Bernd Borchert

Univ. Tübingen WS 13/14

Vorlesung

Kryptographie

Teil 2

25.10.13

Blockverschlüsselung

Oft geht es nicht um kurze Nachrichten, sondern um lange Dateien, die verschlüsselt werden sollen.

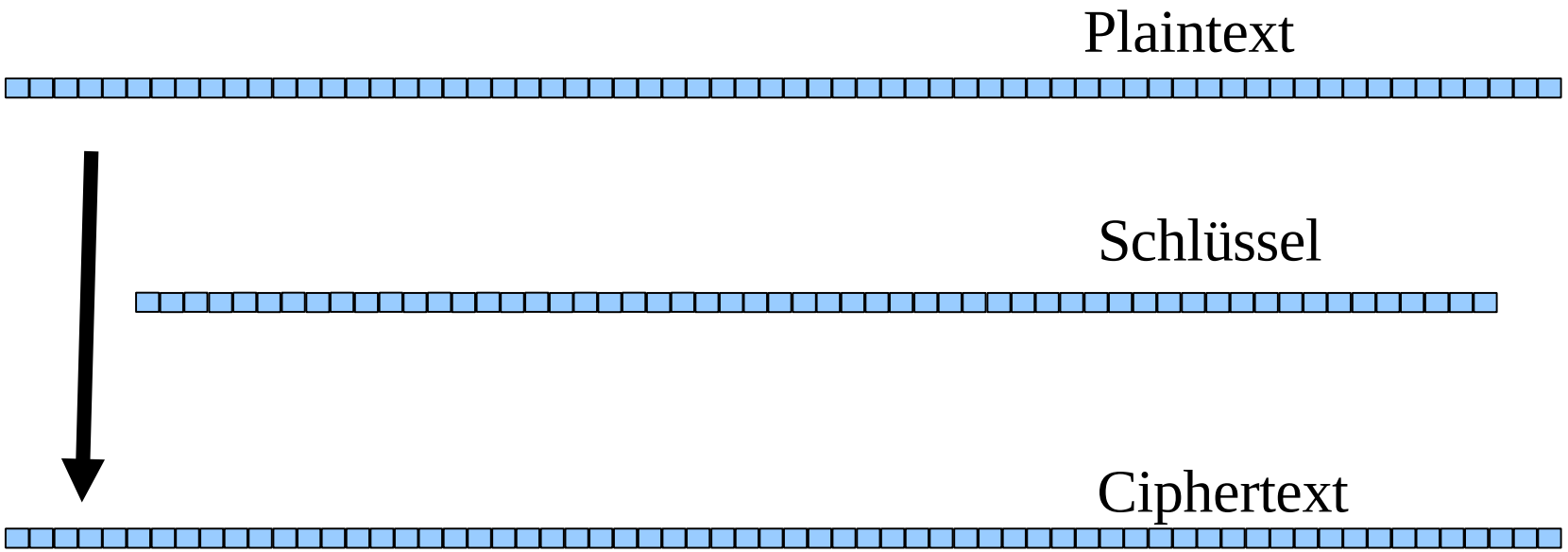
Dateien lassen sich in gleichlange Blöcke fester Länge (z.B. 8 Byte = 64 bit) zerlegen. Ggfs. muss der letzte Block noch aufgefüllt werden (“padding”)

Ein Blockchiffrier-Algorithmus besteht aus 2 Teilen: Einerseits der Chiffrier-Algorithmus für einen Block, und zweitens der *Betriebsmodus*, d.h. die Methode, die Blöcke nacheinander zu chiffrieren (ECB, etc.)

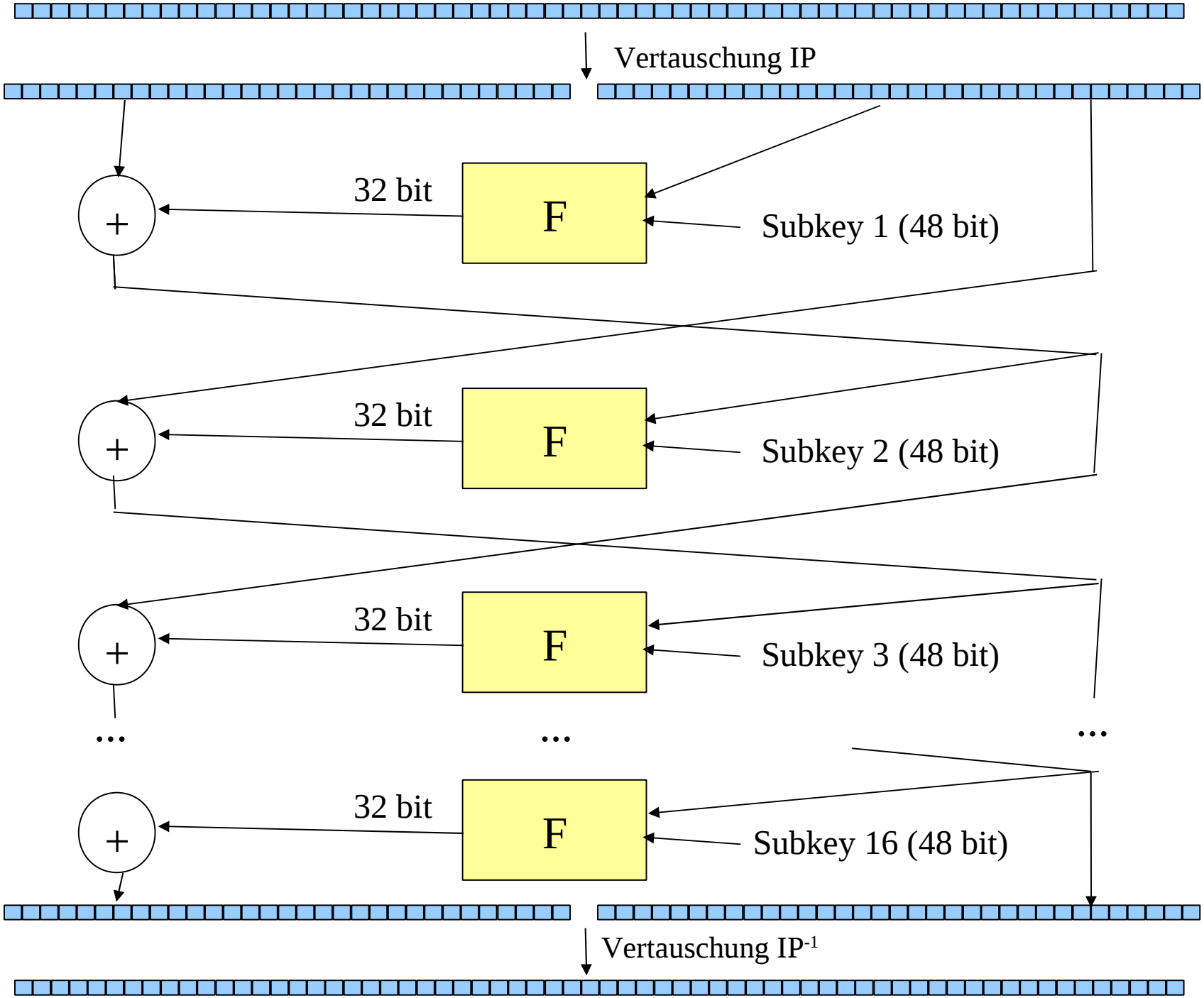
DES

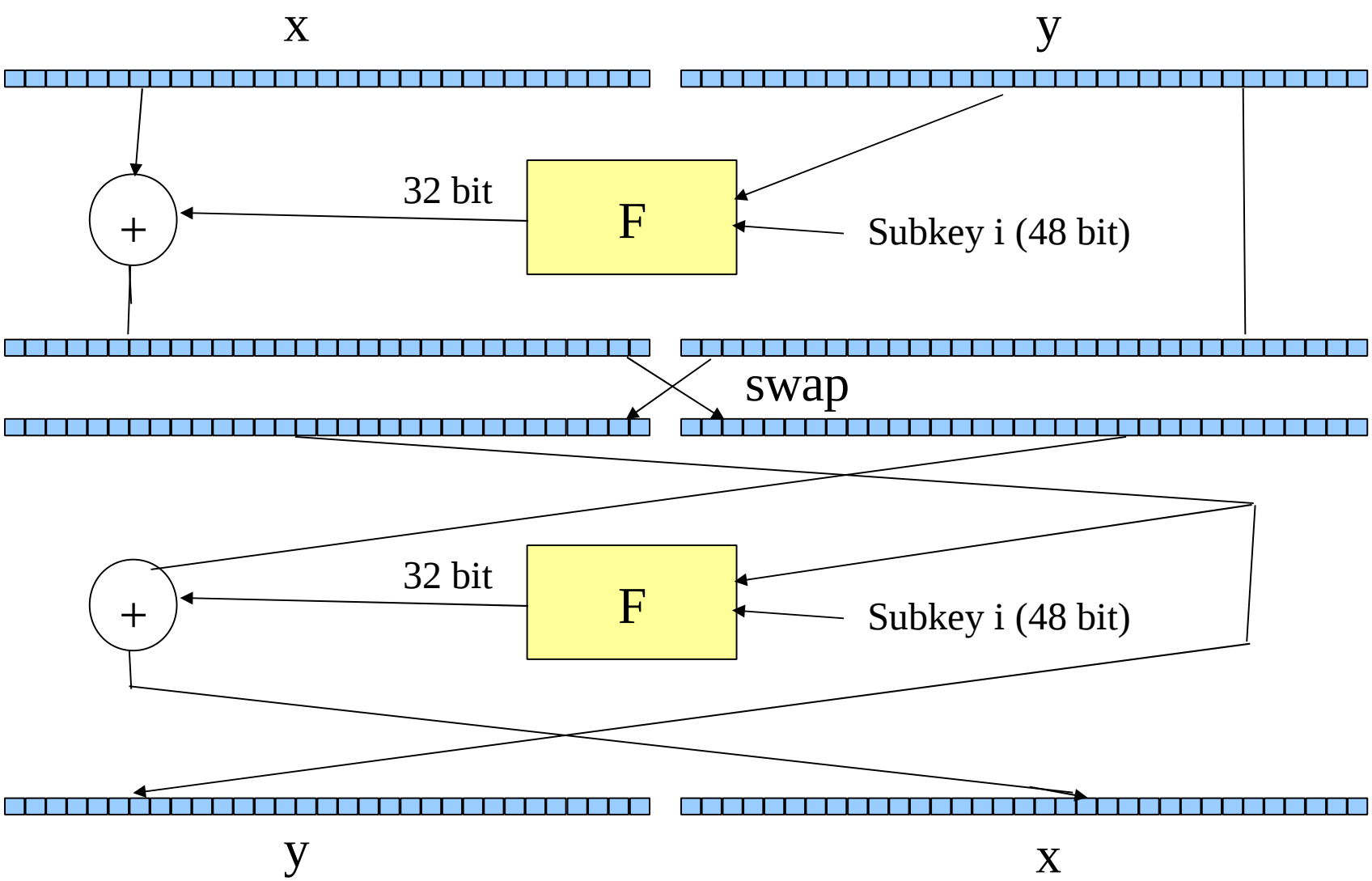
(Data Encryption Standard)

DES verschlüsselt einen 64 bit Block in einen 64 bit Block, und das mit einem Schlüssel der Länge 56 bit.



Entwickelt ca. 1976, bis ca. 1990 galt DES als sicher.

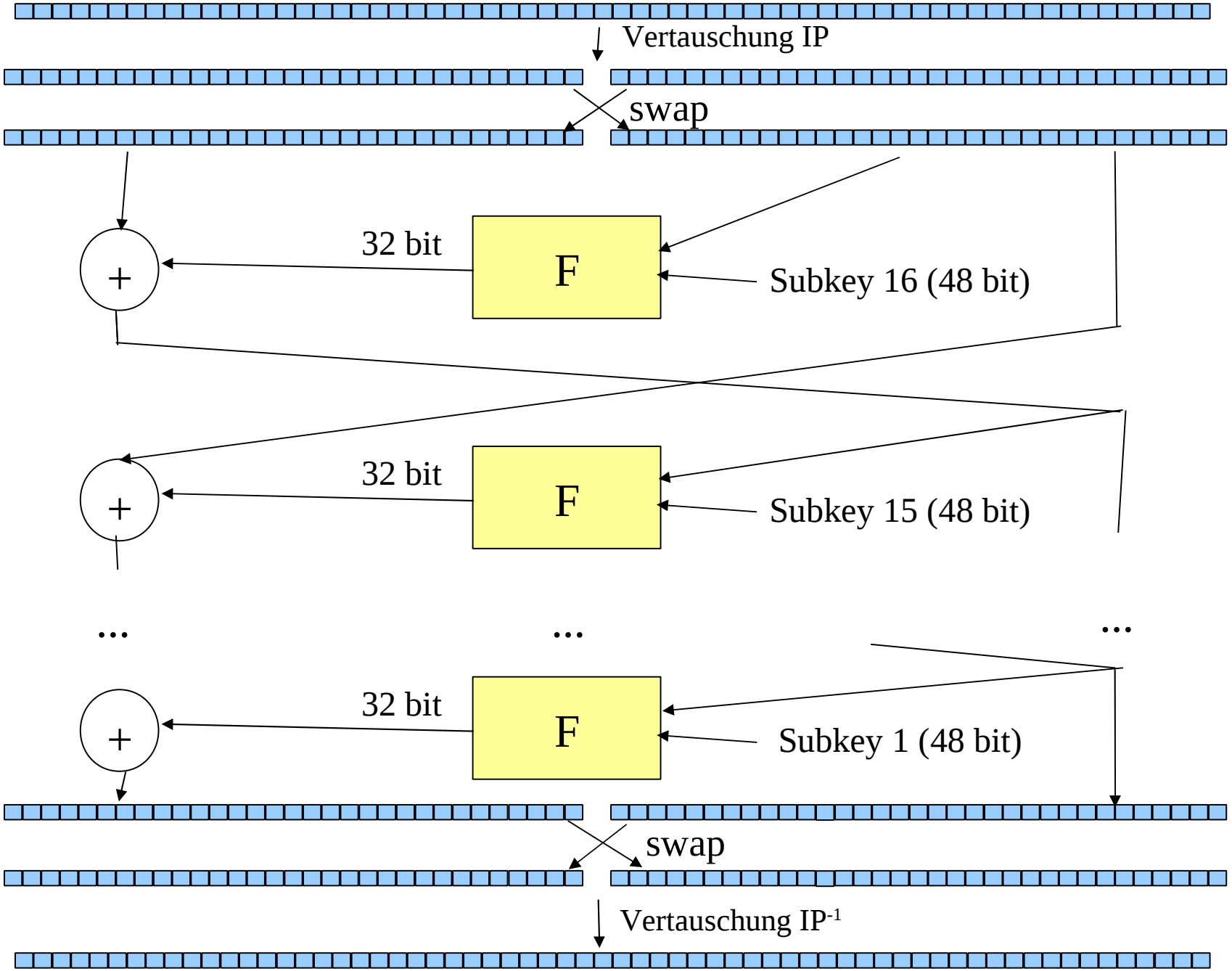

Vertauschung IP
32 bit
F
Subkey 1 (48 bit)
32 bit
F
Subkey 2 (48 bit)
32 bit
F
Subkey 3 (48 bit)
...
...
...
32 bit
F
Subkey 16 (48 bit)
Vertauschung IP-1



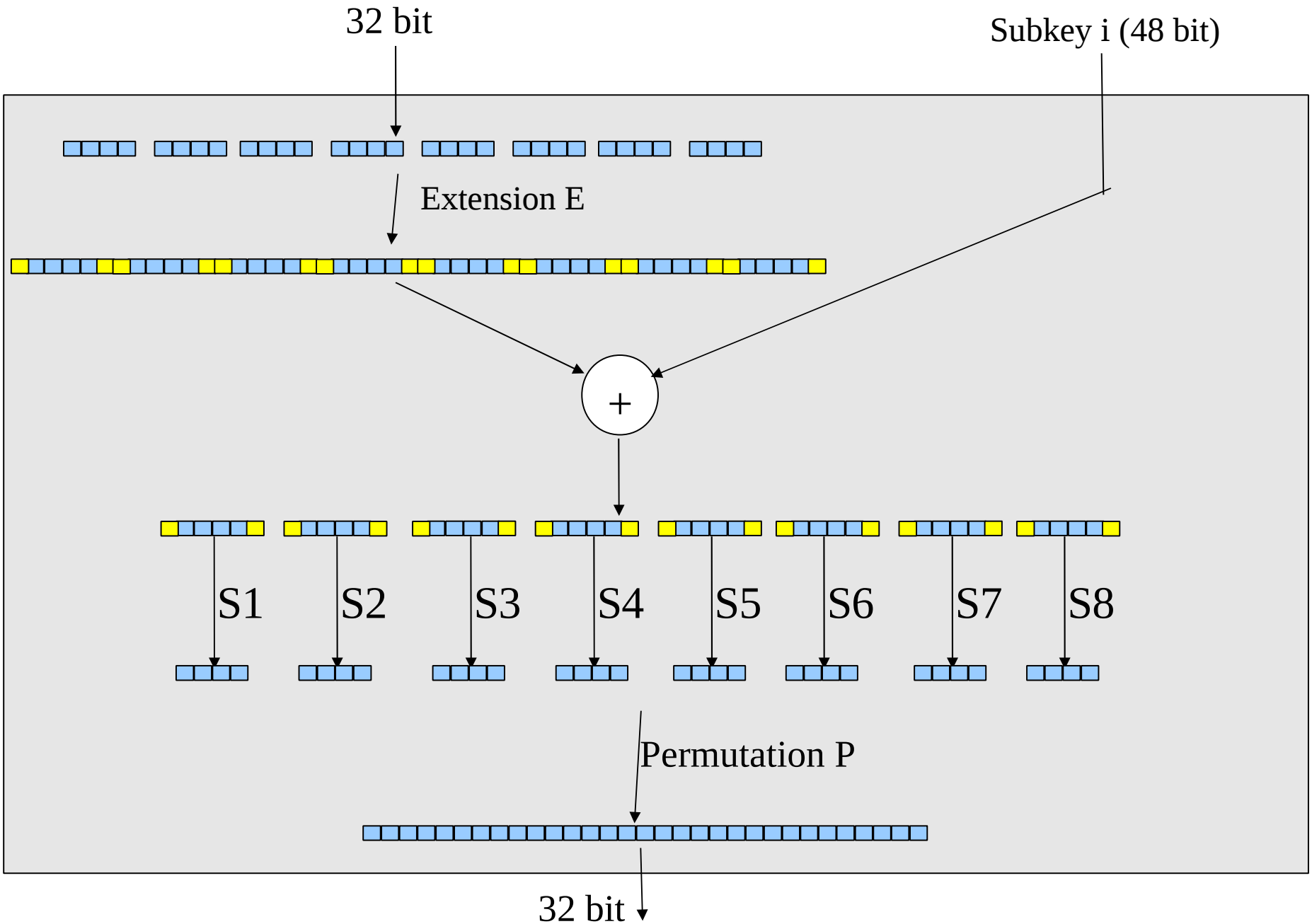
$$x + F(y,\text{Subkey i}) + F(y,\text{Subkey i}) = x$$

Fazit: Egal, wie F aussieht: DES ist umkehrbar durch Swappen und Durchlaufen der 16 Runden in umgekehrter Reihenfolge:

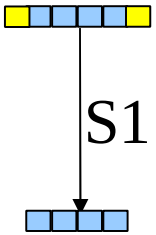
Entschlüsselung DES



Feistel Schaltung F



Feistelbox S1



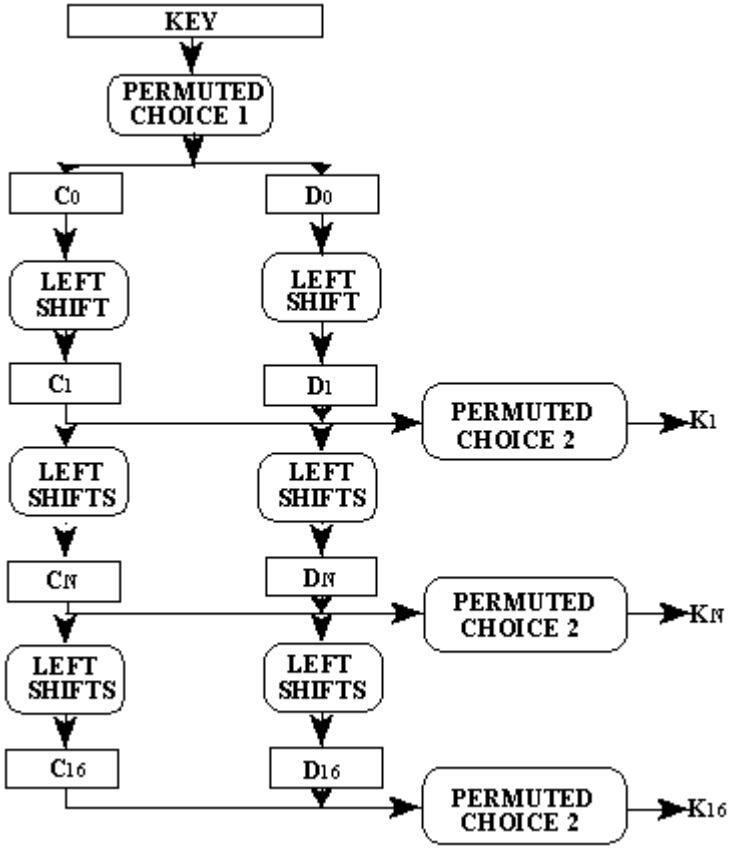
- Die beiden gelben bits werden binär als Zeile 0-3 interpretiert,
- die 4 blauen bits oben binär als Spalte 0-15
- und der in der Tabelle stehende Wert 0-15 wird binär zu den 4 blauen bits unten

S1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2 bis S8 werden analog, aber möglichst unterschiedlich definiert.

DES Subkey Erzeugung

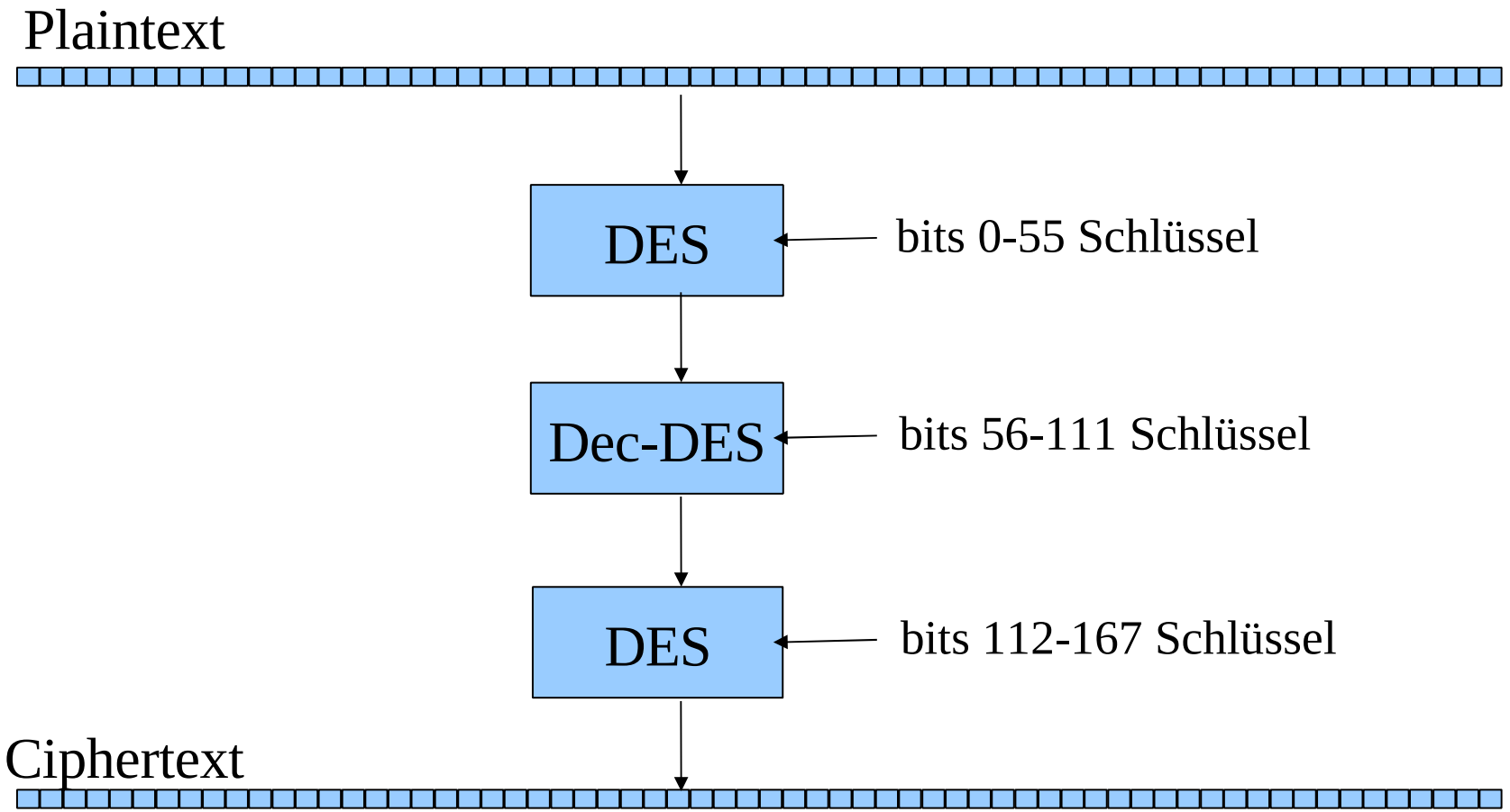
Die 16 48-bit Subkeys für DES werden aus dem vorgegebenen 56 bit Schlüssel durch Halbieren, Weglassen, Shiften, Permutieren und Wiederzusammensetzen erzeugt.
Details:



Iteration Number	Number of Left Shifts
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Triple DES

Triple DES verschlüsselt einen 64 bit Block in einen 64 bit Block, mit einem Schlüssel der Länge 3x56 = 168 bit.



Gilt immer noch als sicher.

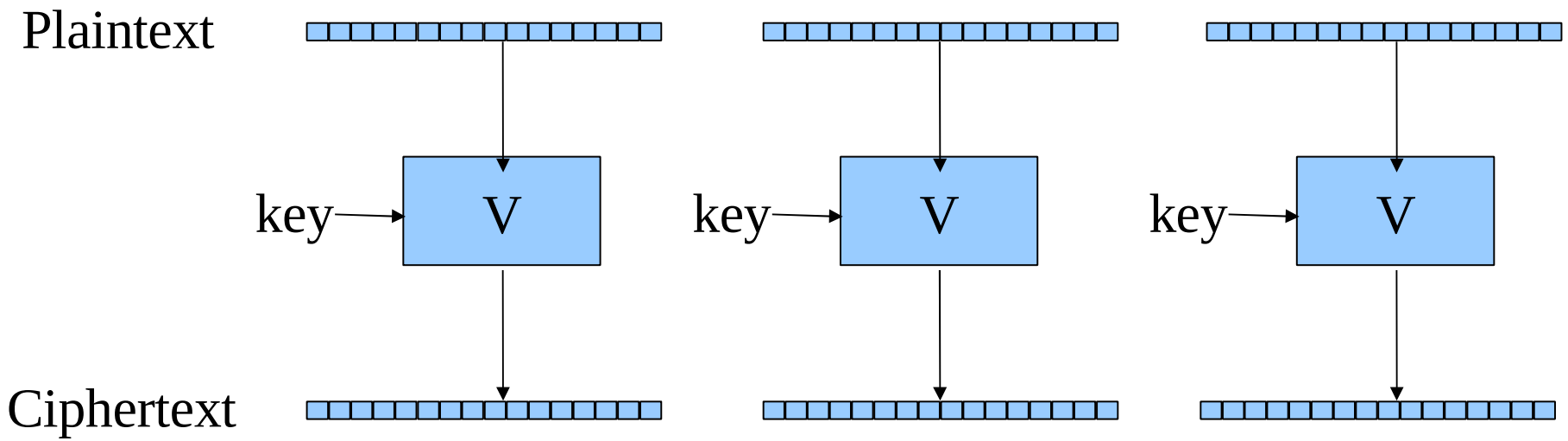
Betriebsmodi

Gegeben ist ein langer Text und eine Blockchiffre inkl. Blocklänge
und Schlüssel. Wie verschlüsselt man den Text?

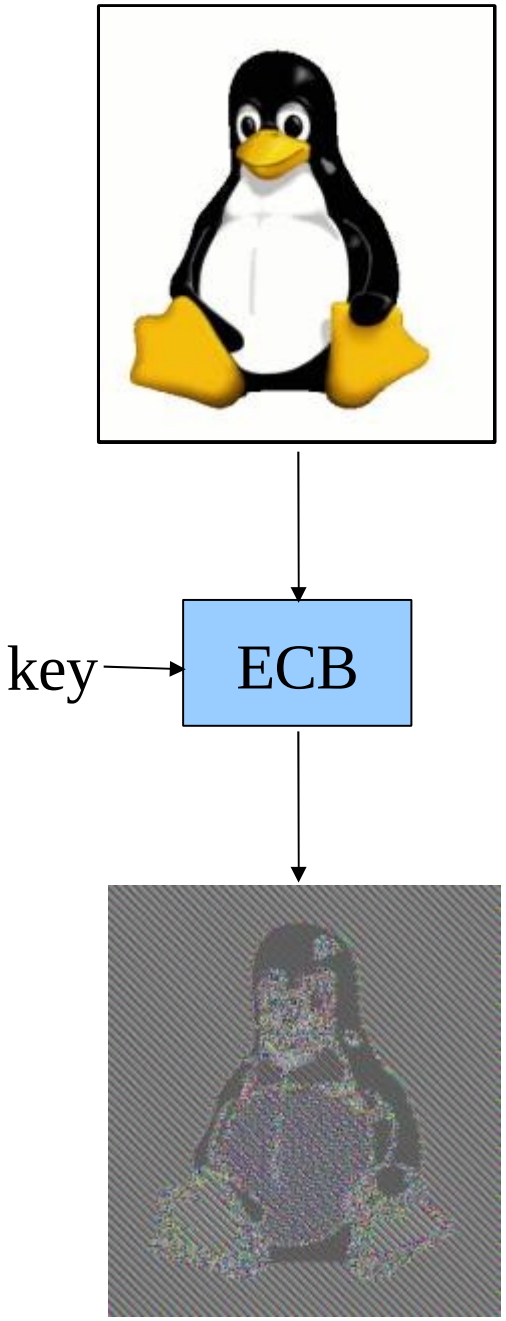
--> Betriebsmodus wählen: ECB, CBC, CFB, oder OFB
--> bei Modus CFB und OFB Initialisierungsvektor (IV) wählen
--> bei Modus ECB und CBC den Text hinten auf Blocklängenvielfaches padden

EBC Modus

Electronic Book Code Modus

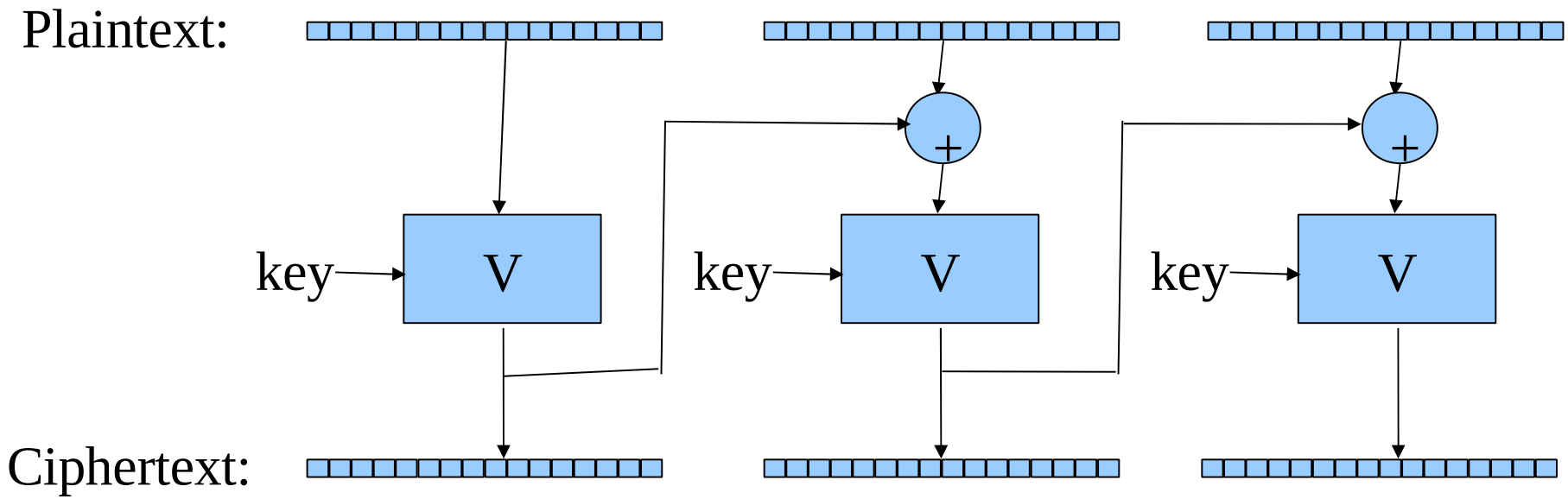


Nachteil ECB

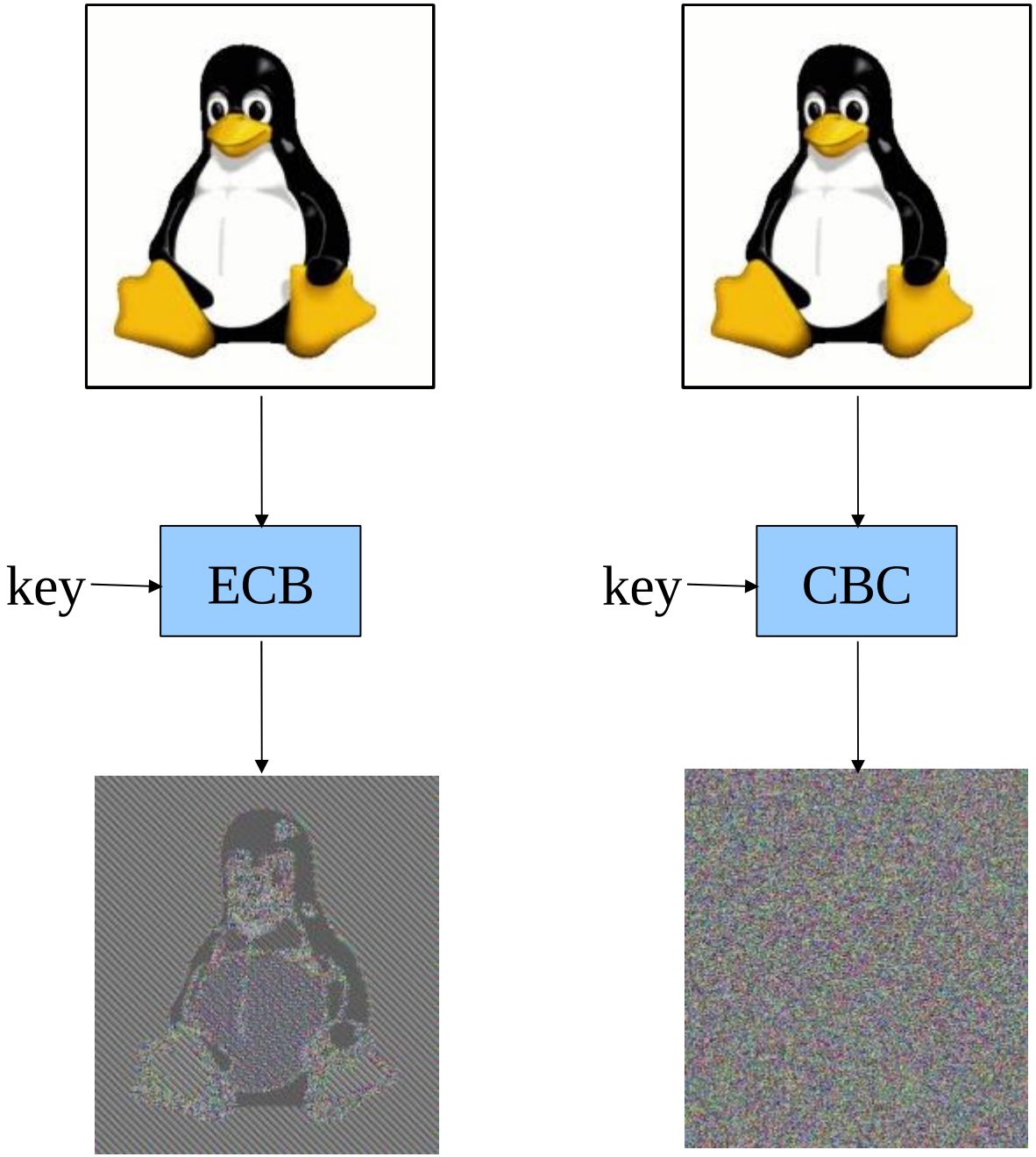


CBC Modus

Cipher Block Chaining Modus

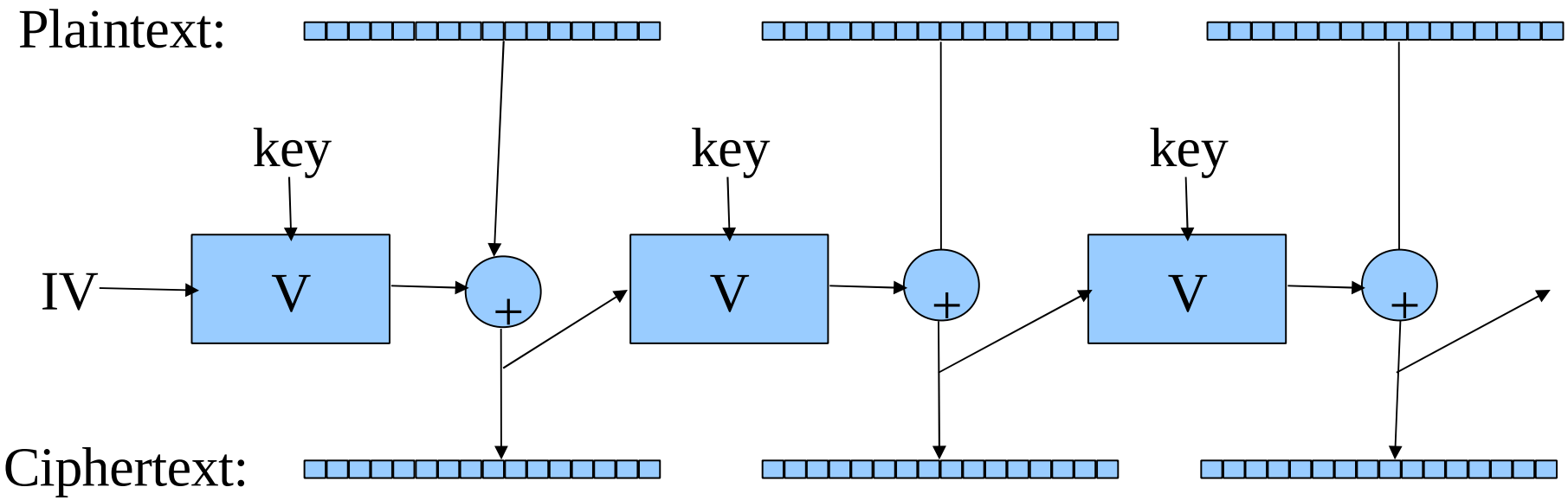


Vorteil CBC



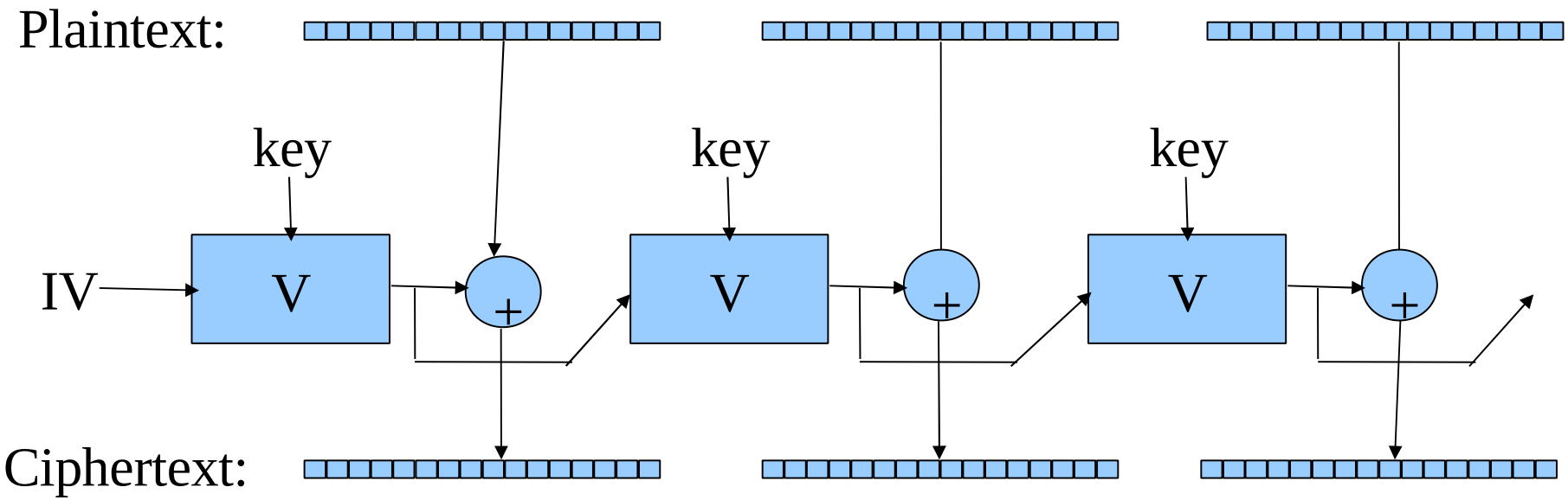
CFB Modus

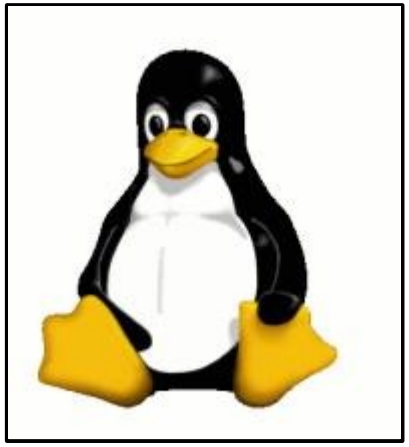
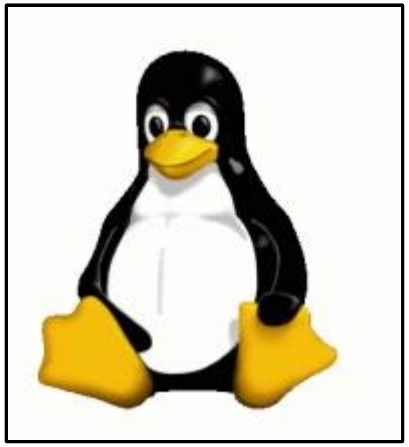
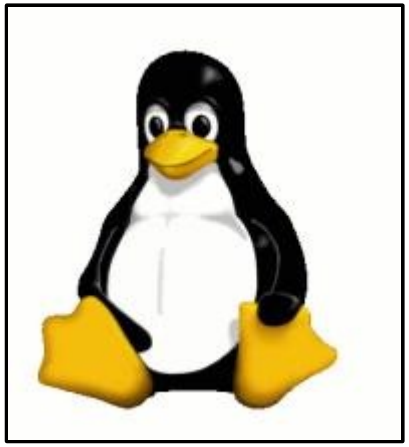
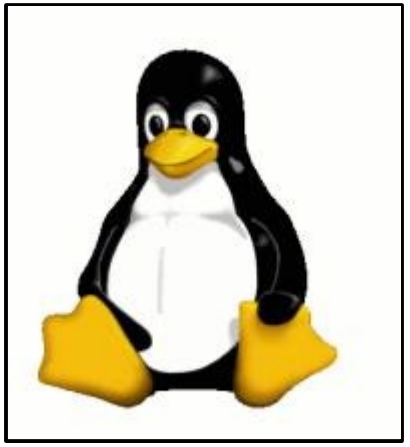
Cipher Feedback Modus



OFB Modus

Output Feedback Modus



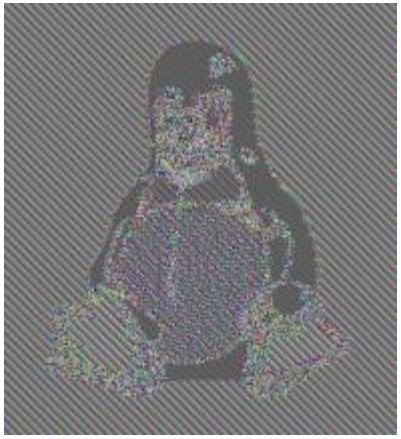
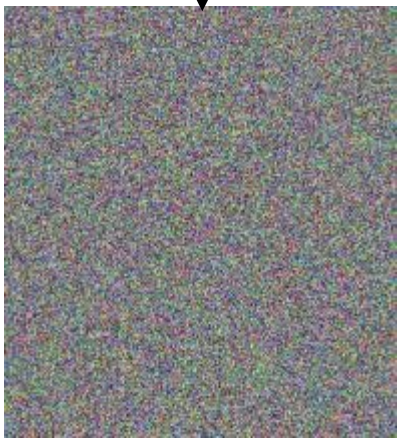
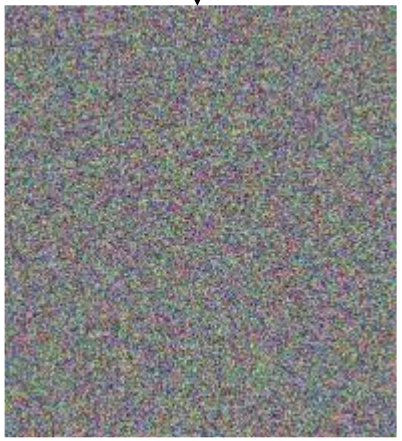





ECB

CBC

CFB

OFB


Math Basics I

Buchstabe --> Wort --> Sprache --> Klasse

Ein **Alphabet** ist ein endliche Menge. die Elemente heißen Zeichen oder Buchstaben. Z.B. {0,1} oder {a,...,z}

Ein **Wort** über einem Alphabet ist eine endliche Aneinanderkettung von Buchstaben des Alphabets. Beispiel “0110101” oder “hallo”, oder das leere Wort mit Länge 0.

Eine **Sprache** über einem Alphabet ist ein Menge von Wörtern. Z.B. {“ja”, nein”, “vielleicht”} oder {“1”,”10”,”100”,”1000”,”10000”,...}.

Eine **Klasse** ist eine Menge von Sprachen über dem gleichen Alphabet. Z.B. {{“0”, “1”},{“00”, “01”, “10”, “11”}}, oder die Menge der regulären Sprachen über {0,1}.

Maths Basics II

EXOR

Definiert als “Entweder-Oder”:

+	0	1
0	0	1
1	1	0

Auf bit-Strings bitweise anzuwenden.
Dort hat es die wunderbare Eigenschaft: a + b + b = a

2 = {0,1} ist mit + als Addition und AND als Multiplikation ein Körper.

Deshalb ist die Menge $\mathbf{2}^n$ der Länge-n bit-Strings ein **2**-Vektoraum.
Die Standardbasis für beispielsweise $\mathbf{2}^3$ ist {100,010,001}.

Zusammenfassung

DES als Blockchiffre (Blocklänge 64, Schlüssellänge 56)

Betriebs-Modi für Blockchiffren: ECB, CBC, CFB, OFB