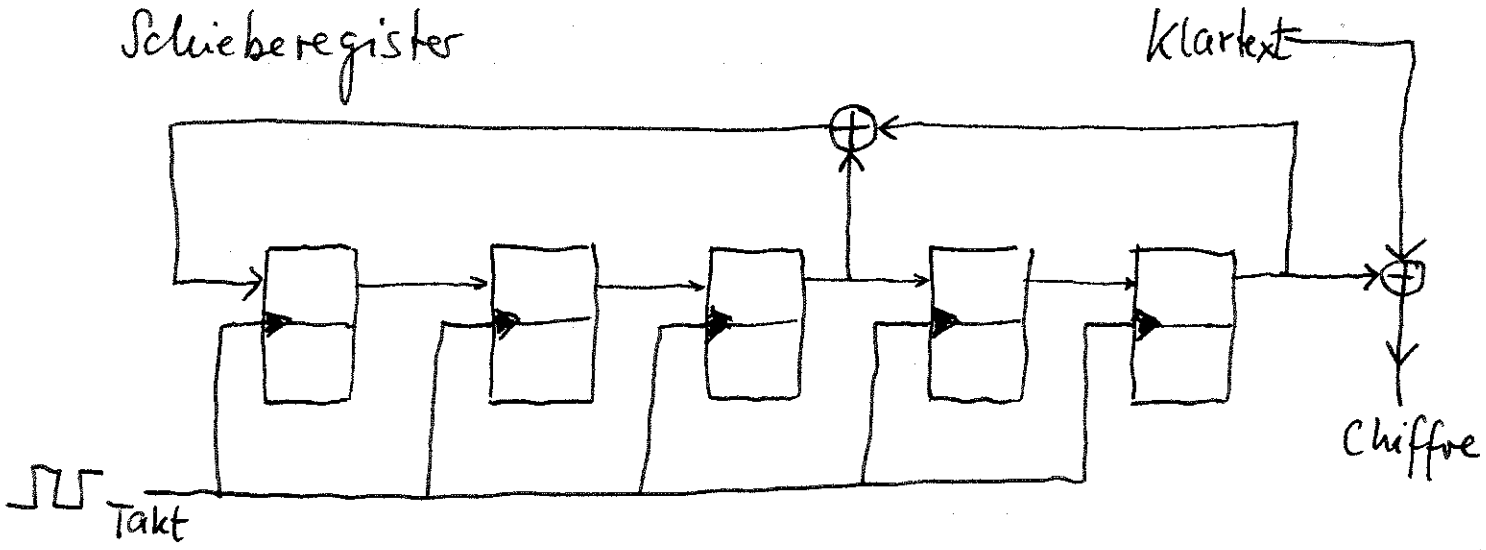


Wünschenswert: Lawineneffekt

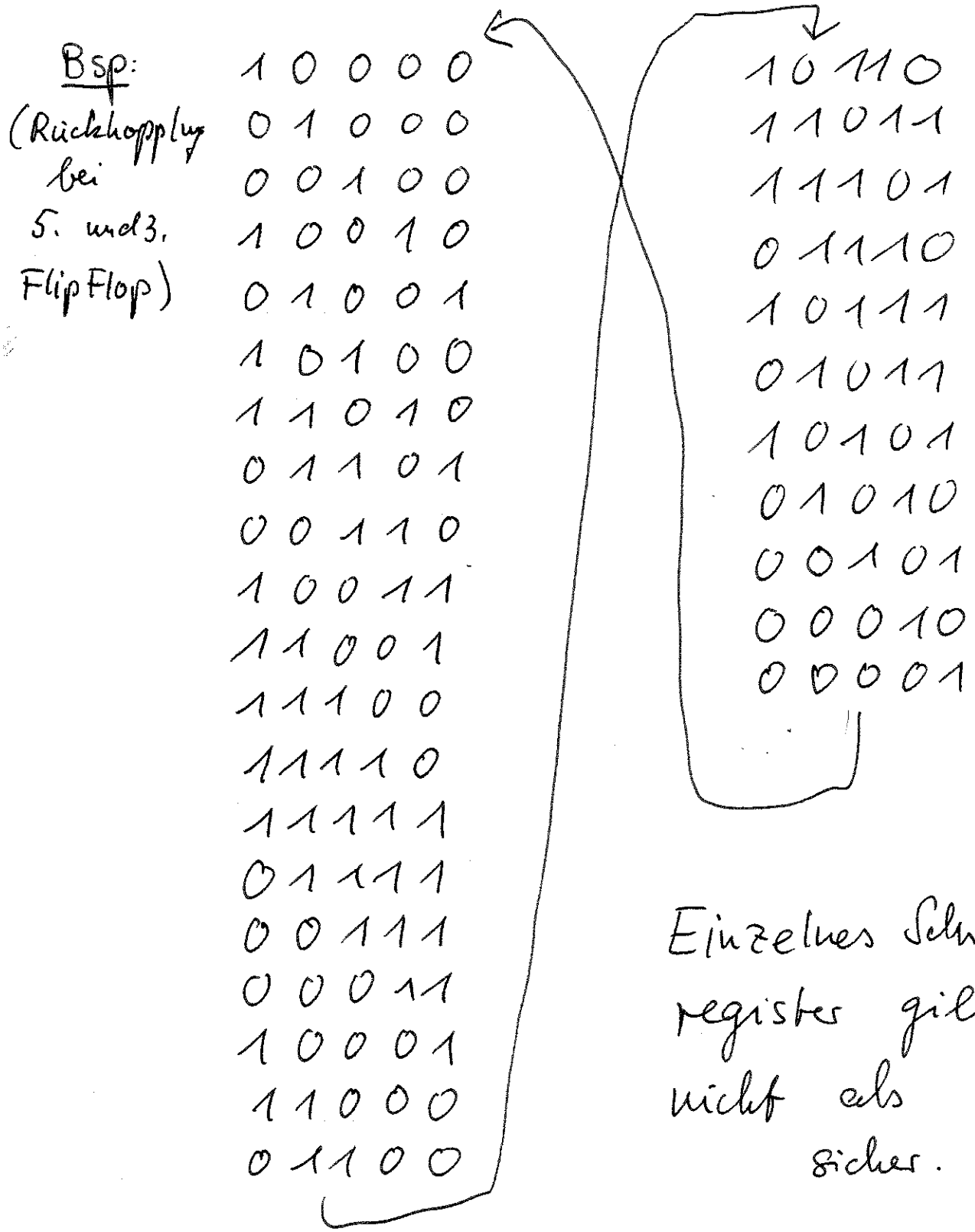
Ändert man nur 1 Buchstaben des Klartexts (bei Beibehalten des Schlüssels k), so unterscheiden sich ursprüngliche Chiffre und Chiffre bei abgeändertem Klartext völlig — als ob die Chiffrebuchstaben per Zufall neu ausgewürfelt wurden.

Bsp: Ist die Chiffre eine Bitfolge, so sollte die neue Chiffre, bei abgeändertem Klartext, sich etwa in der Hälfte des Bits von der ursprünglichen Chiffre unterscheiden.

Beispiel für Stromchiffre: Rückgekoppeltes Schieberegister



Ein Schieberegister, das aus n Flip-Flops besteht, kann bei richtiger Rückkopplungsverschaltung eine maximale Periodenlänge von $2^n - 1$ erreichen.

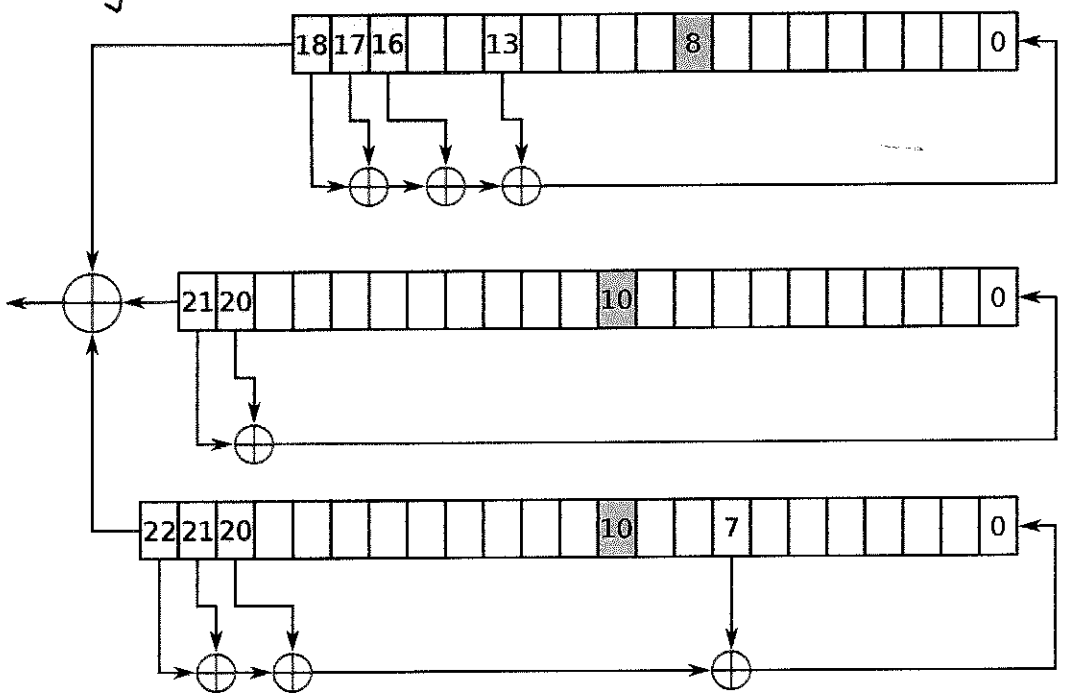


Einzelnes Schieberegister gilt nicht als sicher.

Anschlussverbindungen rückgekoppelter Schieberegister mit $n = 3, 4, \ldots, 168$ Flip Flops mit maximaler Periodenlänge.

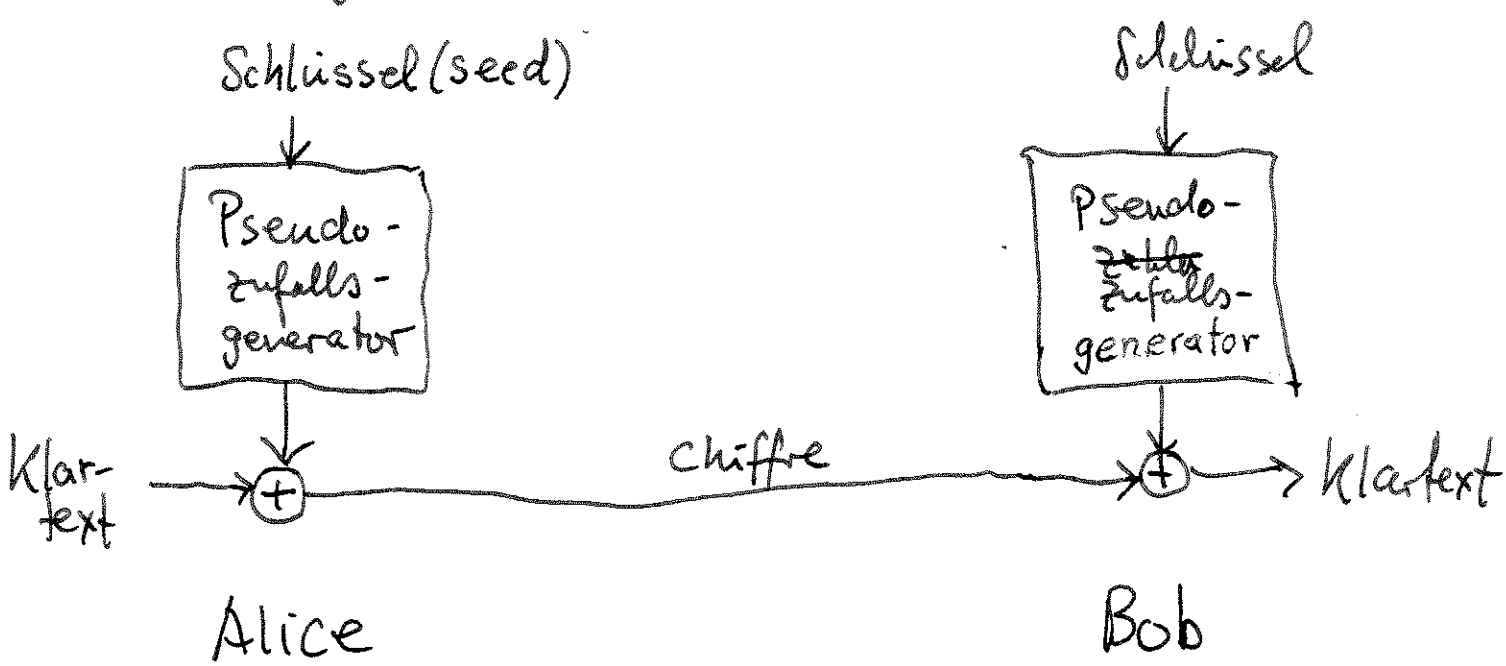
n	XNOR from	n	XNOR from	n	XNOR from	n	XNOR from
3	3,2	45	45,44,42,41	87	87,74	129	129,124
4	4,3	46	46,45,26,25	88	88,87,17,16	130	130,127
5	5,3	47	47,42	89	89,51	131	131,130,84,83
6	6,5	48	48,47,21,20	90	90,89,72,71	132	132,103
7	7,6	49	49,40	91	91,90,8,7	133	133,132,82,81
8	8,6,5,4	50	50,49,24,23	92	92,91,80,79	134	134,77
9	9,5	51	51,50,36,35	93	93,91	135	135,124
10	10,7	52	52,49	94	94,73	136	136,135,11,10
11	11,9	53	53,52,38,37	95	95,84	137	137,116
12	12,6,4,1	54	54,53,18,17	96	96,94,49,47	138	138,137,131,130
13	13,4,3,1	55	55,31	97	97,91	139	139,136,134,131
14	14,5,3,1	56	56,55,35,34	98	98,87	140	140,111
15	15,14	57	57,50	99	99,97,54,52	141	141,140,110,109
16	16,15,13,4	58	58,39	100	100,63	142	142,121
17	17,14	59	59,58,38,37	101	101,100,95,94	143	143,142,123,122
18	18,11	60	60,59	102	102,101,36,35	144	144,143,75,74
19	19,6,2,1	61	61,60,46,45	103	103,94	145	145,93
20	20,17	62	62,61,6,5	104	104,103,94,93	146	146,145,87,86
21	21,19	63	63,62	105	105,89	147	147,146,110,109
22	22,21	64	64,63,61,60	106	106,91	148	148,121
23	23,18	65	65,47	107	107,105,44,42	149	149,148,40,39
24	24,23,22,17	66	66,65,57,56	108	108,77	150	150,97
25	25,22	67	67,66,58,57	109	109,108,103,102	151	151,148
26	26,6,2,1	68	68,59	110	110,109,98,97	152	152,151,87,86
27	27,5,2,1	69	69,67,42,40	111	111,101	153	153,152
28	28,25	70	70,69,55,54	112	112,110,69,67	154	154,152,27,25
29	29,27	71	71,65	113	113,104	155	155,154,124,123
30	30,6,4,1	72	72,66,25,19	114	114,113,33,32	156	156,155,41,40
31	31,28	73	73,48	115	115,114,101,100	157	157,156,131,130
32	32,22,2,1	74	74,73,59,58	116	116,115,46,45	158	158,157,132,131
33	33,20	75	75,74,65,64	117	117,115,99,97	159	159,128
34	34,27,2,1	76	76,75,41,40	118	118,85	160	160,159,142,141
35	35,33	77	77,76,47,46	119	119,111	161	161,143
36	36,25	78	78,77,59,58	120	120,113,9,2	162	162,161,75,74
37	37,5,4,3,2,1	79	79,70	121	121,103	163	163,162,104,103
38	38,6,5,1	80	80,79,43,42	122	122,121,63,62	164	164,163,151,150
39	39,35	81	81,77	123	123,121	165	165,164,135,134
40	40,38,21,19	82	82,79,47,44	124	124,87	166	166,165,128,127
41	41,38	83	83,82,38,37	125	125,124,18,17	167	167,161
42	42,41,20,19	84	84,71	126	126,125,90,89	168	168,166,153,151
43	43,42,38,37	85	85,84,58,57	127	127,126		
44	44,43,18,17	86	86,85,74,73	128	128,126,101,99		

Wesentlich höhere Sicherheit beim Verschalten mehrerer Schieberegister unterschiedlicher Länge.



Stromchiffre A5/1 wie sie im Mobilfunk-Standard GSM verwendet wird.

Verallgemeinertes Modell:



Gängige Pseudozufallsgeneratoren

linearer Kongruenzgenerator:

$$x_{i+1} = (a \cdot x_i + b) \bmod n$$

x_0 ... seed.

max. Periodenlänge ist n.

Bsp: $a = 5$; $b = 17$; $n = 101$; $x_0 = 1$

ergibt:

1, 22, 26, 46, 45, 40, 15, 92, 73, 79, 8, 57, 100, 12,
77, 99, 7, 52, 75, 89, 58, 4, 37, 0, 17, 1

Periodenlänge: 25

Besser: $x_{i+1} = (a x_i^2 + b x_i + c) \bmod n$

speziell: $x_{i+1} = (x_i^2 + 1) \bmod n$

Variante (Blum, Blum, Shub):

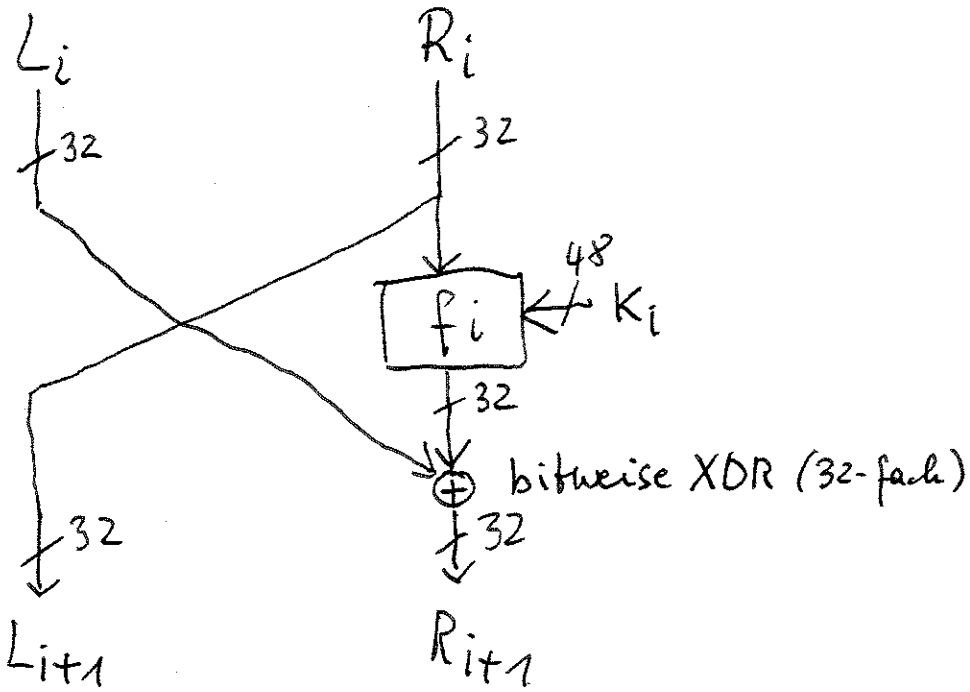
$$x_{i+1} = x_i^2 \bmod n$$

wobei $n (= p \cdot q)$ p, q geheim.

Blockweise Chiffrierung mittels Feistel-Netzwerk (am Beispiel DES)

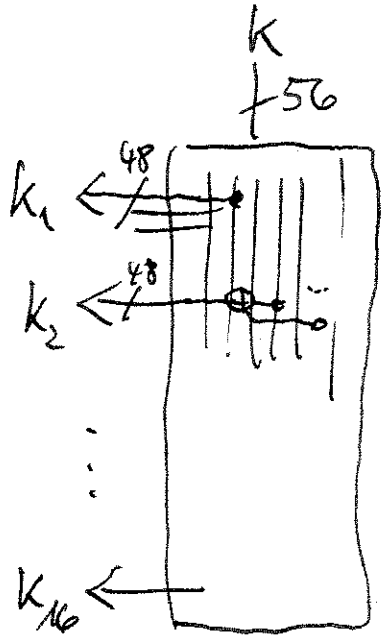
Blocklänge = 64 Schlüssellänge = 56

16 Runden:



In Formeln: $L_{i+1} = R_i$

$R_{i+1} = L_i \oplus f_i(R_i, K_i)$

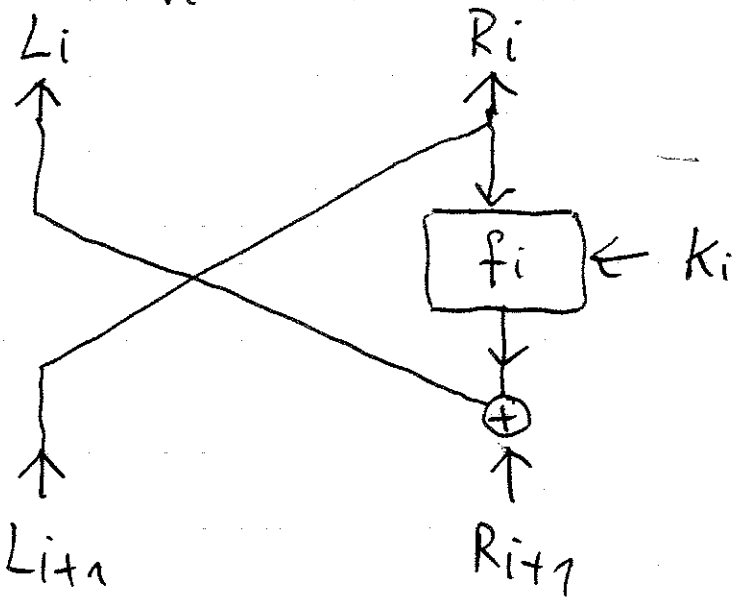


Rundenschlüssel-Erstellung

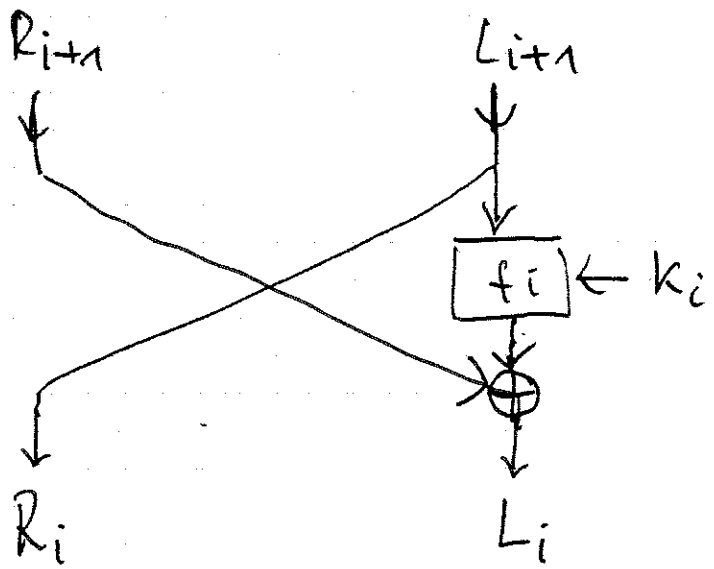
Dechiffrieren (bei Kenntnis von k_i)

$z = x \oplus y$

$x = y \oplus z$



Dasselbe neu gezeichnet (oben ↔ unten, links ↔ rechts)



Schlüssellänge 56 wird als zu kurz angesehen.

Besser: Tripel-DES ; Schlüssel $k_1 k_2$ mit 112 Bit

$$\text{Triple-DES}(x, k_1 k_2) =$$

$$\text{DES}\left(\overline{\text{DES}}^{-1}\left(\text{DES}(x, k_1), k_2\right), k_1\right)$$