共通鍵暗号

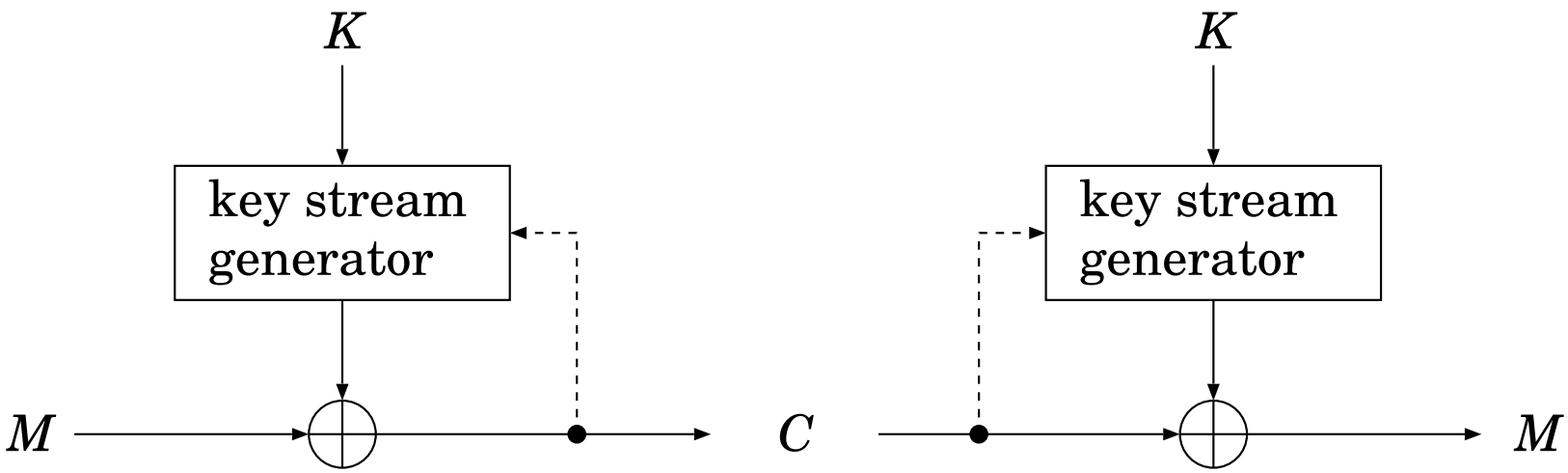
廣瀬勝一

ブロック暗号とストリーム暗号

ブロック暗号　平文・暗号文の文字の集まりに作用する.

ストリーム暗号　平文・暗号文の個々の文字に作用する.

例)



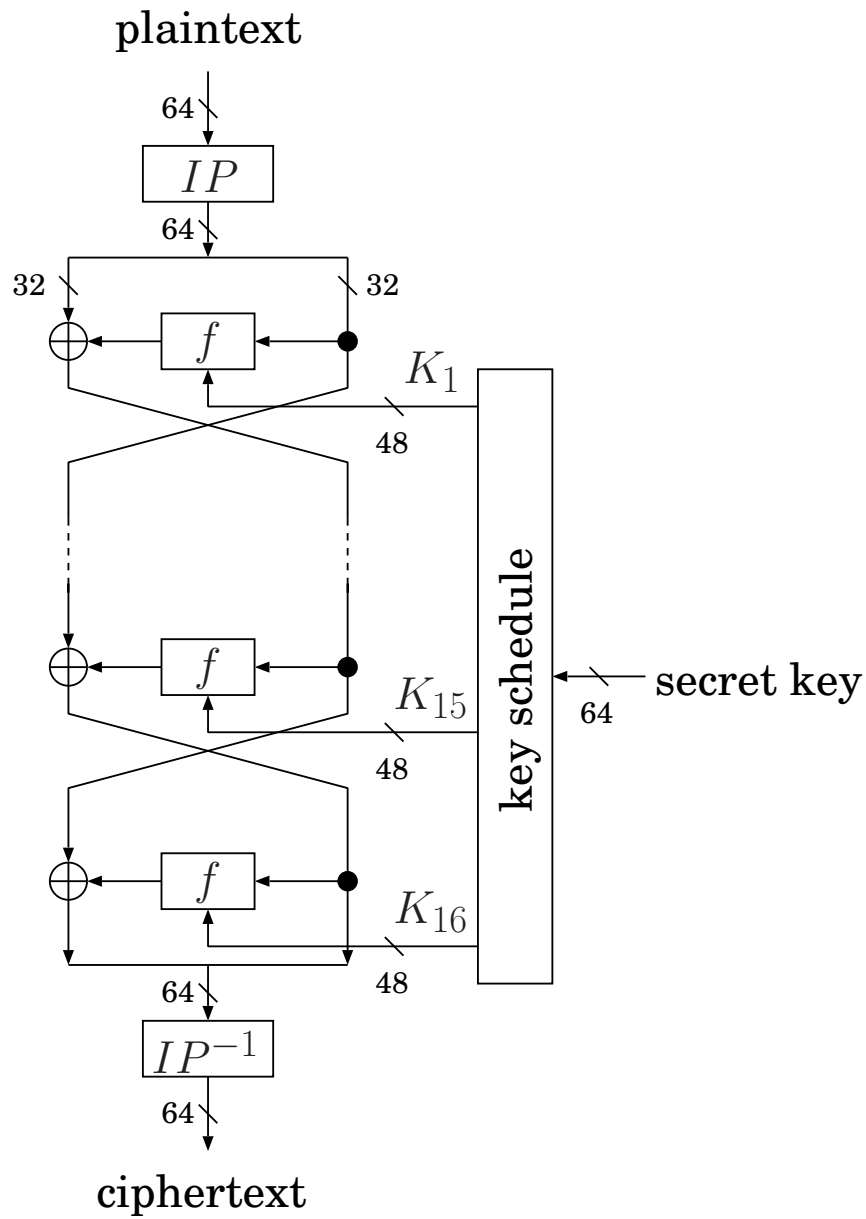
DES (Data Encryption Standard，データ暗号化標準)

IBM，1975 年

Feistel 構造

ブロック長は 64 ビット
（平文・暗号文の長さ）

鍵長は 64 ビット
（8 ビットはパリティ）

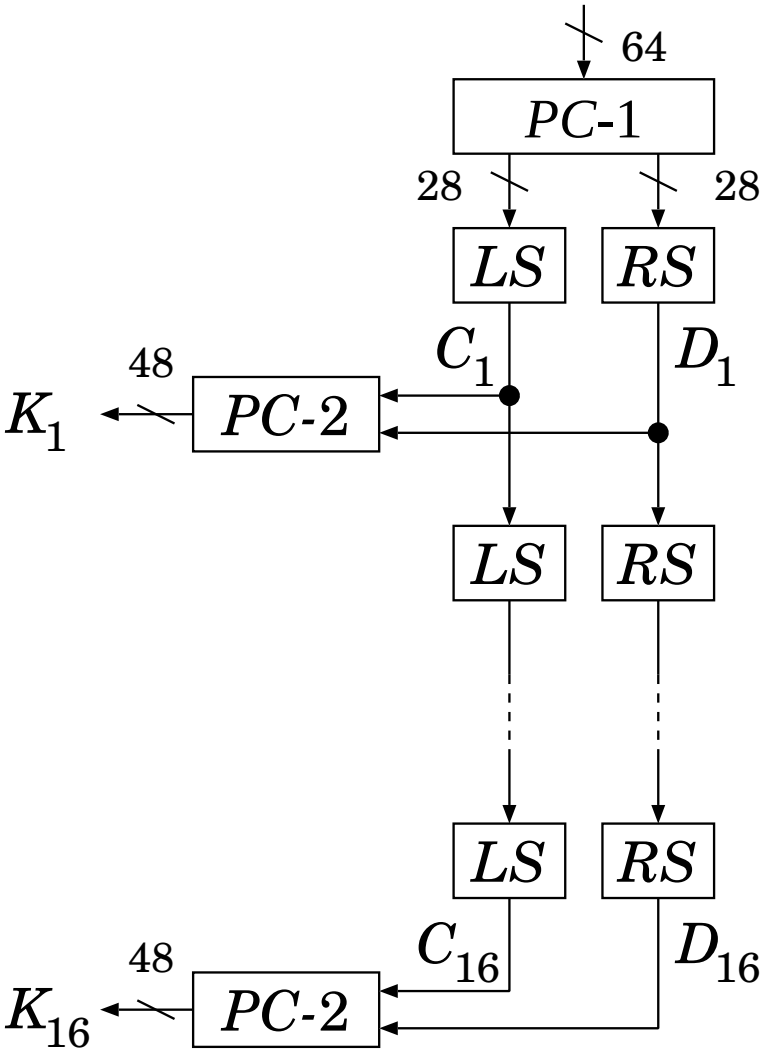


IP（初期転置）

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

例）32 番目の出力ビットは 8 番目の入力ビットである.

鍵スケジュール (1/2)



LS (shift left)

1	2	3	4	5	6	7	8
1	1	2	2	2	2	2	2
9	10	11	12	13	14	15	16
1	2	2	2	2	2	2	1

RS (shift right)

1	2	3	4	5	6	7	8
0	1	2	2	2	2	2	2
9	10	11	12	13	14	15	16
1	2	2	2	2	2	2	1

鍵スケジュール (2/2)

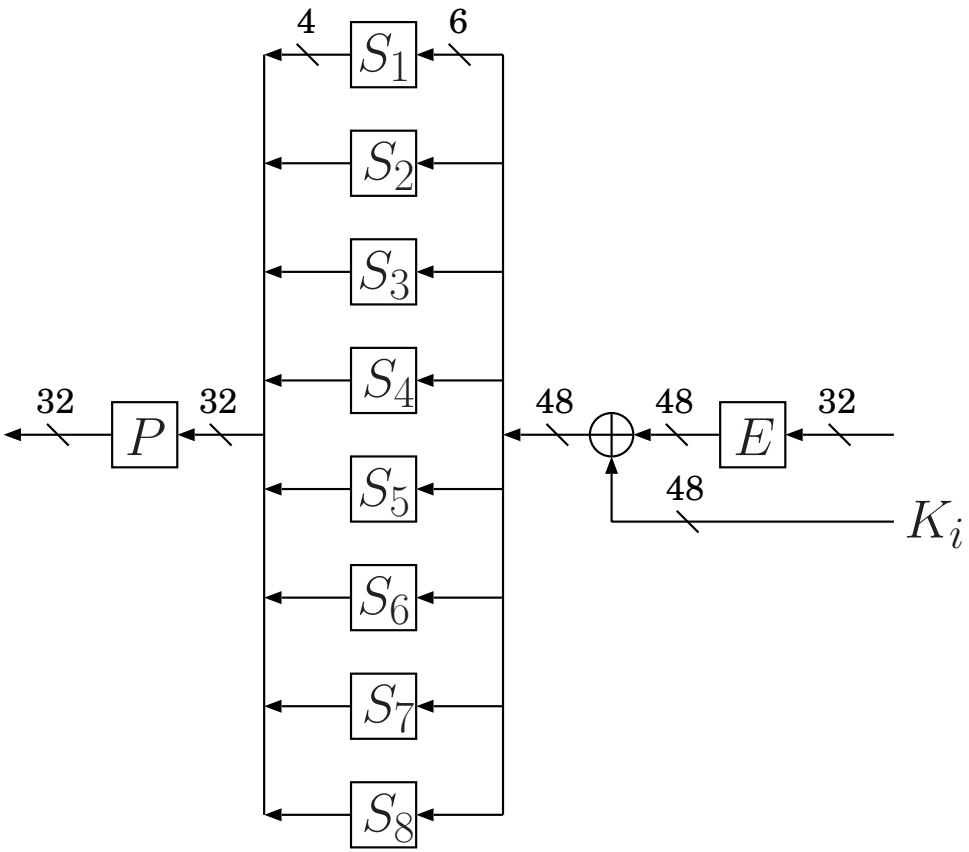
$PC\text{-}1 : \{0,1\}^{64} \to \{0,1\}^{56}$

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

$PC\text{-}2 : \{0,1\}^{56} \to \{0,1\}^{48}$

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

f 関数



- E は拡大関数
- P は転置
- S_i は S ボックス（換字ボックス）

S ボックスは DES の唯一の非線形変換である.

拡大関数 E と転置 P

$E : \{0,1\}^{32} \to \{0,1\}^{48}$

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

$P : \{0,1\}^{32} \to \{0,1\}^{32}$

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

S ボックス

$S_i(b_1, b_2, b_3, b_4, b_5, b_6)$ で (b_1, b_6) は行，(b_2, b_3, b_4, b_5) は列を指定する．

S_1

E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D

S_2

F	1	8	E	6	B	3	4	9	7	2	D	C	0	5	A
3	D	4	7	F	2	8	E	C	0	1	A	6	9	B	5
0	E	7	B	A	4	D	1	5	8	C	6	9	3	2	F
D	8	A	1	3	F	4	2	B	6	7	C	0	5	E	9

S ボックス

S_3

A	0	9	E	6	3	F	5	1	D	C	7	B	4	2	8
D	7	0	9	3	4	6	A	2	8	5	E	C	B	F	1
D	6	4	9	8	F	3	0	B	1	2	C	5	A	E	7
1	A	D	0	6	9	8	7	4	F	E	3	B	5	2	C

S_4

7	D	E	3	0	6	9	A	1	2	8	5	B	C	4	F
D	8	B	5	6	F	0	3	4	7	2	C	1	A	E	9
A	6	9	0	C	B	7	D	F	1	3	E	5	2	8	4
3	F	0	6	A	1	D	8	9	4	5	B	C	7	2	E

S_5

2	C	4	1	7	A	B	6	8	5	3	F	D	0	E	9
E	B	2	C	4	7	D	1	5	0	F	A	3	9	8	6
4	2	1	B	A	D	7	8	F	9	C	5	6	3	0	E
B	8	C	7	1	E	2	D	6	F	0	9	A	4	5	3

S ボックス

S_6

C	1	A	F	9	2	6	8	0	D	3	4	E	7	5	B
A	F	4	2	7	C	9	5	6	1	D	E	0	B	3	8
9	E	F	5	2	8	C	3	7	0	4	A	1	D	B	6
4	3	2	C	9	5	F	A	B	E	1	7	6	0	8	D

S_7

4	B	2	E	F	0	8	D	3	C	9	7	5	A	6	1
D	0	B	7	4	9	1	A	E	3	5	C	2	F	8	6
1	4	B	D	C	3	7	E	A	F	6	8	0	5	9	2
6	B	D	8	1	4	A	7	9	5	0	F	E	2	3	C

S_8

D	2	8	4	6	F	B	1	A	9	3	E	5	0	C	7
1	F	D	8	A	3	7	4	C	5	6	B	0	E	9	2
7	B	4	1	9	C	E	2	0	6	A	D	F	3	5	8
2	1	E	7	4	A	8	D	F	C	9	0	3	5	6	B

暗号解析

Kerckhoff の原理

暗号解析者はどのような暗号方式が使用されているかを知っている.

攻撃

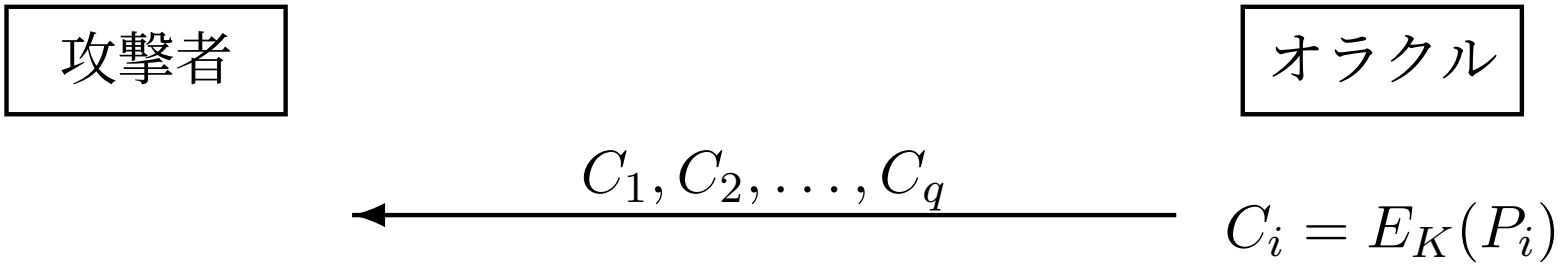
- 暗号文単独攻撃 (ciphertext-only attack)
- 既知平文攻撃 (known-plaintext attack)
- 選択平文攻撃 (chosen-plaintext attack)
- 選択暗号文攻撃 (chosen-ciphertext attack)

目標

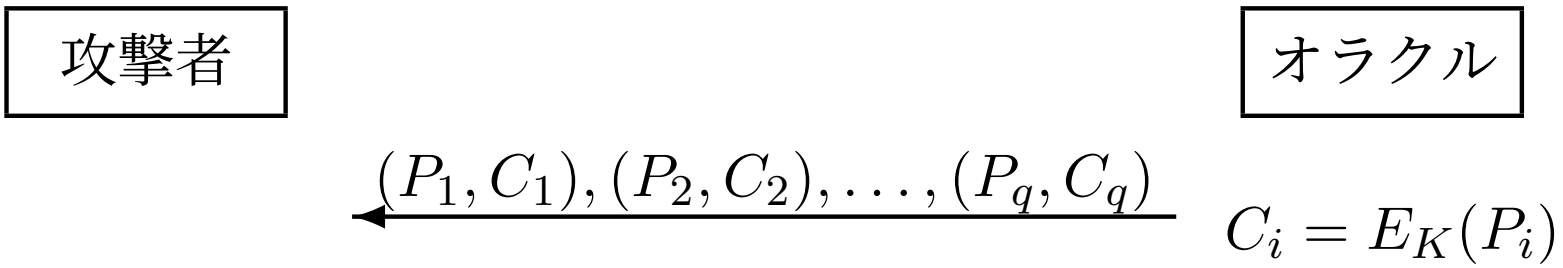
- 鍵の回復 (key recovery)
- 識別 (distinguishing)　無作為に選択された置換との識別

暗号文単独攻撃と既知平文攻撃

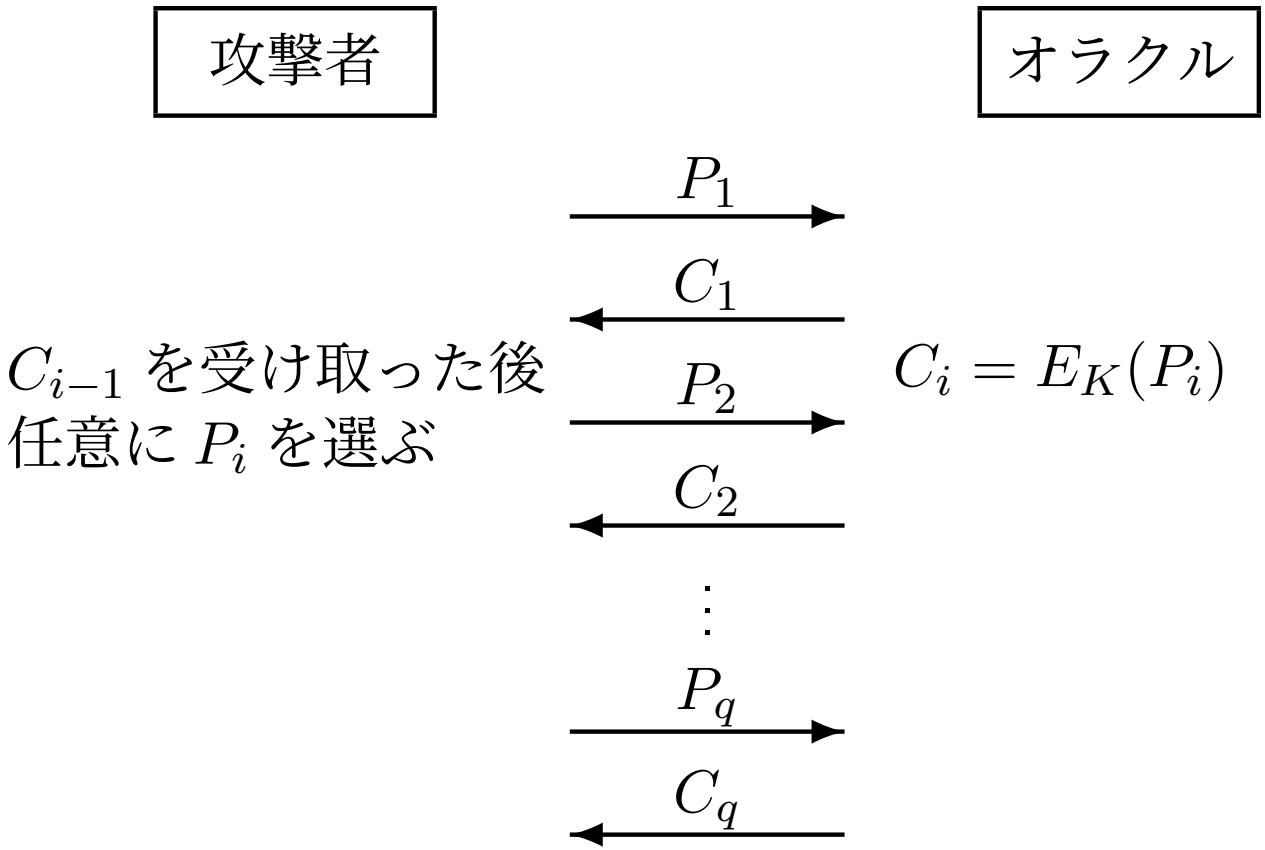
暗号文単独攻撃



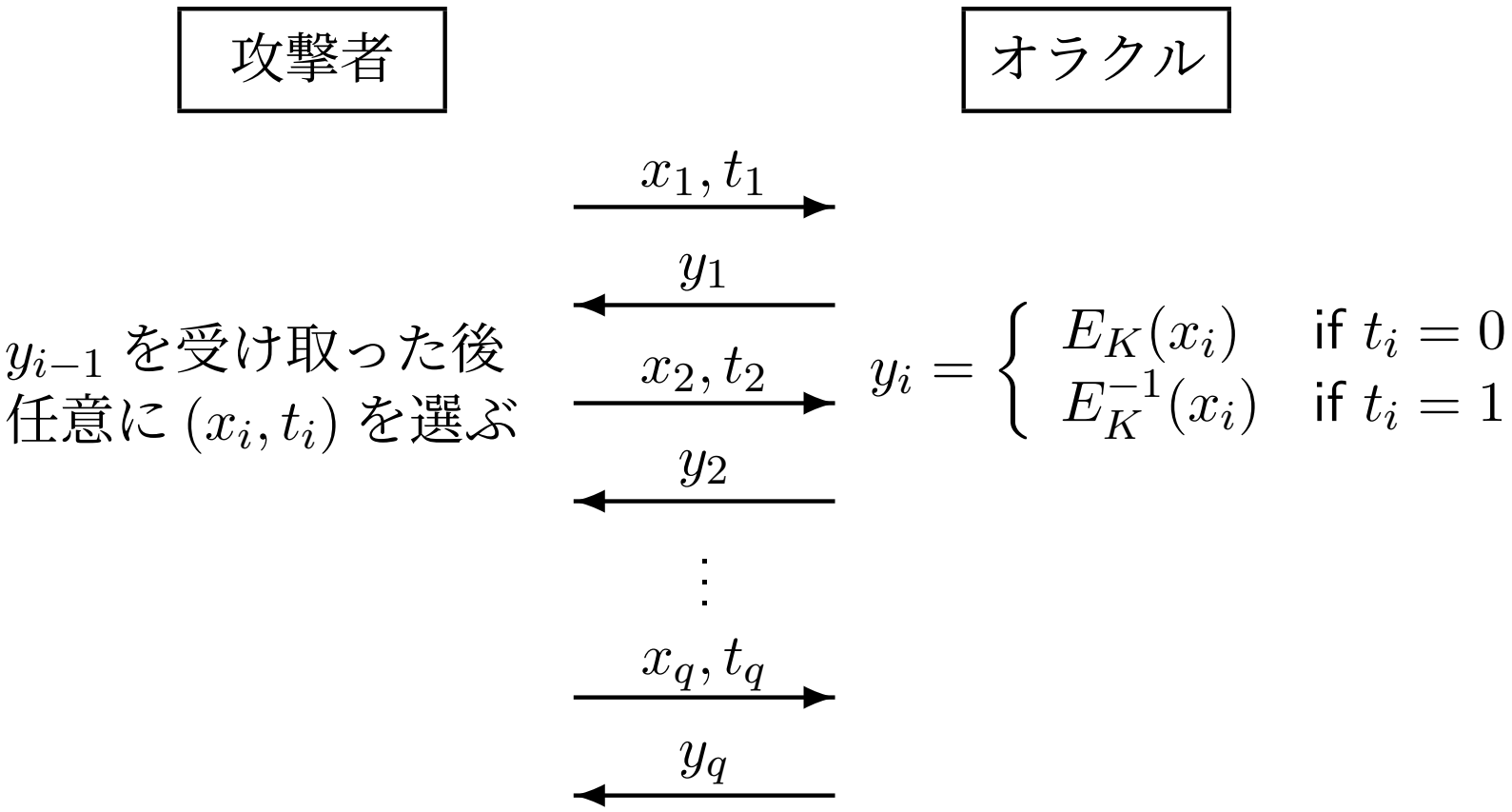
既知平文攻撃



選択平文攻撃



選択暗号文攻撃


攻撃者
オラクル
x_1, t_1
y_1
y_{i-1} を受け取った後
任意に (x_i, t_i) を選ぶ
x_2, t_2
y_2
x_q, t_q
y_q
$y_i = \begin{cases} E_K(x_i) & \text{if } t_i = 0 \\ E_K^{-1}(x_i) & \text{if } t_i = 1 \end{cases}$

ブロック暗号に対する二つの強力な暗号解読法

差分解読 (differential cryptanalysis) (1990, Biham & Shamir)
　選択平文攻撃

線形解読 (linear cryptanalysis) (1993, Matsui)
　既知平文攻撃

1994 年，線形解読法により，2^{43} 個の平文と暗号文の組を用いて，DES が解読された（暗号化に用いられた秘密鍵が特定された）.

鍵の全数探索

1999 年，“DES Cracker” と呼ばれる専用ハードウェアと 10 万台の計算機を用いて，22 時間 15 分で一組の平文と暗号文の暗号化に用いられた秘密鍵が特定された. (1 秒当り 2450 億個の鍵が検査された)
(`http://www.eff.org/descracker/`)

DES を利用する場合は，3 重暗号

$$E_{K_3}(D_{K_2}(E_{K_1}(\cdot)))$$

が推奨されている.

- $K_1 = K_3$ でも良い.
- $K_1 = K_2$ のときは通常の暗号化と同じ.

環 (Ring)

集合 R について，二つの演算 $+$ と $\cdot$ が定義され，以下の条件が満たされるとき，R は環と呼ばれる．なお，$+$ は加法，$\cdot$ は乗法と呼ばれる．

- R は加法について可換群をなす．
  - R が加法 $+$ について群をなす．
  - 任意の $a, b \in R$ について，$a + b = b + a$.
- R は乗法について閉じている．
- R の乗法が結合則を満たす．
  - 任意の $a, b, c \in R$ について，$(ab)c = a(bc)$.
- R は乗法に関する単位元を持つ．
- 分配則が成立する．即ち，任意の $a, b, c \in R$ について，

$$(a + b) \cdot c = a \cdot c + a \cdot c \qquad a \cdot (b + c) = a \cdot b + a \cdot c$$

R の乗法が可換であるとき，R は可換環と呼ばれる．

例

例 1）$\mathbb{Z}$ は，加法と乗法について（可換）環をなす.

例 2）各要素が実数の n 次正方行列の集合は，加法と乗法について環をなす．可換環ではない.

例 3）$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ は，法 n の加法と乗法について（可換）環をなす.

- $\mathbb{Z}_n$ は法 n の加法について可換群をなす.
- $\mathbb{Z}_n$ は法 n の乗法について閉じている.
- 法 n の乗法は結合則を満たす.
- 1 は法 n の乗法についての単位元である.
- 分配則が成立する.

例

R を可換環とする.

$R[x]$ を R の要素を係数とする多項式の集合とする.
$R[x]$ は環をなす.

例）$\mathbb{Z}_5[x]$
$f(x) = 3x^2 + 4x + 1$, $g(x) = 2x + 4$ のとき,

$$\begin{aligned} f(x) + g(x) &= 3x^2 + x \\ f(x) \cdot g(x) &= 6x^3 + 12x^2 + 8x^2 + 16x + 2x + 4 \\ &= x^3 + 3x + 4 \end{aligned}$$

係数の加法と乗法は $\mathbb{Z}_5$ の加法と乗法によって行われる.

体 (Field)

集合 F について，加法 $+$ と乗法 $\cdot$ が定義され，以下の条件が満たされるとき，F は体と呼ばれる．

- F は可換環をなす．
- すべての $a \in F \setminus \{0\}$ に対して，乗法についての逆元 a^{-1} が存在する．ここで，0 は加法についての F の単位元である．

体 F の別の定義

- F は加法について可換群をなす．
- $F \setminus \{0\}$ は乗法について可換群をなす．
- 分配則が成立する．

例

例 1）$\mathbb{Q}, \mathbb{R}$ は加算，乗算について体をなす.

例 2）n が素数であるとき，またそのときに限り $\mathbb{Z}_n$ は法 n の加算，乗算について体をなす.

n が素数でないとき，$\forall a \in \mathbb{Z}_n \setminus \{0\}$ について

- $\gcd(a, n) = 1 \Rightarrow a \cdot b \bmod n = 1$ を満たす $b \in \mathbb{Z}_n$ が存在する
- $\gcd(a, n) \neq 1 \Rightarrow \forall b \in \mathbb{Z}_n$ について $a \cdot b \bmod n \neq 1$

例）$n = 15 = 3 \times 5$ について

- $2^{-1} = 8, 7^{-1} = 13$
- 6 の逆元は存在しない

有限体

元の個数が有限の体

素体 $\mathrm{GF}(q)$

- 素数 q について，$\mathbb{Z}_q$ と q を法とする加算，乗算による体

素体の拡大体 $\mathrm{GF}(q^m)$

- $\mathbb{Z}_q$ の元を係数とする $m-1$ 次以下のすべての多項式の集合からなる
- 多項式の係数の演算は $\mathrm{GF}(q)$ の演算と同一
- 多項式の乗算はある m 次の既約多項式を法とする

$\mathrm{GF}(q^m)$ の例

$\mathrm{GF}(2^3)$

- 元の集合は $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$
- 3 次の既約多項式 $x^3 + x + 1$ を法とする乗法を考える.

加算の例

$$(x^2 + x) + (x^2 + 1) = x + 1$$

乗算の例

$$\begin{aligned}(x^2 + x)(x^2 + 1) &= x^4 + x^2 + x^3 + x \\ &= (x^2 + x) + x^2 + (x + 1) + x \\ &= x + 1\end{aligned}$$

$\mathrm{GF}(q^m)$ の例

除算 $f/g = f \cdot g^{-1}$

乗算に関する逆元

f	f^{-1}
1	1
x	x^2+1
$x+1$	x^2+x
x^2	x^2+x+1
x^2+1	x
x^2+x	$x+1$
x^2+x+1	x^2

AES (Advanced Encryption Standard)

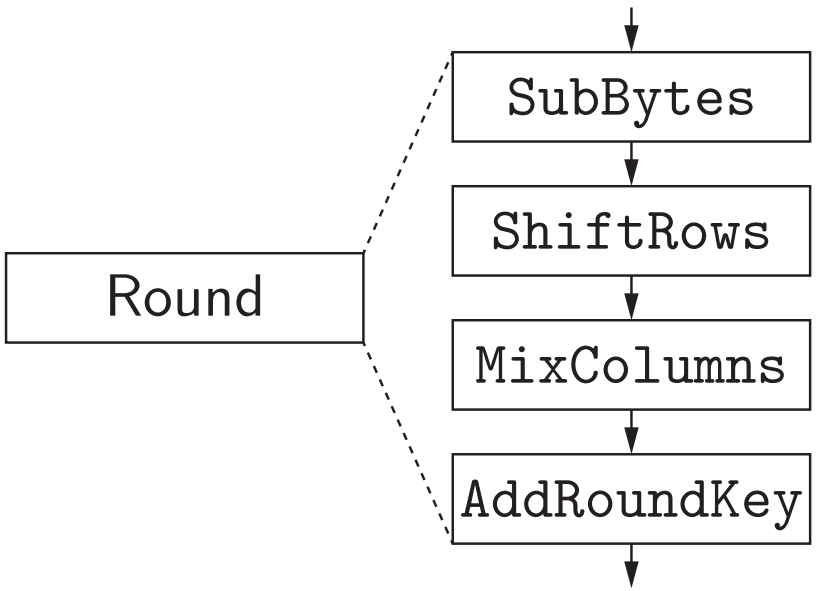
Rijndael (Daemen & Rijmen, 1998)

SPN 構造 (Substitution-Permutation Network)

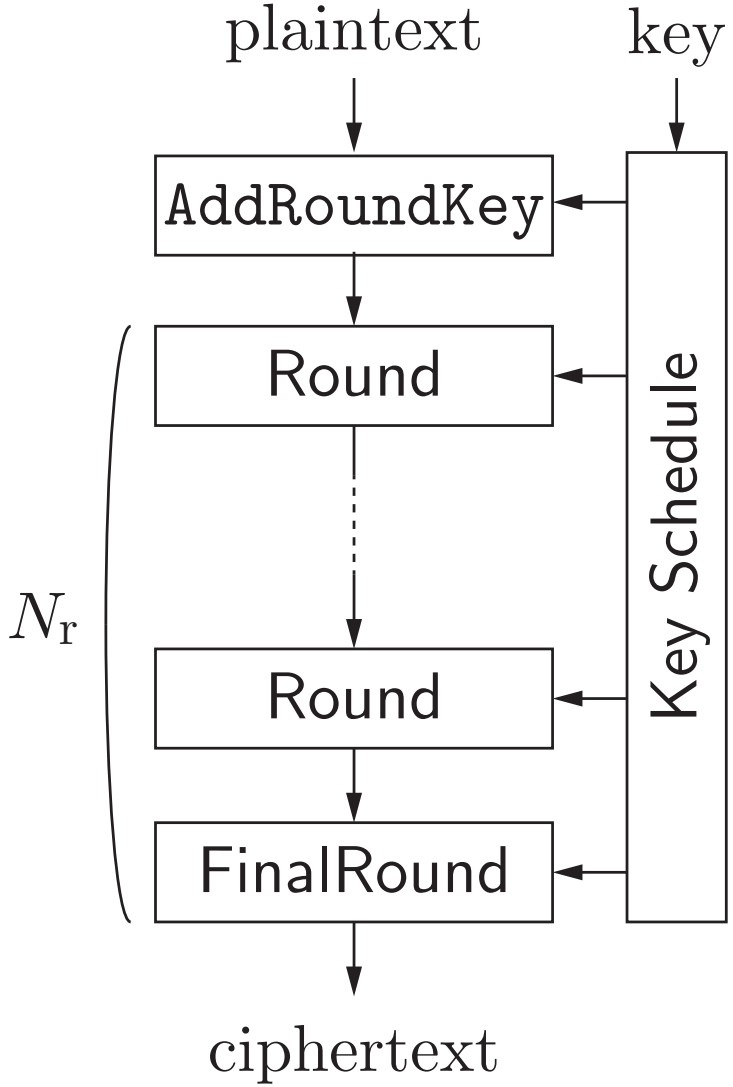
ブロック長　128 ビット

鍵長　128, 192, 256 ビット

鍵長	128	192	256
N_r	10	12	14



FinalRound は `MixColumns` を省略



状態

4 種類の変換 (`AddRoundKey`, `SubBytes`, `ShiftRows`, `MixColumns`) は状態に対して適用される.

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

- 各バイト $s_{i,j} \in \{0,1\}^8$ は $\mathrm{GF}(2^8)$ の要素と見なされる.
- 乗法は $x^8 + x^4 + x^3 + x + 1$ を法とする.

初期状態

m_0	m_4	m_8	m_{12}
m_1	m_5	m_9	m_{13}
m_2	m_6	m_{10}	m_{14}
m_3	m_7	m_{11}	m_{15}

$m = (m_0, m_1, \ldots, m_{15})$ は平文であり，$m_i \in \{0,1\}^8$ である．

SubBytes

AES の唯一の非線形変換である.

S ボックス $\mathrm{S}_{\mathrm{RD}} : \{0,1\}^8 \to \{0,1\}^8$

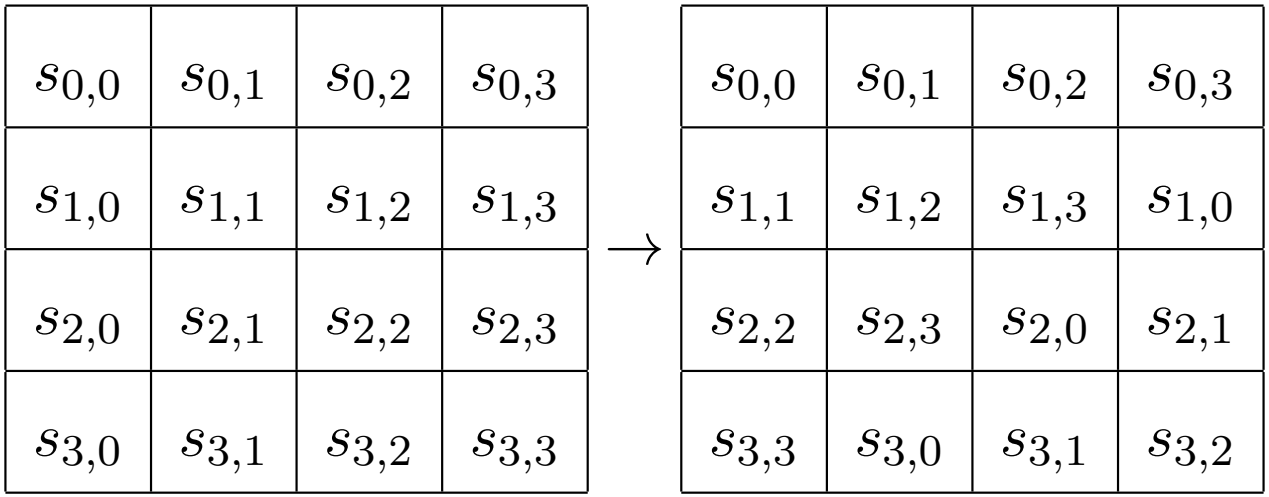
$$\mathrm{S}_{\mathrm{RD}}(s_{i,j}) = f(g(s_{i,j})),$$

ここで,

$$g(\alpha) = \begin{cases} \alpha^{-1} & \text{if } \alpha \neq 00 \\ 00 & \text{if } \alpha = 00 \end{cases}$$

$$f(y) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} y^{\mathrm{T}} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

ShiftRows



第 i 行目を i 個左巡回シフトする.

MixColumns (1/2)

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$\rightarrow$

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

$$\begin{pmatrix} b_{3,i} \\ b_{2,i} \\ b_{1,i} \\ b_{0,i} \end{pmatrix} = \begin{pmatrix} 02 & 01 & 01 & 03 \\ 03 & 02 & 01 & 01 \\ 01 & 03 & 02 & 01 \\ 01 & 01 & 03 & 02 \end{pmatrix} \begin{pmatrix} a_{3,i} \\ a_{2,i} \\ a_{1,i} \\ a_{0,i} \end{pmatrix}$$

MixColumns (2/2)

前ページの計算では，各列が $\mathrm{GF}(2^8)$ 上の多項式と見なされ，次式が計算されていることになる．

$$b_i(x) = c(x)\, a_i(x) \bmod x^4 + 1$$

ここで

$$c(x) = \mathtt{03}\, x^3 + \mathtt{01}\, x^2 + \mathtt{01}\, x + \mathtt{02}$$

であり，$1 \leq i \leq 4$ について

$$a_i(x) = a_{3,i}x^3 + a_{2,i}x^2 + a_{1,i}x + a_{0,i}$$
$$b_i(x) = b_{3,i}x^3 + b_{2,i}x^2 + b_{1,i}x + b_{0,i}$$

である．

AddRoundKey

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$\oplus$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

$\oplus$ はビットごとの排他的論理和 XOR である.

鍵スケジュール (1/2)

鍵長 128 ビットの仕様を述べる

$w_{i,j} \in \{0,1\}^8$ $(0 \leq i \leq 3, 0 \leq j \leq 43)$

$0 \leq j \leq 43$ について $(w_{0,j}, w_{1,j}, w_{2,j}, w_{3,j})$ を計算

第 r ラウンドのラウンド鍵は K_r

K_0				K_1				
$w_{0,0}$	$w_{0,1}$	$w_{0,2}$	$w_{0,3}$	$w_{0,4}$	$w_{0,5}$	$w_{0,6}$	$w_{0,7}$	
$w_{1,0}$	$w_{1,1}$	$w_{1,2}$	$w_{1,3}$	$w_{1,4}$	$w_{1,5}$	$w_{1,6}$	$w_{1,7}$	$\cdots$
$w_{2,0}$	$w_{2,1}$	$w_{2,2}$	$w_{2,3}$	$w_{2,4}$	$w_{2,5}$	$w_{2,6}$	$w_{2,7}$	
$w_{3,0}$	$w_{3,1}$	$w_{3,2}$	$w_{3,3}$	$w_{3,4}$	$w_{3,5}$	$w_{3,6}$	$w_{3,7}$	

鍵スケジュール (2/2)

$0 \le j \le 43$ について $(w_{0,j}, w_{1,j}, w_{2,j}, w_{3,j})$ の計算

1. $0 \le j \le 3$ について，$w_{i,j} = k_{i,j}$ $(0 \le i \le 3)$
2. $j \ge 4$ について

   $j \equiv 0 \pmod 4$ のとき

$$w_{i,j} = \begin{cases} w_{0,j-4} \oplus \mathrm{S_{RD}}(w_{1,j-1}) \oplus \mathrm{RC}(j/4) & (i = 0) \\ w_{i,j-4} \oplus \mathrm{S_{RD}}(w_{i+1 \bmod 4,j-1}) & (i = 1, 2, 3) \end{cases}$$

   $j \not\equiv 0 \pmod 4$ のとき

$$w_{i,j} = w_{i,j-4} \oplus w_{i,j-1}$$

ここで，$\mathrm{RC}(l) = x^{l-1} \bmod x^8 + x^4 + x^3 + x + 1$ $(1 \le l \le 10)$.

暗号利用モード

ブロック暗号を用いて任意長の平文を暗号化する方法

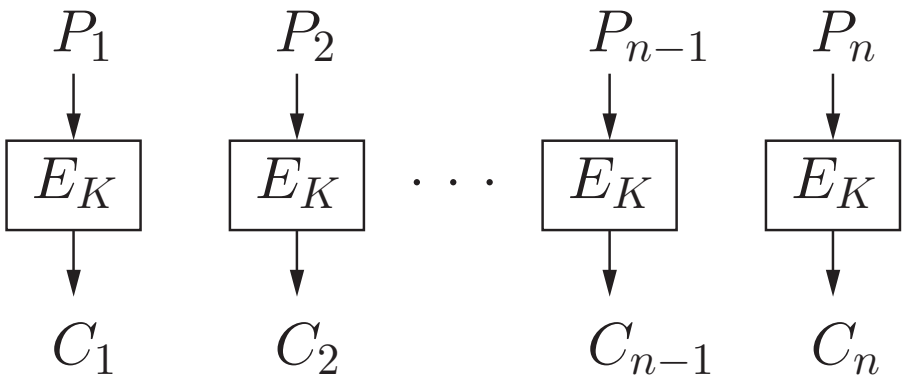
- Electronic codebook mode (ECB)
- Cipher block chaining mode (CBC)
- Cipher feedback mode (CFB)
- Output feedback mode (OFB)
- Counter mode (CTR)

CFB, OFB, CTR はストリーム暗号として働くモード

以降の表記法

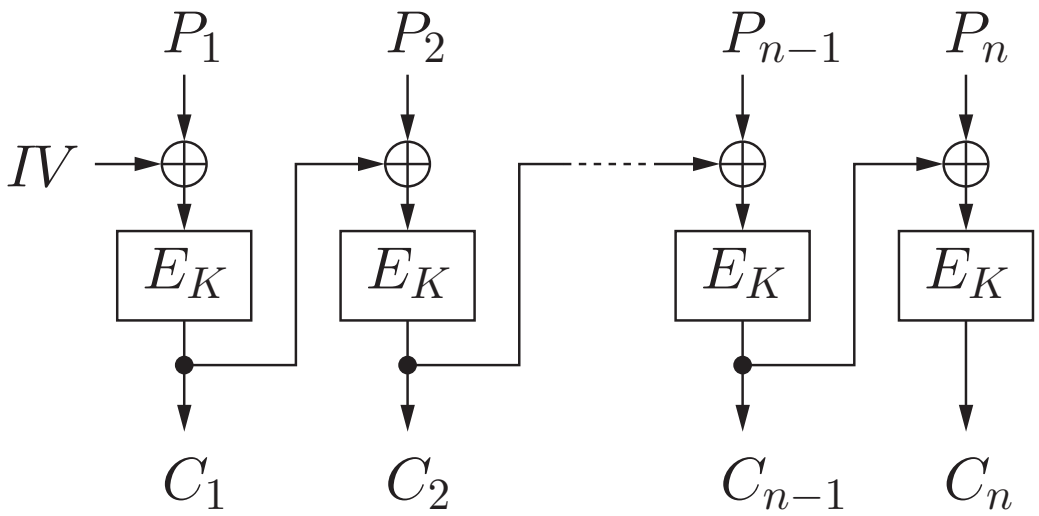
- msb_u は入力の上位 u ビットを出力する関数
- lsb_u は入力の下位 u ビットを出力する関数
- $x \| y$ は二値系列 x, y の連接

ECB



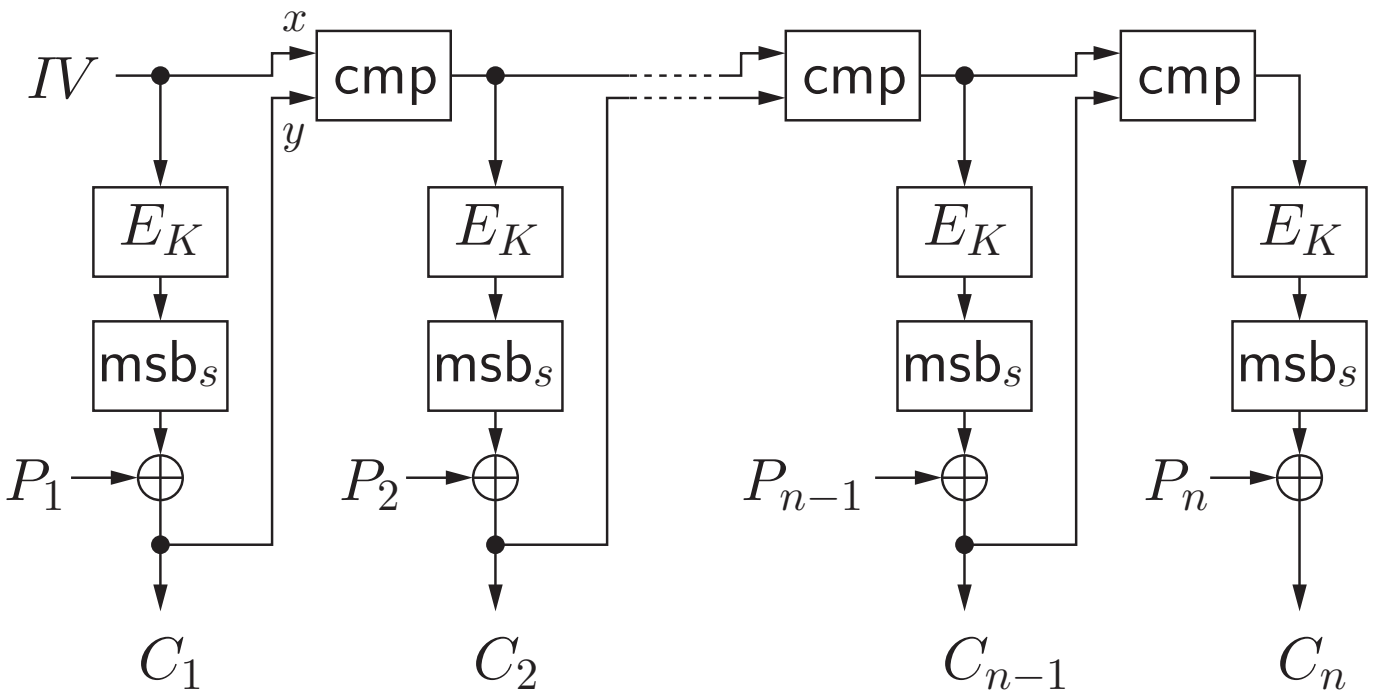
単にブロックごとに暗号化

CBC



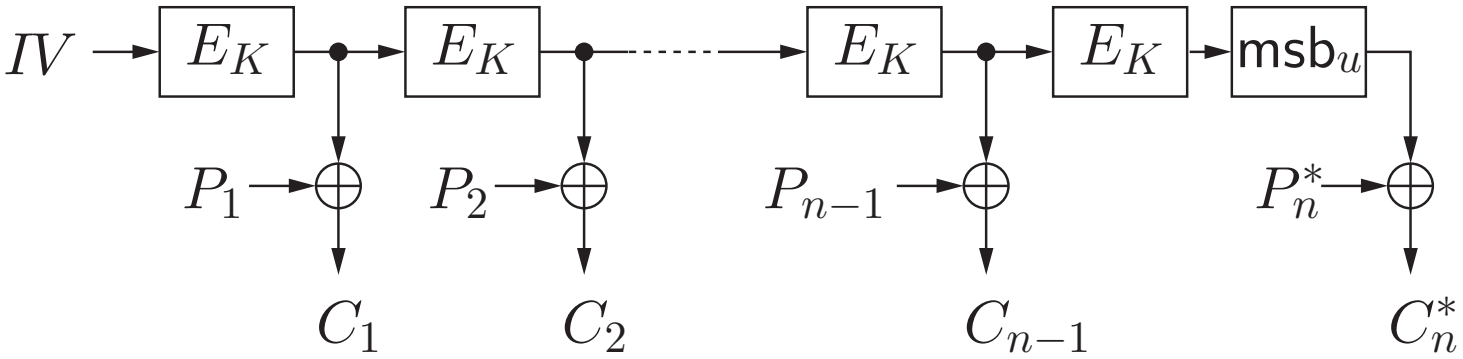
IV は初期ベクトル

CFB



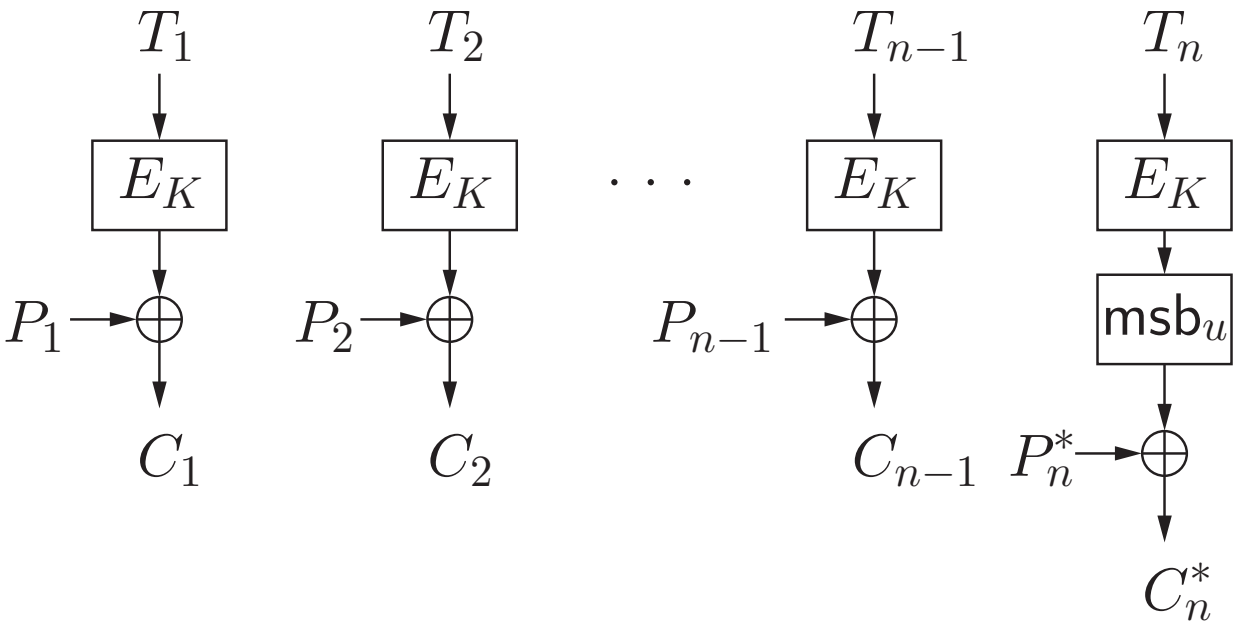
- IV は初期ベクトル
- $\mathsf{cmp}(x, y) = \mathsf{lsb}_{b-s}(x) \| y$（$b$ は E_K のブロック長）
- P_i, C_i の長さは s ビット

OFB



IV は初期ベクトル

CTR



T_i はカウンタの値

【例】$T_i \leftarrow T_{i-1} + 1$

演習問題

1. DES の暗号化関数が置換であることを証明せよ.
2. `MixColumns` の行列による計算と多項式による計算が等価であることを説明せよ.
3. AES の復号アルゴリズムを説明せよ.
4. 各暗号利用モードについて，復号法を説明せよ.