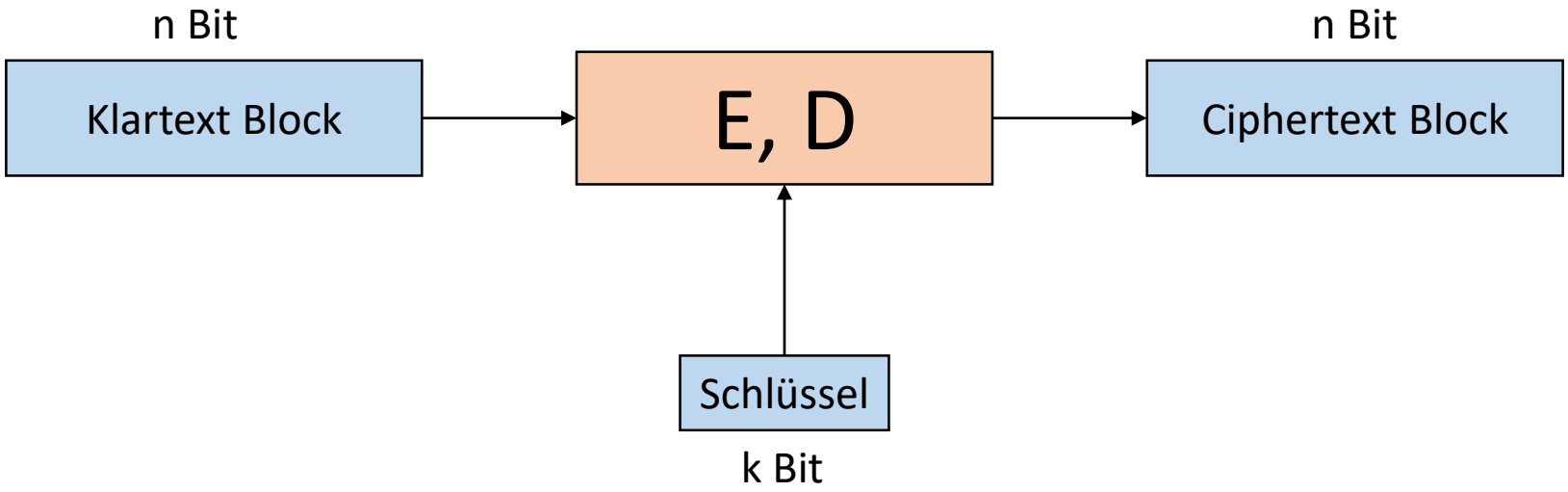
IT-Sicherheit

Blockchiffren

Version vom 14.11.2018

Grundsätzliche Funktion

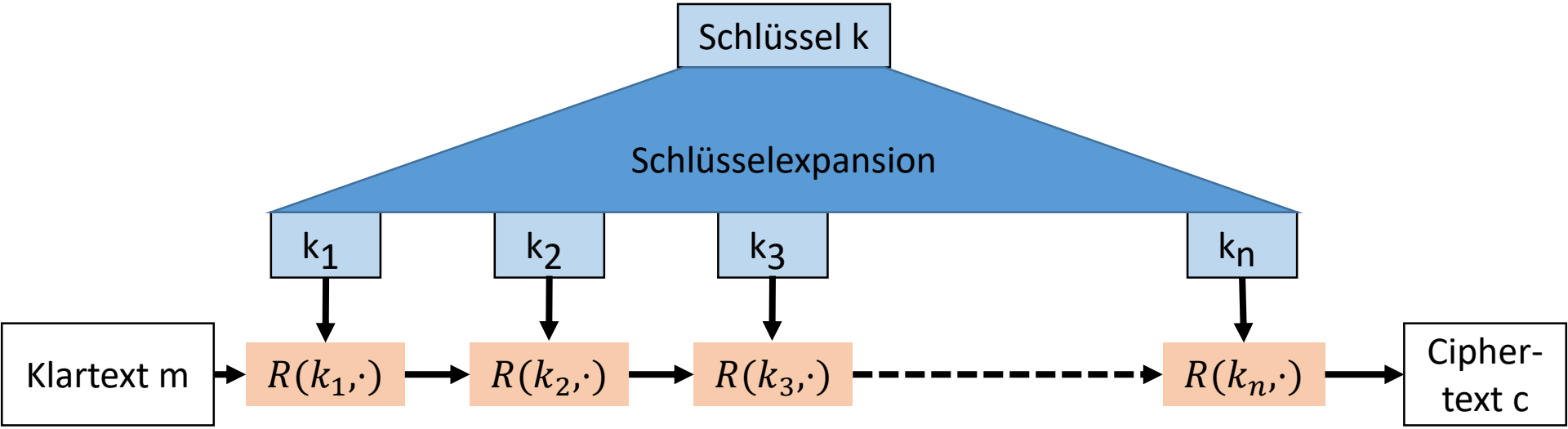


Beispiele:

3DES: n=64 Bit, k=168 Bit

AES n=128 Bit, k=128, 192, 256 Bit

Aufbau: Iterationen



Definition:
R(k, m) ist die **Rundenfunktion** des Blockchiffres.

Beispiele:

- 3DES: n=48 Runden
- AES: n=10 Runden (bei 128bit key), n=12 (192bit key), n=14 (256bit key)

Pseudo-Zufällige Permutation

Pseudo-Zufällige Funktion

Eine Pseudo-Zufällige Funktion (PRF) ist definiert über (K,X,Y):

$$F: K \times X \rightarrow Y$$

so, dass ein effizienter Algorithmus existiert, um F(k,x) zu berechnen.

Pseudo-Zufällige Permutation

Eine Pseudo-Zufällige Permutation (PRP) ist definiert über (K,X):

$$E: K \times X \rightarrow X$$

so, dass

1. Ein effizienter, **deterministischer** Algorithmus existiert, um E(k,x) zu berechnen.
2. $E(k,\cdot)$ bijektiv ist.
3. Ein effizienter Umkehralgorithmus D(k,y) existiert.

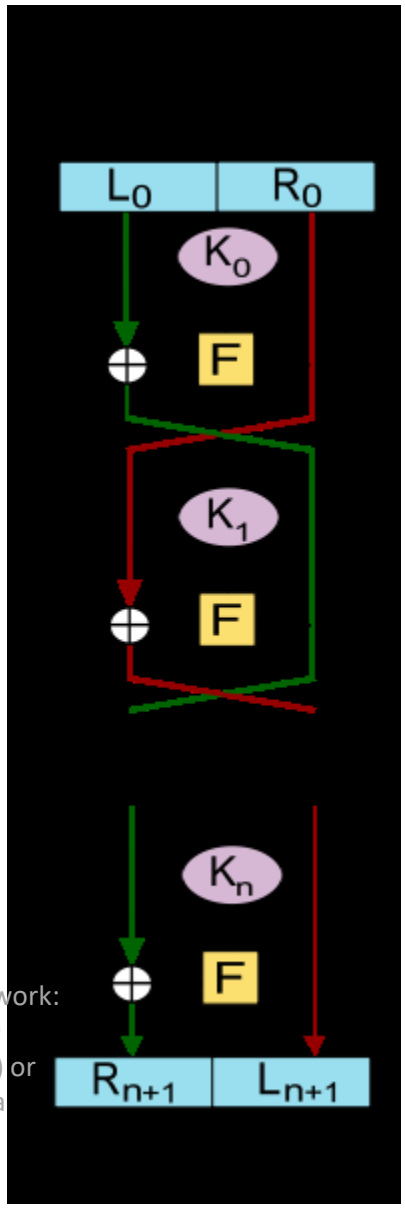
Feistel-Chiffren

Feistel-Chiffren (nach Horst Feistel) teilen den Plaintextblock in zwei Hälften L und R auf. Für jede Runde des Chiffres beim Verschlüsseln gilt dann:

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus F(R_i, k_i)$$

Wobei F die Rundenfunktion ist und k_i der für diese Runde abgeleitete Schlüssel.

Die meisten Blockchiffren sind Feistel-Chiffren (nennenswerte Ausnahme: AES)



Konfusion und S-Boxen

Als **Konfusion** wird der Umstand bezeichnet, dass ein einzelnes Bit des Ciphertexts von mehreren Bits des Schlüssels abhängig sein soll. Konfusion ist ein Designziel bei Verschlüsselungsverfahren, um mögliche Rückschlüsse von Ciphertext und Schlüssel zu erschweren. (Definiert von C. Shannon)

Erreicht wird Konfusion in der Praxis durch den Einsatz von S-Boxen (Substitution Boxes) innerhalb der Rundenfunktion F. Diese geben eine standardisierte, **nicht-lineare** Ersetzung vor.

S-Box der AES-Rundenfunktion

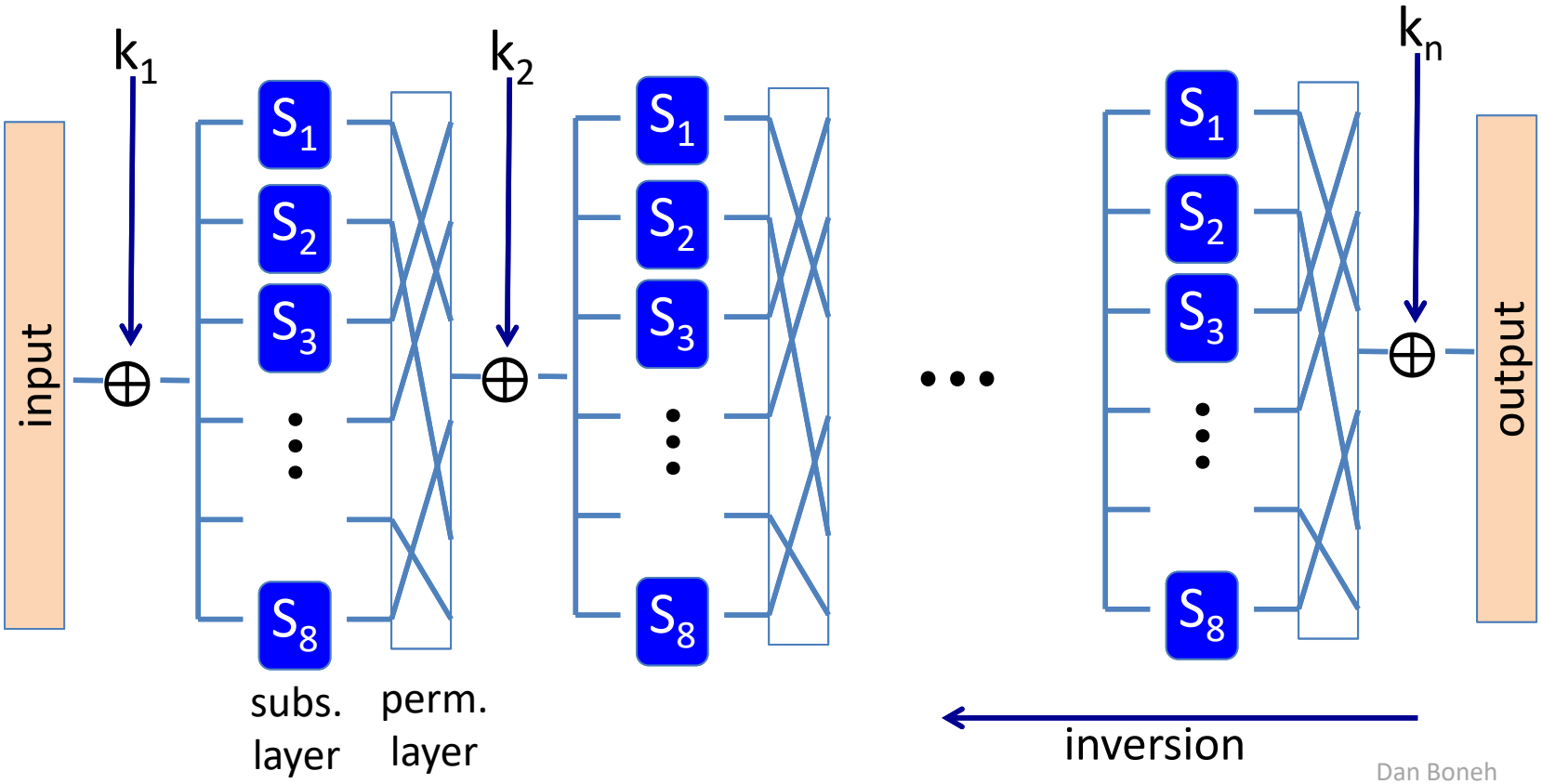
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Diffusion und P-Boxen

Als Diffusion wird die Eigenschaft bezeichnet, nach der sich bei einem sicheren Cipher bei Änderung eines einzelnen Bits der Klartext (statistisch) die Hälfte der Ciphertext-Bits ändern soll. Damit soll erreichet werden, dass Änderungen am Klartext zu keinem erkennbaren Muster im Ciphertext führen.

Dies wird erreicht, indem bei jeder Runde die Bits nach einem im Standard angegebenen Muster neu angeordnet werden. Dieses Muster wird als **P-Box** (permutation box) bezeichnet.

AES (Überblick)



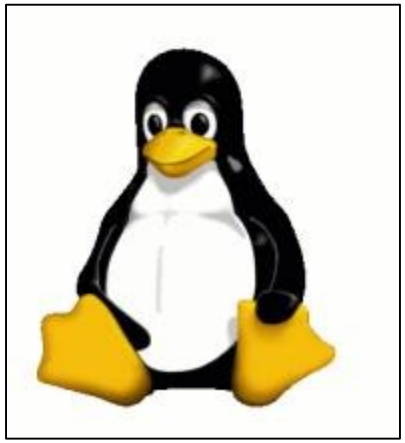
Verwendung von Blockchiffren

- ECB (Electronic Code Book)
  - Jeder Block wird identisch verschlüsselt.
  - Tritt ein Block innerhalb einer Nachricht mehrfach auf, so tritt auch dessen Chiffrat im Ciphertext mehrfach auf.

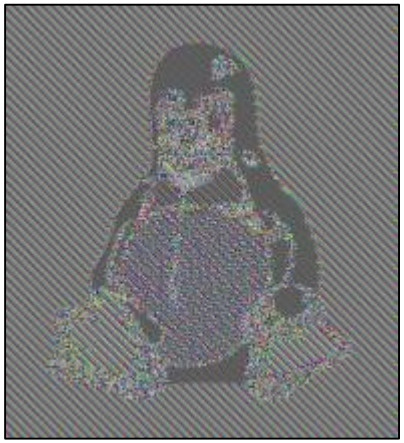
  ➔Angriffe über bekannte Strukturen und statistische Analysen möglich.

  ➔In nur wenigen Szenarien sinnvoll einzusetzen!
- CBC (Cipher Block Chaining)
  - Vor der Verschlüsselung wird jeder Plaintext-Block per XOR mit dem vorangegangenen Ciphertext-Block kombiniert. Der erste Block der Nachricht wird mit einem unverschlüsselt übertragenen Initialisierungsvektor verknüpft.
  - häufig verwendet, Padding ist notwendig
- CTR (Counter Mode)
  - Eine Kombination aus einer Nonce und einem Integer-Zähler wird verschlüsselt. Das Ergebnis wird per XOR mit dem Plaintext kombiniert um den Ciphertext zu erhalten.
  - Kann (fast) wie ein Stromchiffre verwendet werden!
  - Paralellisierbar ohne die Nachteile von ECB.

Angriff auf ECB visualisiert



Plaintext



im ECB-Modus verschlüsselt

mit CBC verschlüsselt

Tux the Penguin, the Linux mascot. Created in 1996 by Larry Ewing with The GIMP