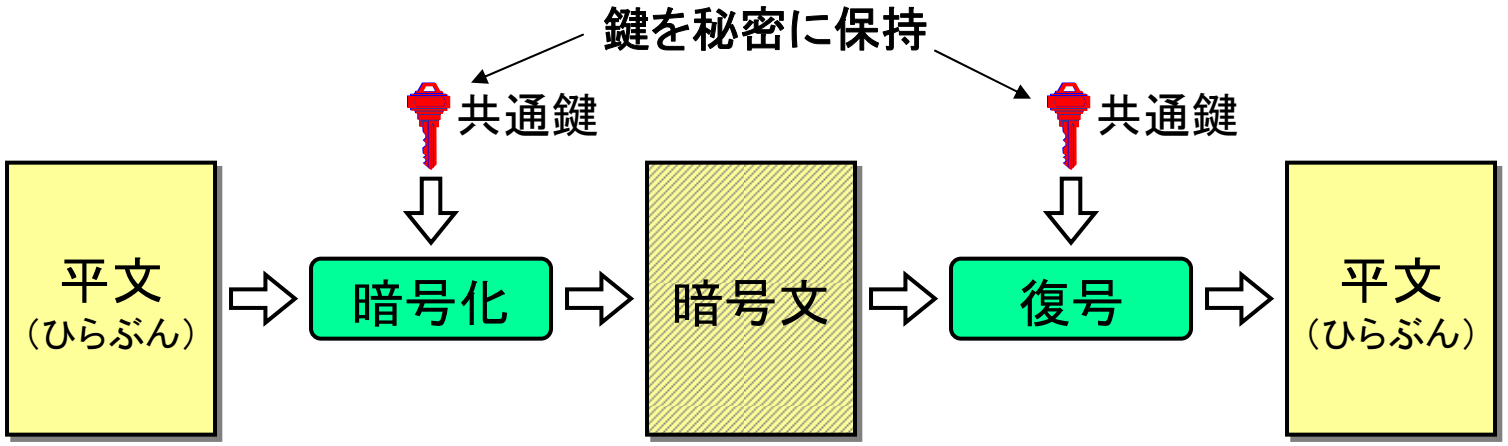
３．共通鍵暗号とDES暗号

共通鍵暗号

共通鍵暗号＝慣用暗号＝対称鍵暗号＝秘密鍵暗号



ブロック暗号

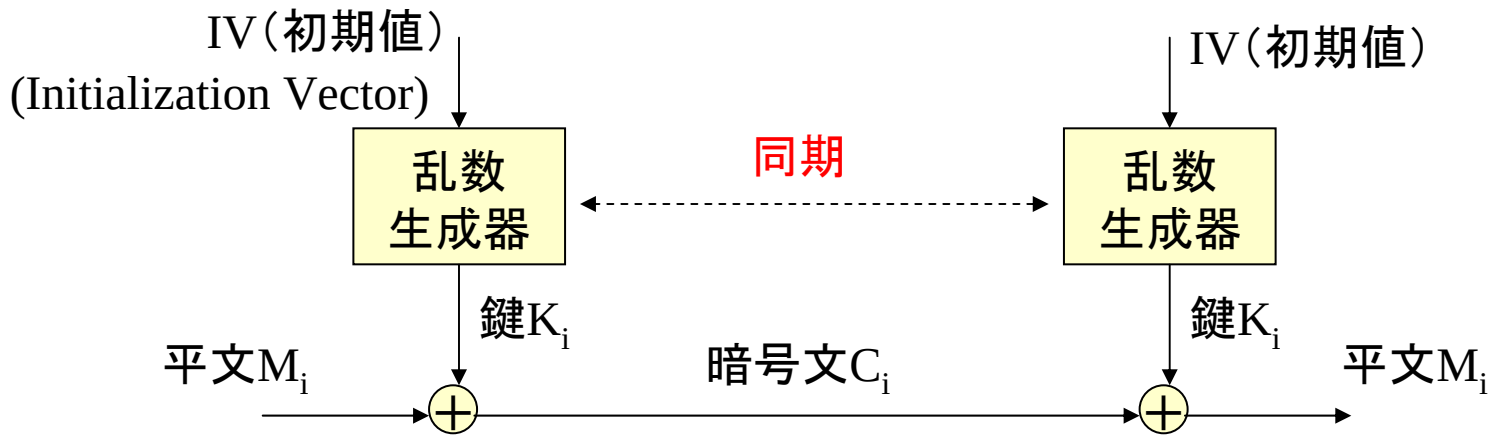
平文を一定のブロック長（64ビット、128ビット等）毎に区切って、
暗号化、復号を行う。

ストリーム暗号

平文を1ビット（または1文字）単位で、暗号化、復号を行う。

ストリーム暗号の仕組み（同期式）

同期式ストリーム暗号



送信側　　受信側

$C_i = M_i \oplus K_i$ ⟶ $M_i = C_i \oplus K_i$

$C_{i+1} = M_{i+1} \oplus K_{i+1}$ ⟶ ✕ 喪失

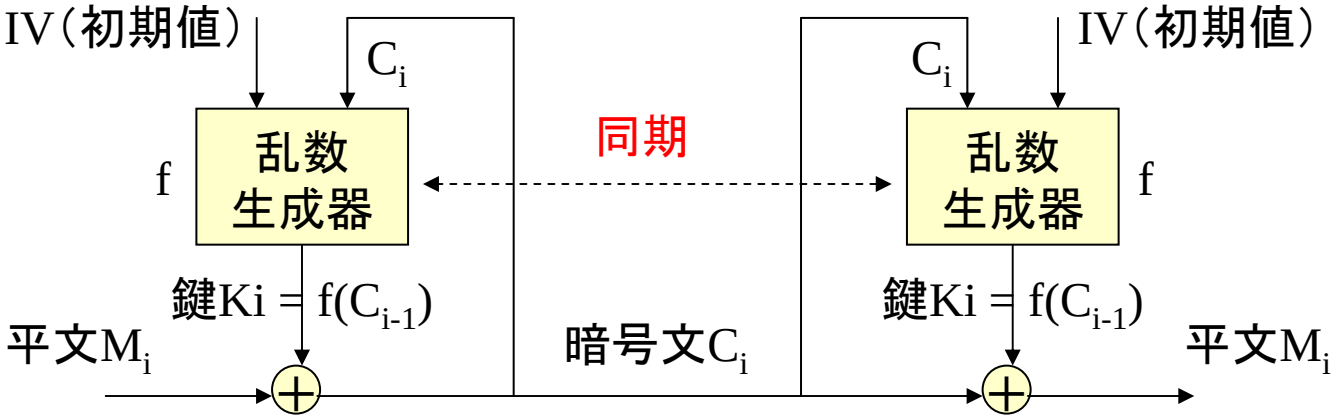
$C_{i+2} = M_{i+2} \oplus K_{i+2}$ ⟶ $M'_{i+2} = C_{i+2} \oplus K_{i+1}$　復号結果が異常

以降、すべて異常

（注）排他的論理和 $\begin{cases} 0 \oplus 0 = 0 & 0 \oplus 1 = 1 \\ 1 \oplus 0 = 1 & 1 \oplus 1 = 0 \end{cases}$

ストリーム暗号の仕組み（自己同期式）

自己同期式ストリーム暗号



送信側　　受信側

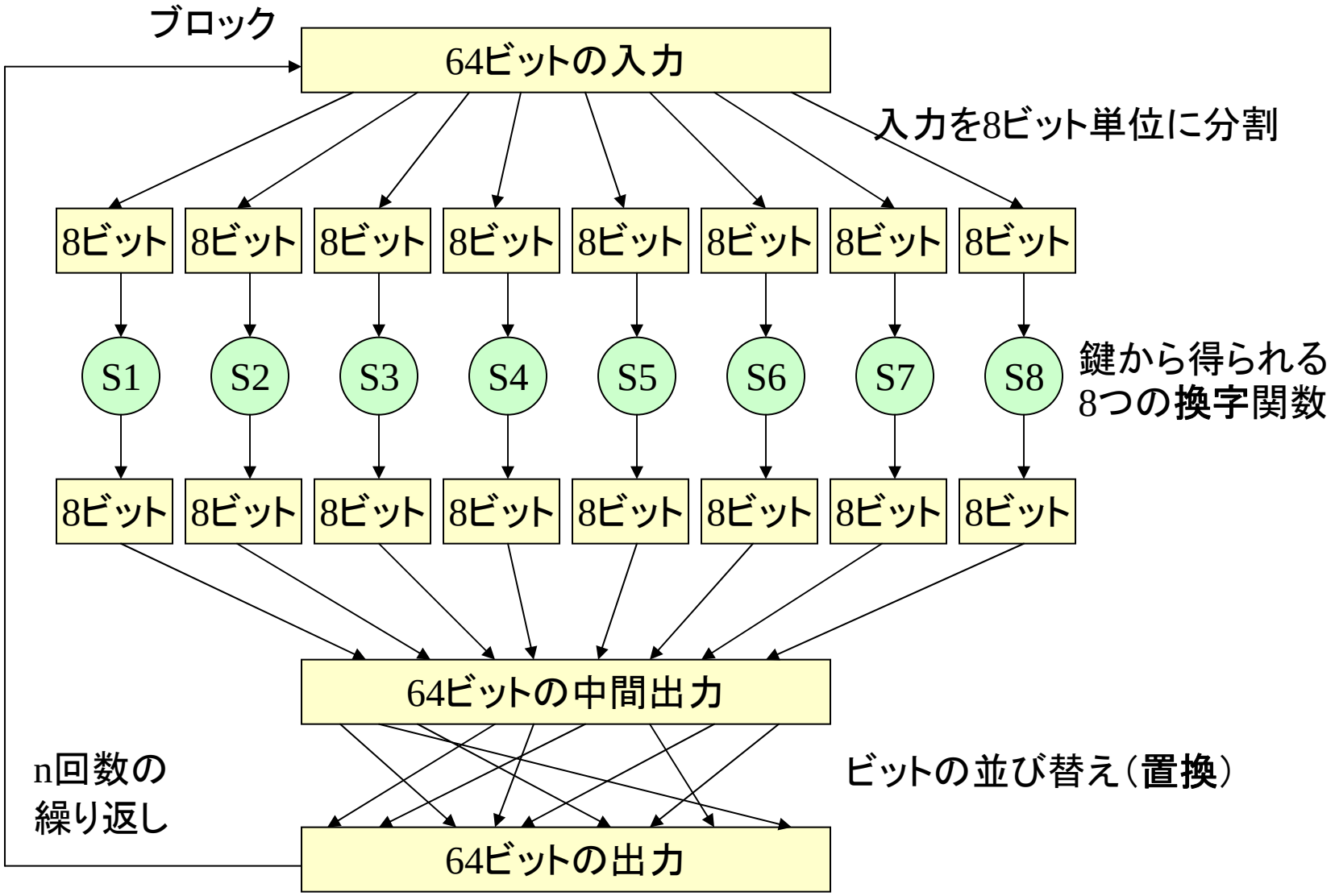
$C_i = M_i \oplus f(C_{i-1})$ ⟶ $M_i = C_i \oplus f(C_{i-1})$

$C_{i+1} = M_{i+1} \oplus f(C_i)$ ⟶ ✕ 喪失

$C_{i+2} = M_{i+2} \oplus f(C_{i+1})$ ⟶ $M'_{i+2} = C_{i+2} \oplus f(C_i)$　復号結果が異常

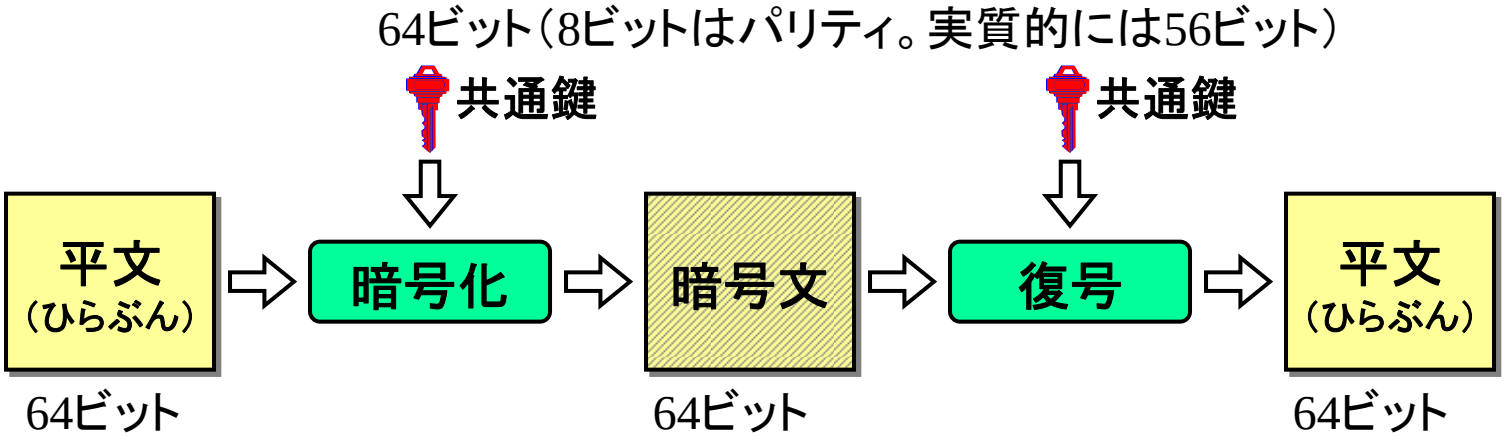
$C_{i+3} = M_{i+3} \oplus f(C_{i+2})$ ⟶ $M_{i+3} = C_{i+3} \oplus f(C_{i+2})$　正しく復号（同期回復）

ブロック暗号の仕組み


ブロック
64ビットの入力
入力を8ビット単位に分割
8ビット
8ビット
8ビット
8ビット
8ビット
8ビット
8ビット
8ビット
S1
S2
S3
S4
S5
S6
S7
S8
鍵から得られる
8つの換字関数
8ビット
8ビット
8ビット
8ビット
8ビット
8ビット
8ビット
8ビット
64ビットの中間出力
n回数の
繰り返し
ビットの並び替え（置換）
64ビットの出力

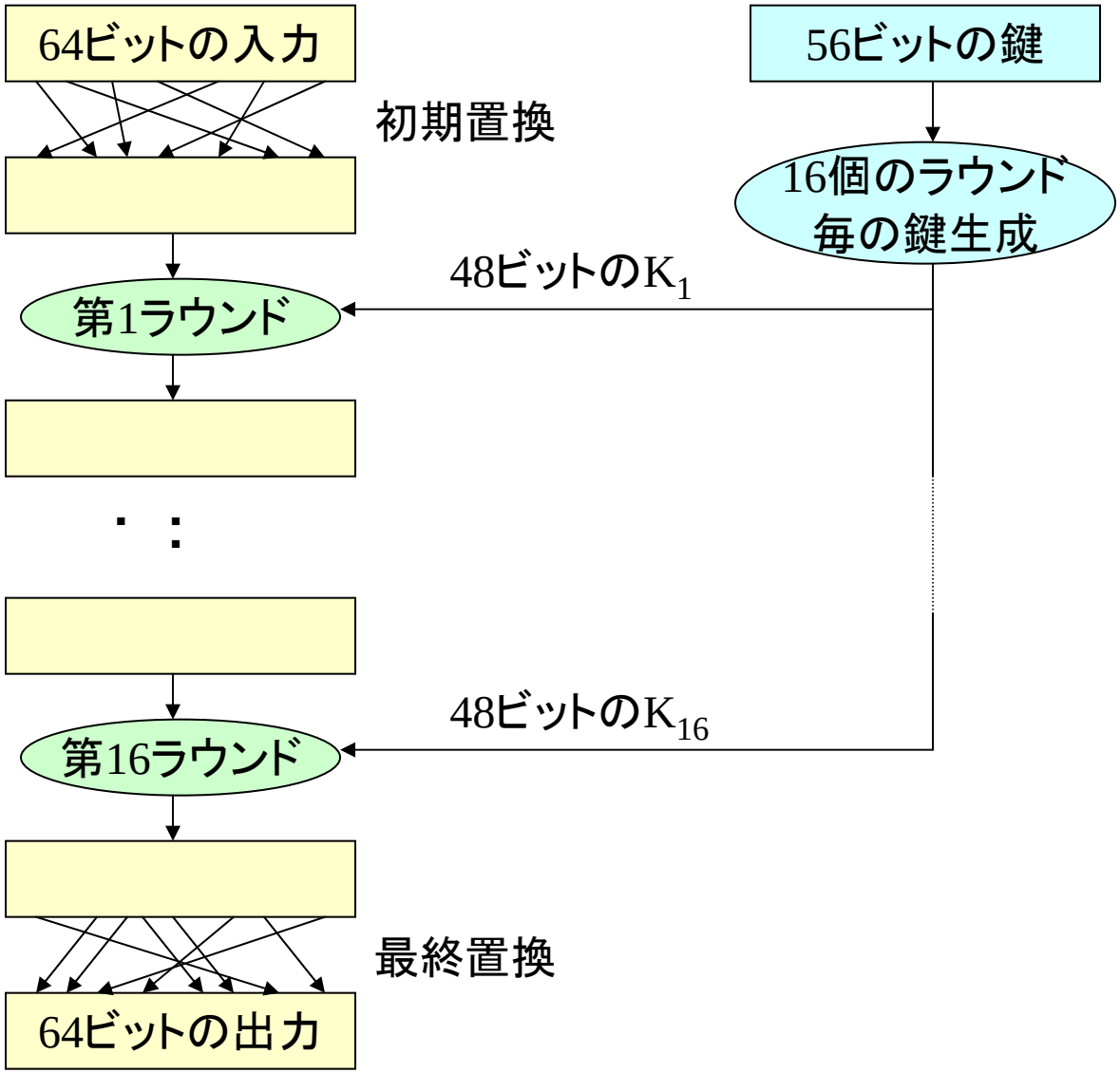
DES暗号

DES(Data Encryption Standard):
米国連邦政府の標準暗号。IBMにより1974年に開発。代表的な共通鍵暗号。



平文のうちの64ビット（1ブロック）を64ビットの鍵で、64ビット（1ブロック）の暗号文に変換

DESの基本構造


64ビットの入力
初期置換
56ビットの鍵
16個のラウンド
毎の鍵生成
48ビットのK1
第1ラウンド
48ビットのK16
第16ラウンド
最終置換
64ビットの出力

初期置換、最終置換

初期置換（IP）

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

最終置換（IP^{-1}）

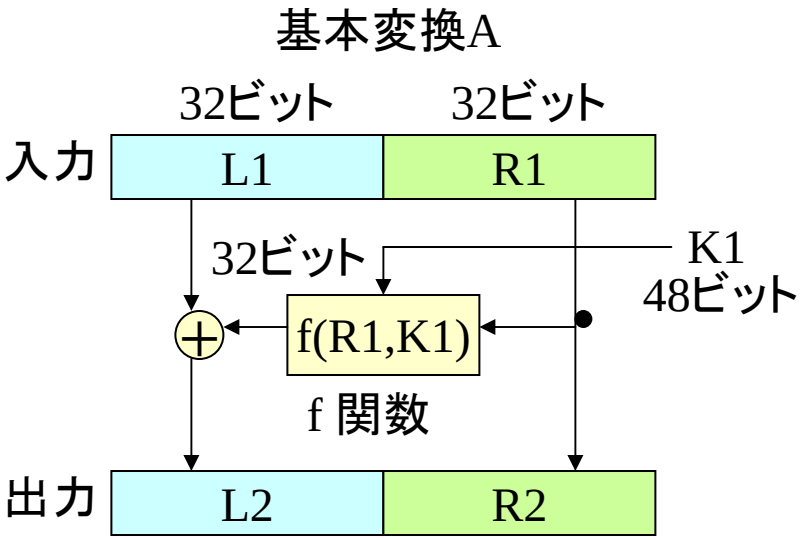
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

ます目の数字は置換前のビット位置

- 並び替えは規則的（安全性向上には無縁）
- 最終置換は初期置換の逆関数

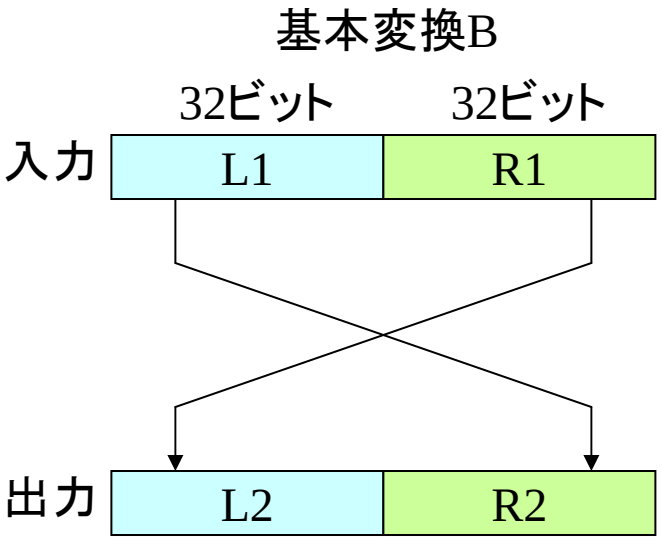
（例）入力の1ビット目は初期置換の40ビット目へ、その40ビット目は最終置換の1ビット目へ

基本変換（ラウンドでの変換）



$L2 = L1 \oplus f(R1,K1)$

$R2 = R1$



$L2 = R1$

$R2 = L1$

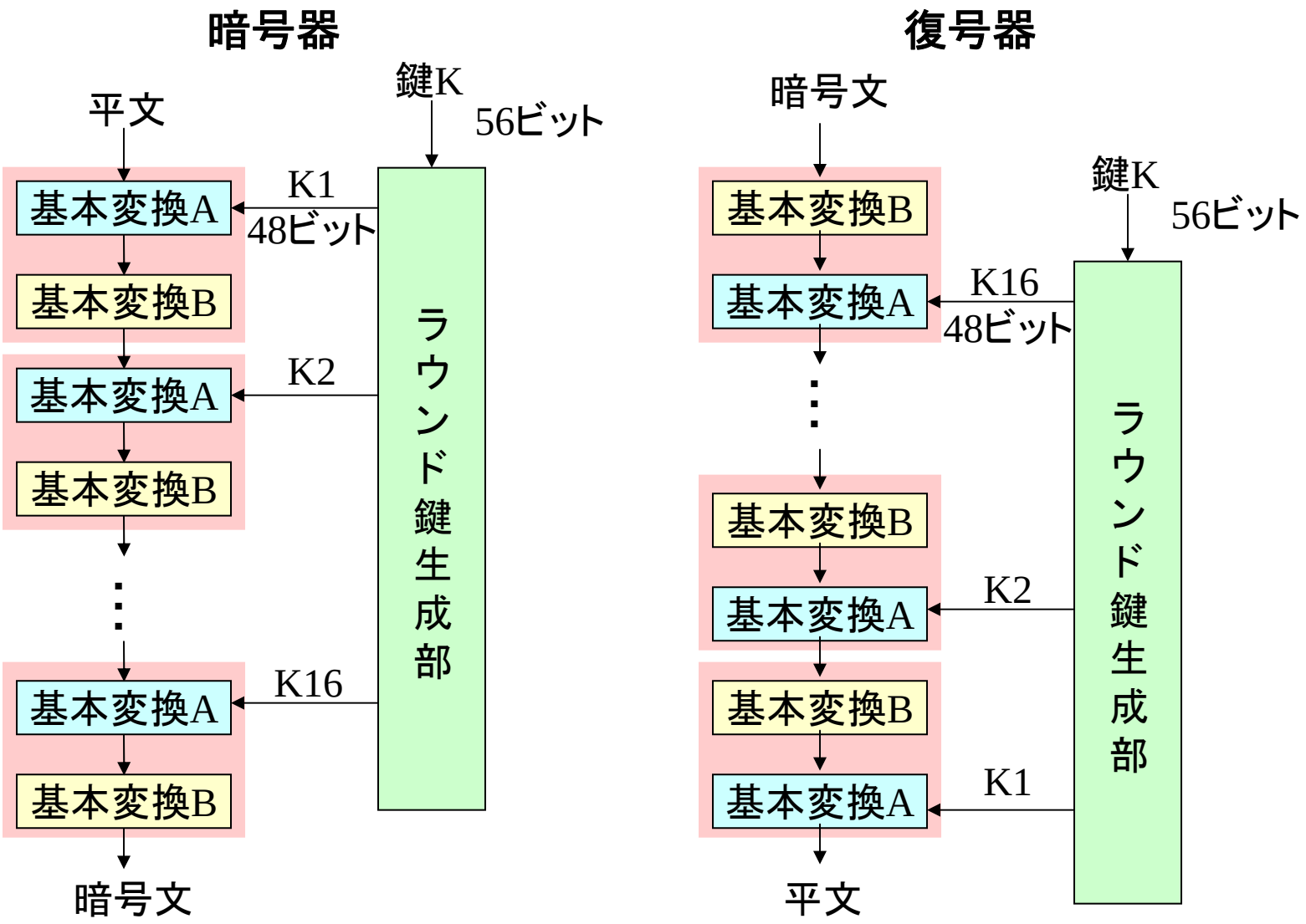
基本変換A、基本変換B それぞれは2回続けて実行すれば、元に戻る
（**インボリューション**：involution）

∵ 排他的論理和は2回続けて実行すれば、元に戻る

（例）

$$\begin{array}{r} 0101 \\ \oplus\ 1100 \\ \hline 1001 \end{array} \Rightarrow \begin{array}{r} 1001 \\ \oplus\ 1100 \\ \hline 0101 \end{array}$$

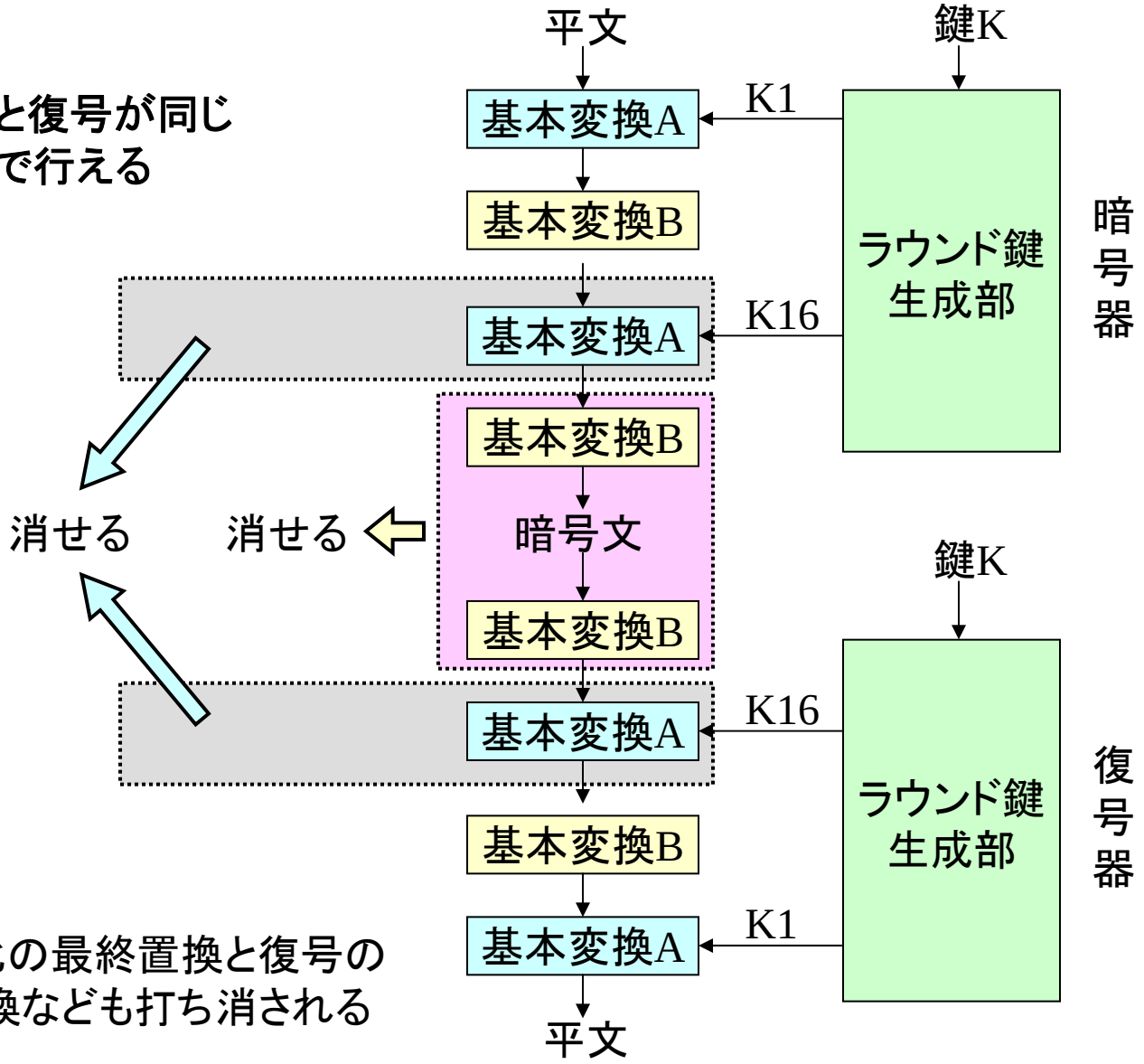
暗号器、復号器


暗号器
平文
鍵K
56ビット
基本変換A
基本変換B
K1
48ビット
K2
K16
ラウンド鍵生成部
暗号文
復号器
暗号文
鍵K
56ビット
K16
48ビット
K2
K1
ラウンド鍵生成部
平文

復号の仕組み

特徴

暗号化と復号が同じ
仕組みで行える



（注）暗号化の最終置換と復号の
初期置換なども打ち消される

ブロック暗号の適用法(1)

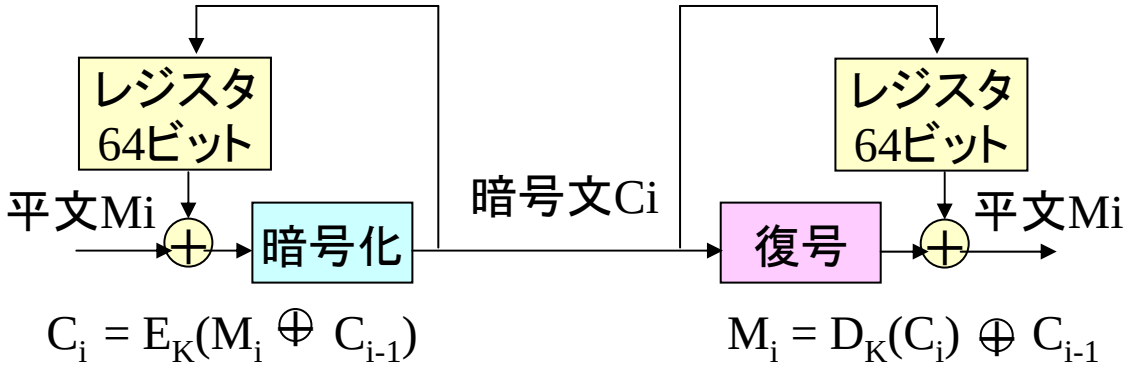
64ビットより大きな平文を暗号化するには、暗号の繰り返し適用が必要

1. **ECB (Electronic Code Book)**

平文64ビット毎に、暗号化を繰り返す

2. **CBC (Cipher Block Chaining)**

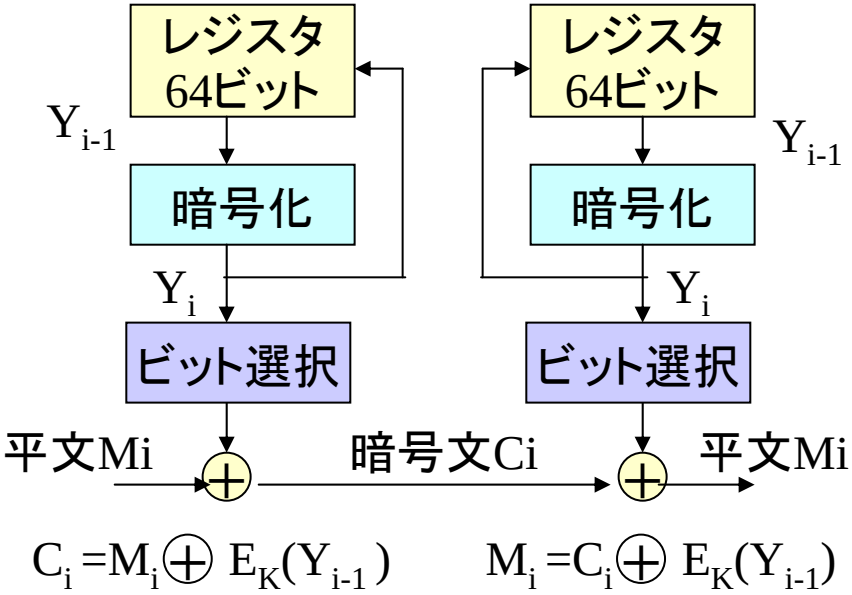
一つ前の暗号文と現時点の平文との排他的論理和をとった結果を暗号化



ブロック暗号の適用法(2)

３．OFB (Output Feedback)

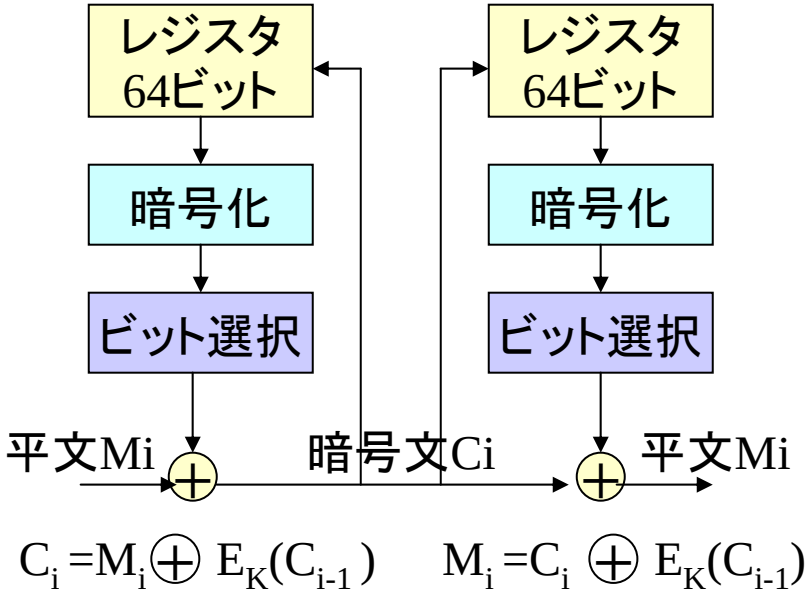
平文にランダムな系列を加える
（ストリーム暗号）



$C_i = M_i \oplus E_K(Y_{i-1})$　　$M_i = C_i \oplus E_K(Y_{i-1})$

４．CFB (Cipher Feedback)

直前の暗号文を暗号化し、その結果
と平文を加える（ストリーム暗号）



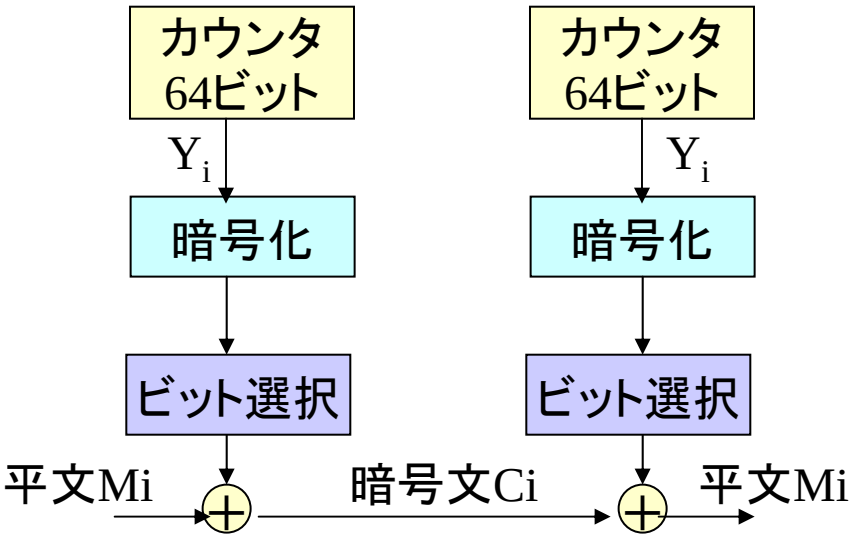
$C_i = M_i \oplus E_K(C_{i-1})$　　$M_i = C_i \oplus E_K(C_{i-1})$

無線通信（携帯電話等）で利用

ブロック暗号の適用法(3)

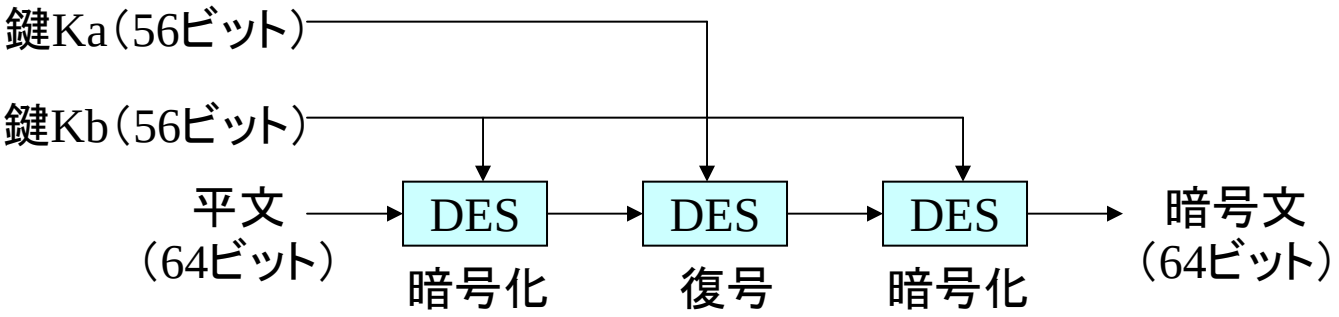
５．CTR (Counter)

カウンタ値を暗号化し、その結果と平文を加える（ストリーム暗号）

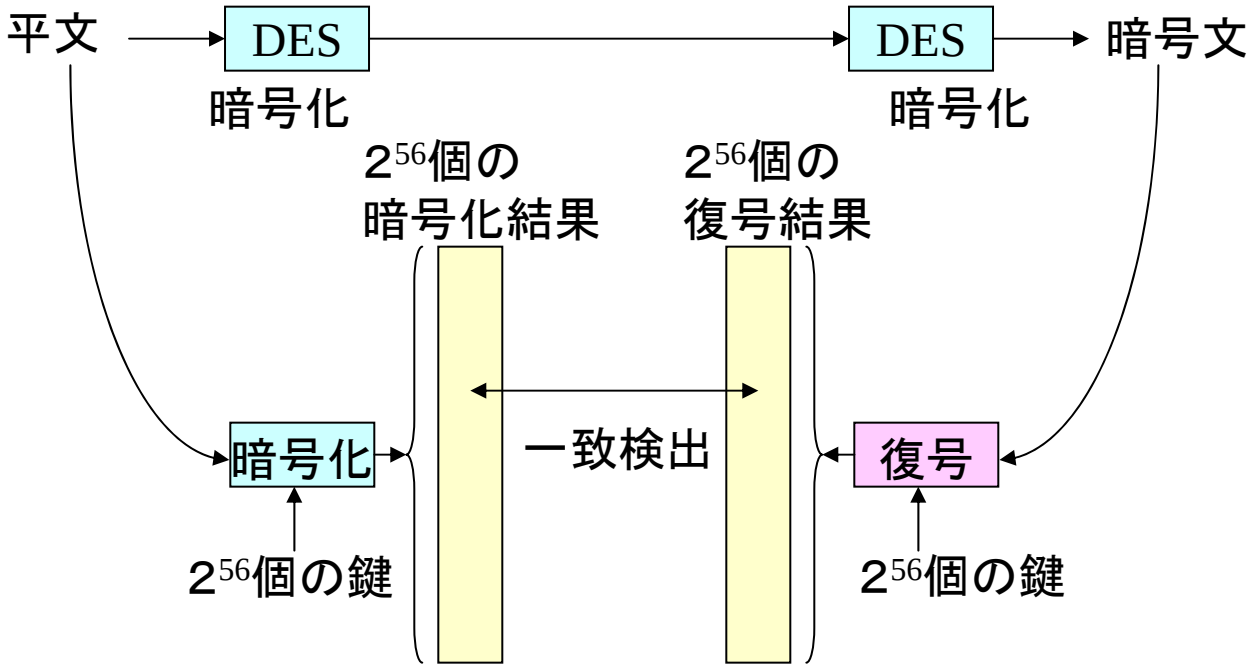


Triple DES

Triple DESの構成



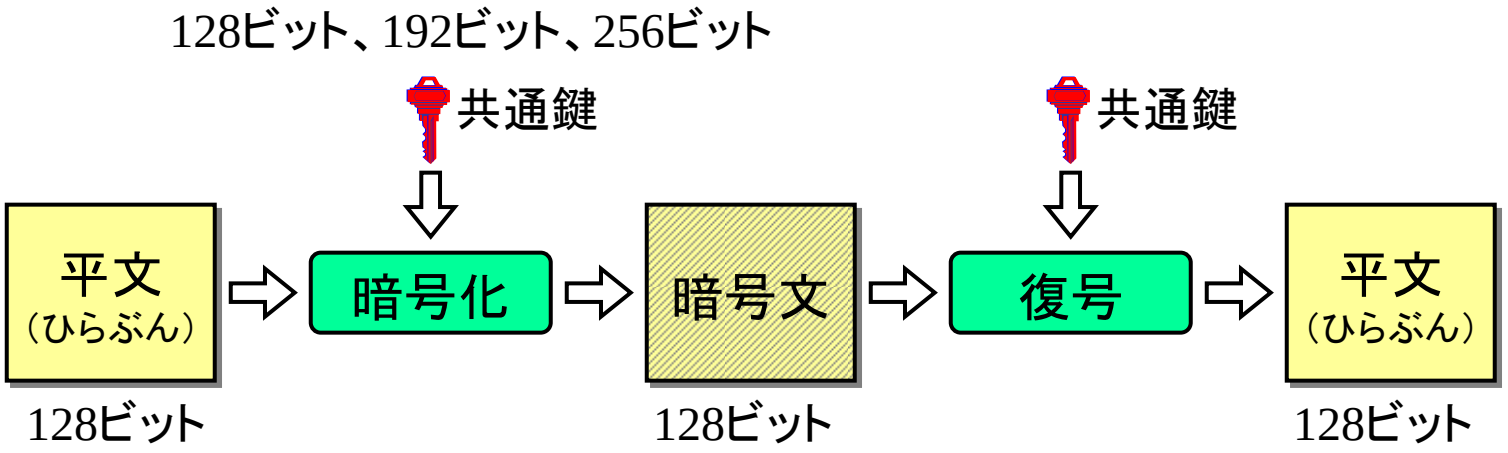
二重暗号化に対する中間一致攻撃



AES

AES (Advanced Encryption Standard)

・DESの後継となる米国連邦政府の標準共通鍵暗号
・公募、審査を経て、ベルギーで開発されたRijndael (ラインダール）を選定し、2001年に標準暗号として制定
・安全性、処理効率に優れる



付. 共通鍵暗号の例

名称	鍵長(bit)	ブロック長(bit)	段数	開発元	発表年
DES	56	64	16	IBM	1977
Triple DES	112,168	64	16×3	IBM	1977
FEAL-N	64	64	N	NTT	1987
MULTI2	256	64	可変	日立製作所	1989
IDEA	128	64	8	ETH, Ascom	1991
MISTY1,2	128	64	8	三菱電機	1992
Blowfish	32-448	64	16	Counterpane	1993
RC2	1-128	64	18	RSA	1997
RC5	1-256	32,64,128	可変	RSA	1994
CAST	40-128	64	可変	Nortel	1997
Camellia	128,196,256	128	18,24	NTT,三菱	2000
AES(Rijndael)	128,196,256	128	10,12,14	NIST	2001