共通鍵暗号

ネットワークと情報セキュリティ4

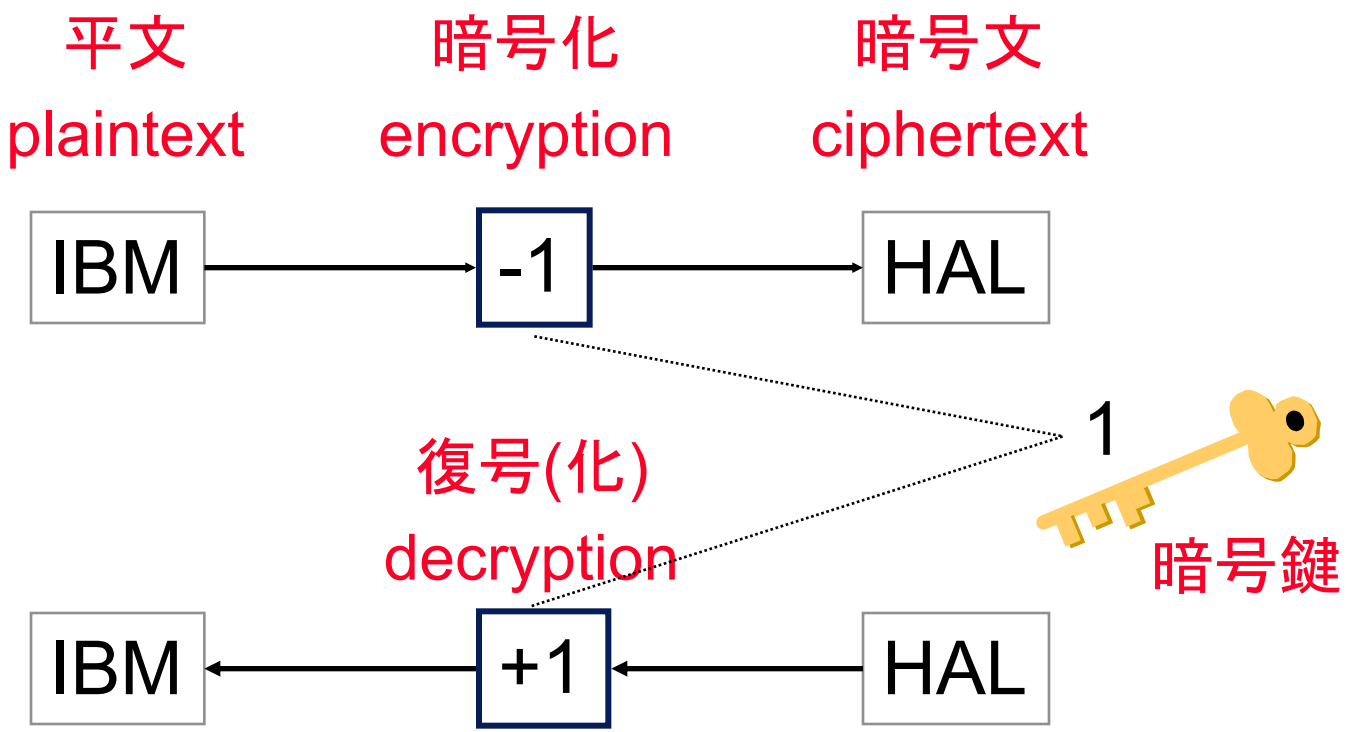
菊池　浩明

Contents

- 4.1 暗号技術の概要
- 4.2 共通鍵暗号
  - ブロック暗号
  - 運用モード
  - 暗号解読
  - （4.3　セキュアハッシュ関数は「電子署名」の回で行う）

暗号技術の概要

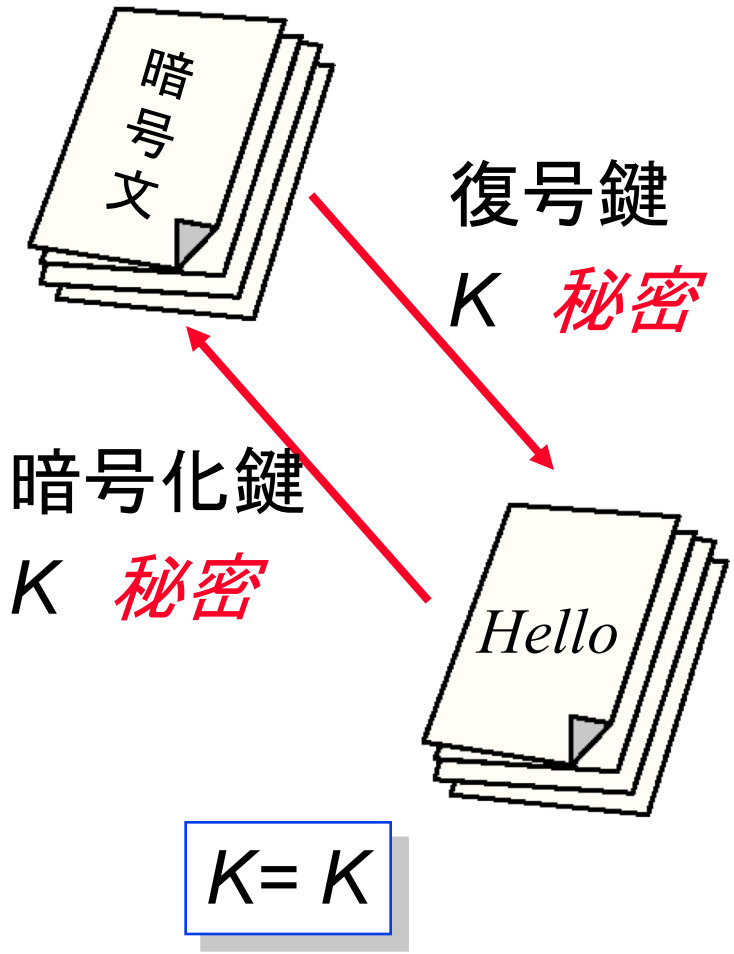
暗号の基礎



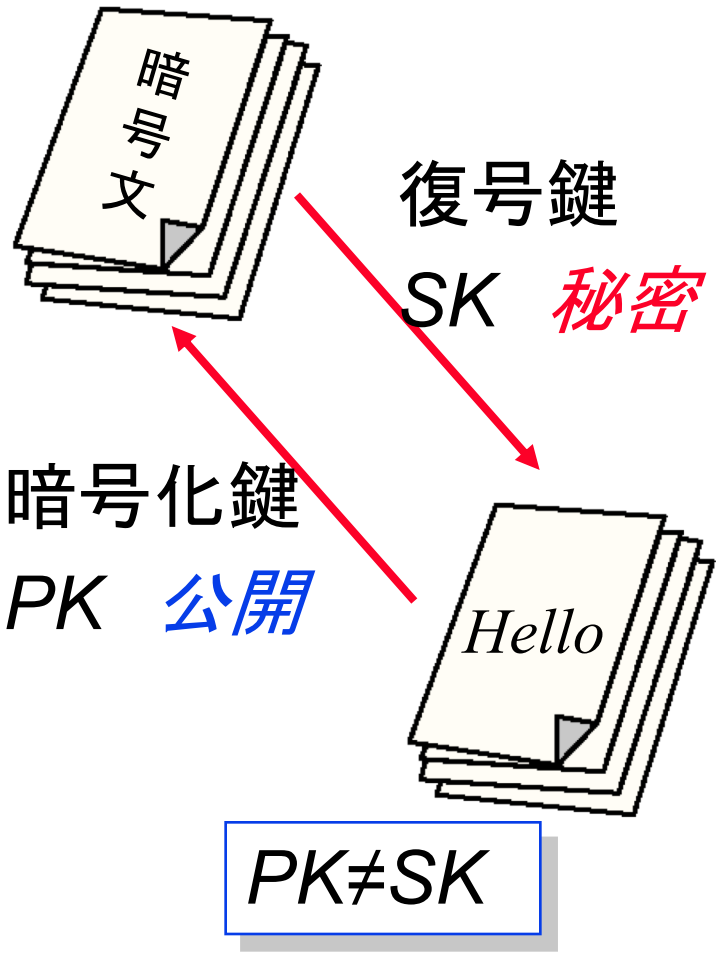
- シーザ暗号(Caesar)

共通鍵暗号と公開鍵暗号

- 共通鍵暗号



- 公開鍵暗号



電子政府推奨暗号

電子政府における調達のために参照すべき暗号のリスト
（CRYPTREC暗号リスト）

平成２５年３月１日
総　　務　　省
経　済　産　業　省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	3-key Triple DES(注3)
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省政策統括官（情報通信担当）及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。

[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

シーザ暗号 (Caesar Cipher)

- In Rome.
  - Simple substitution cipher

a	b	c	d	e	f	g	h	I	k	l	m	n	o	p	q	r	s	t	v	x
D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	A	B	C

- ROT13

a	b	c	d	e	f	g	h	I	j	k	l	m
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

n	o	p	q	r	s	t	u	v	w	x	y	z
A	B	C	D	E	F	G	H	I	J	K	L	M

ビジネル暗号 (Vigenere Cipher)

- 16 century, Blasie de Vigenere

```
  thi sis adu mmy mes sag e
+ ABC ABC ABC ABC ABC ABC A
= TIK SJU AEW MNA MFU SBI E
```

バーナム暗号 (Vernam Cipher)

- 1926, Gilbert Vernam (AT&T)
  - “*One-time Pad*”
  - 平文 M，鍵 K
  - 暗号文 C = $E_K(X) = X \oplus K$ (bitwise XOR)
  - 復号　M = D(C) = C⊕K
  - 例）
    - M = 1010, K = 1100, C =
    - M = C⊕K = 0110⊕1100 = 1010 = M⊕K⊕K = M
  - 欠点：　M文と同じ長さのKが必要

バーナム暗号とEXOR

- 排他的論理和 Exclusive OR (EXOR)

M	K	暗号 M⊕ K	復号 M ⊕ K ⊕ K
A	B	A⊕B	A
0	0		
0	1		
1	0		
1	1		

バーナム暗号の安全性

- Theorem 1.5 (完全秘匿性)
  - The Vernam cipher provides perfect secrecy for any distribution of the plaintext
- Proof
  - For any x and y,

$$\begin{aligned}\Pr[X = x, Y = y] &= \Pr[X = x, K = x \oplus y] \\ &= \Pr[X = x] \times \Pr[K = x \oplus y] \\ &= \Pr[X = x] \times 2^{-n}.\end{aligned}$$

  - By $\Pr[Y = y] = 2^{-n}$, we deduce $\Pr[X = x \mid Y = y] = \Pr[X = x]$ for any x and y (Perfect secrecy)

演習

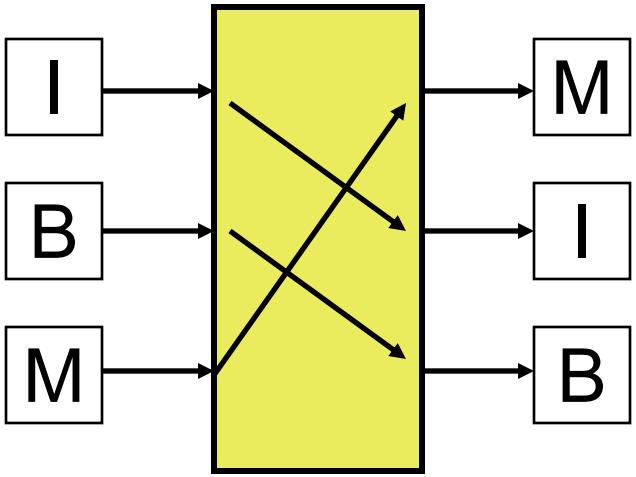
- 8ビットのバーナム暗号を行う.
  - K = $6E_{(16)}$で, M = $99_{(16)}$ を暗号化せよ.
  - C = $D8_{(16)}$ を復号せよ.

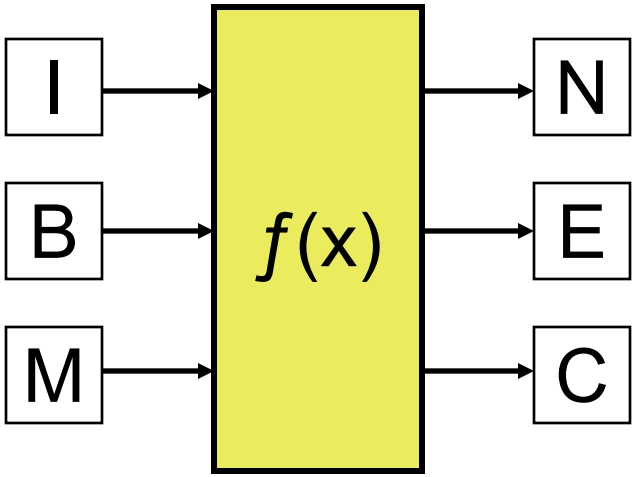
ブロック暗号

DES, AES

換字と転置

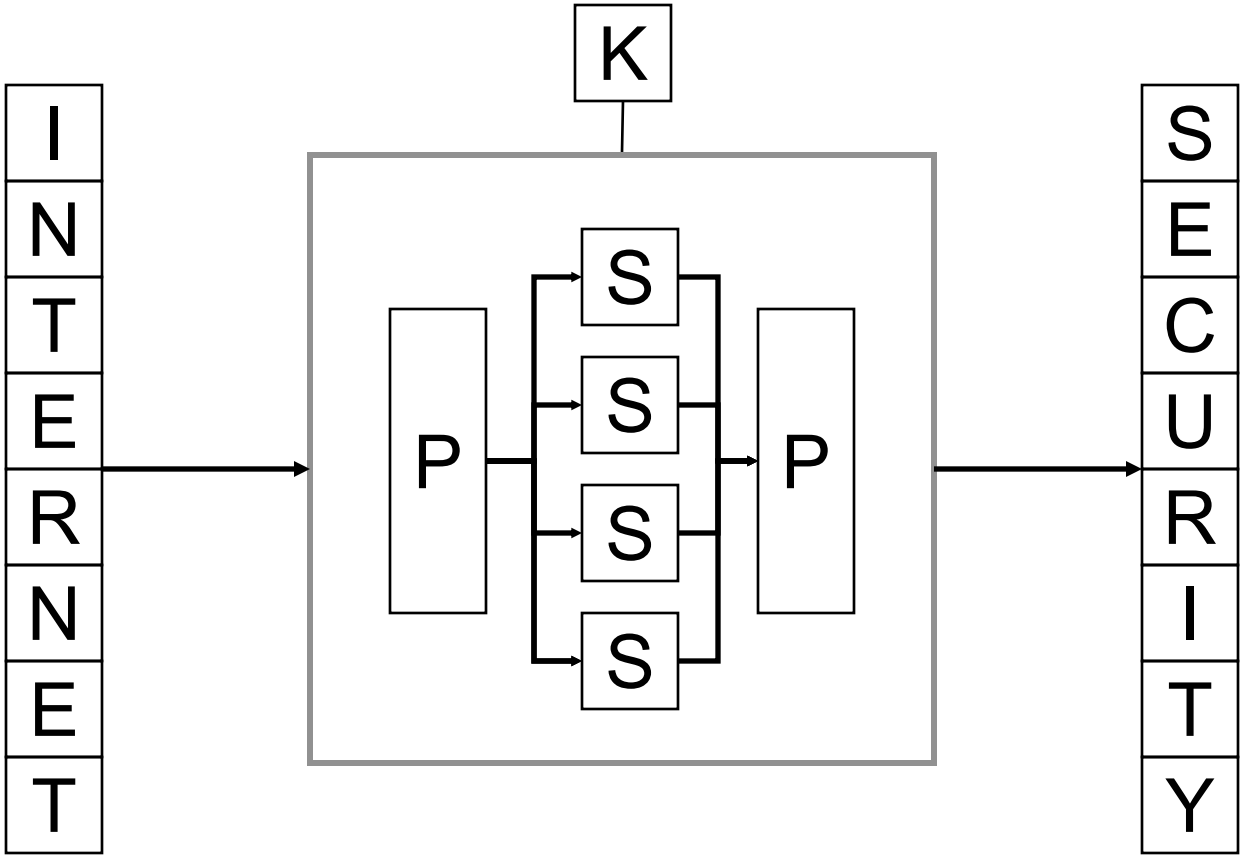
- 転置 Permutation
- 換字 Substitution





ブロック暗号

- S-BoxとP-Boxの組み合わせ



ブロック暗号アルゴリズム

- DES (Data Encryption Standard)
  - 1977 米商務省標準局 (National Bureau of Standards (現NIST)により標準化, FIPS PUB 46
  - 56-bit key, 64-bit block
  - 1960 IBM Luciferを元にNSAが改良
  - 銀行，商用
  - 1994 NISTが5年期間を延長．→AES
  - トリプルDES.

    $C = E_1(D_2(E_1(P)))$
- IDEA
  - 1991, X. Lai and J. Massey(ETH)
  - 128-bit key, 64-bit block cipher
  - PGP
- SAFER K-64
  - SP-NET
  - 64-bit blocks cipher with 64-bit keys

AES (Advanced Encryption Standard)

- AES
  - 1999 NISTによる標準化 (FIPS PUB 46-3)
  - アルゴリズム公募，安全性とコストによる評価
  - 候補 21→15→5
- Rijndael
  - 提案者Joan Daemen and Vincent Rijmen（ベルギー）
  - 128, 192, 256-bit block and key length

http://www.wits88.com/mgmt.htm
http://en.wikipedia.org/wiki/Vincent_Rijmen

S-DES（Simplified DES）

	DES	S-DES	AES
	1977 NBS	1996 E. Schaefer W. Stallings, “Cryptography and Network Security”, Prentice Hall, pp.56-63	2000 NIST
鍵長	56 bit	10 bit	128 bit (192, 256)
メッセージ長	64 bit	8 bit	128 bit
ラウンド数	16	2	10 (12, 14)
S-Box	6bit→4bit 8個	4bit→2bit 2個	16 x 16 (8→8bit)1個

S-DES 1. Permutation 転置

- plaintext M
- IP初期転置
  - Initial permutation

IP

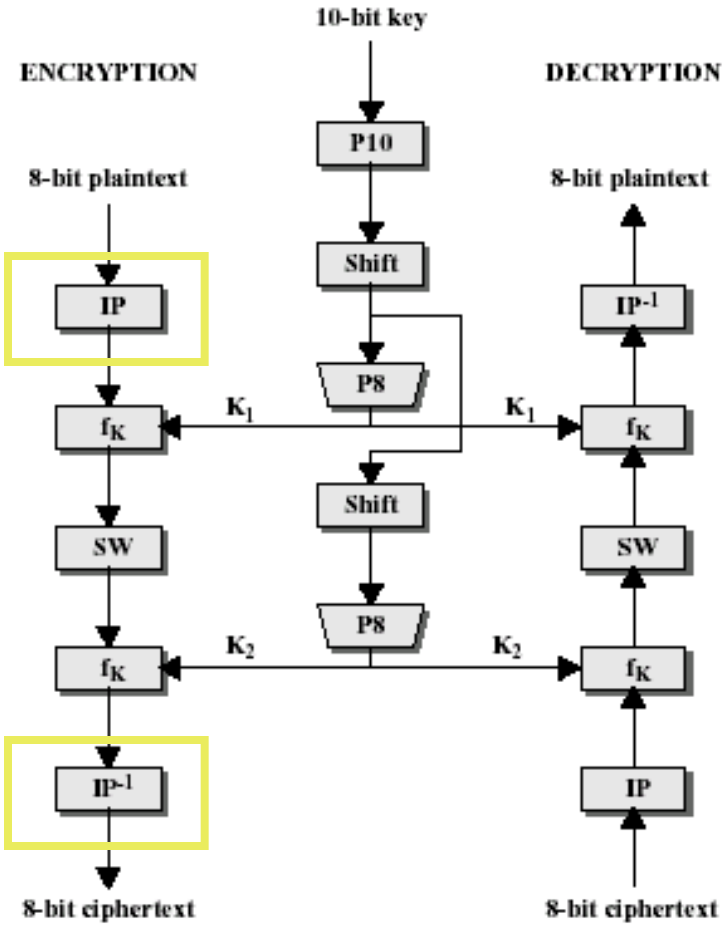
4	1	3	5	7	2	8	6

M=1 1 1 1 0 0 1 1

IP(M)=1 0 1 1 1 1 0 1

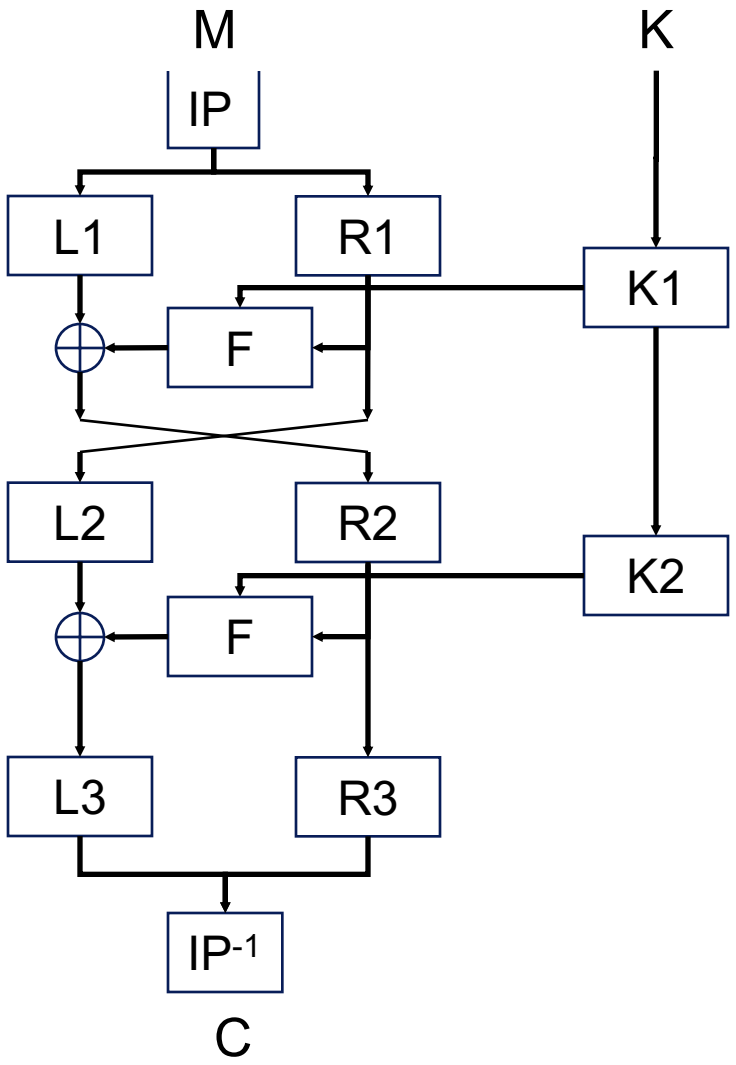
IP^{-1}

2	6	3	1	4	8	5	7



S-DES 2. Round

- Round 1
  - L1=IP(M)の左4bit
  - R1=同右4bit
  - F_K: Kによる関数
- Round 2
  - L2=R1
  - R2=L1⊕F(R1,K1)
- Round 3
  - R3 = R2
  - L3= L2⊕F(R2,K2)
  - 暗号文 C=IP^{-1}(L3, R3)



S-DES 3. Key generation

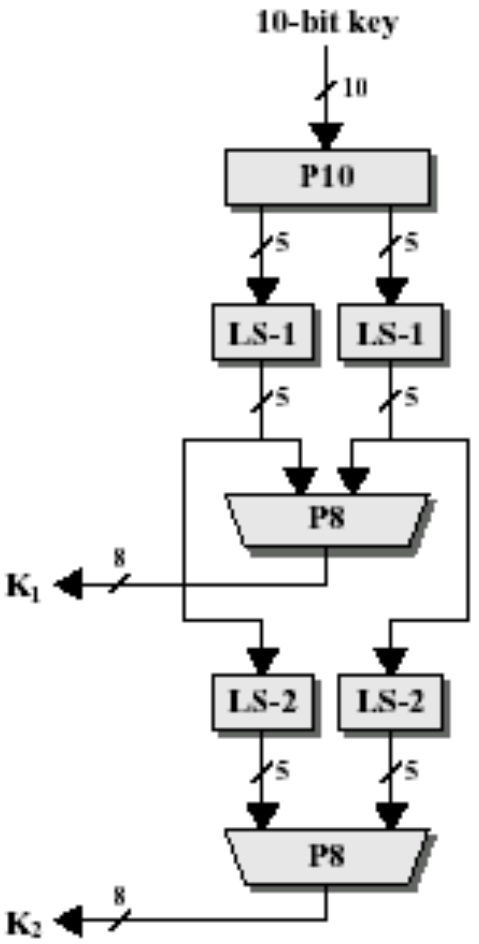
- P10

3	5	2	7	4	10	1	9	8	6

- LS-1(5 bit毎に左1bit)

- P8 (10→8)

6	3	7	4	8	5	10	9



010
100
000
100

S-DES 4. Function F

- F(R,K)
  - E/P:

4	1	2	3	2	3	4	1

  - N=E/P(R) ⊕ K
    = (N1,N2)
  - 例）

R=0100

E/P=0010 1000

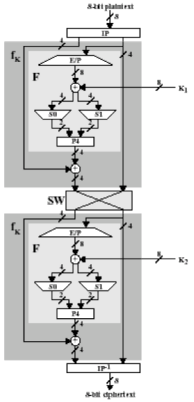
⊕ K = 0100 0001

N=(N1,N2) =0110 1001

  - Y1=S1(N1)
  - Y2=S2(N2)
  - P4:

2	4	3	1

  - F(R,K)=P4(Y1,Y2)



S-BOX

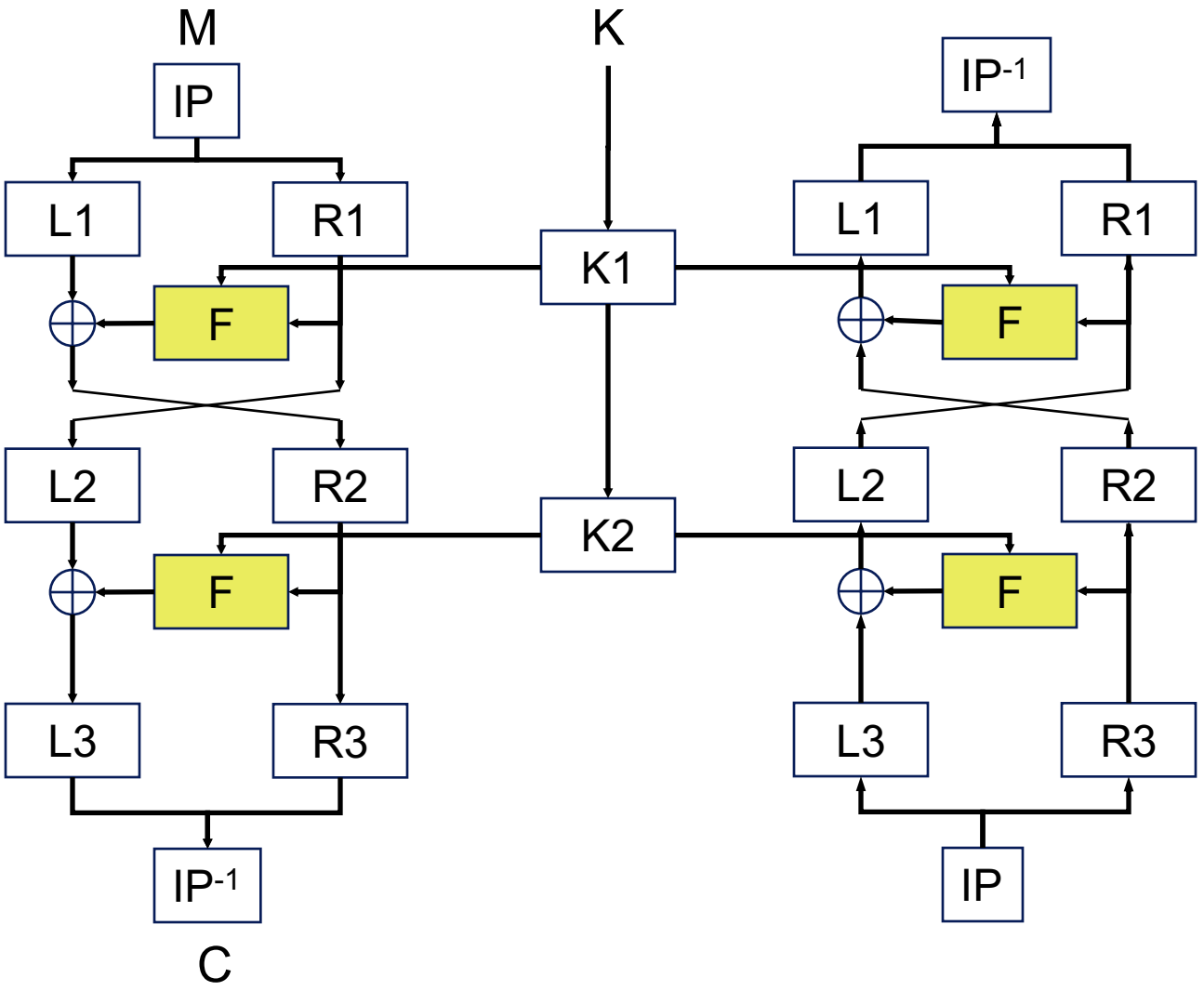
- S1
  - N1=0110の時
  - 列 14= 00, 行23 = 11
  - Y1=11

23 \ 14	00	01	10	11
00	01	00	11	10
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

- S2

23 \ 14	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	00	11

S-DES 全体図



S-DES 復号

- 復号

  (L3,R3)=IP(C)

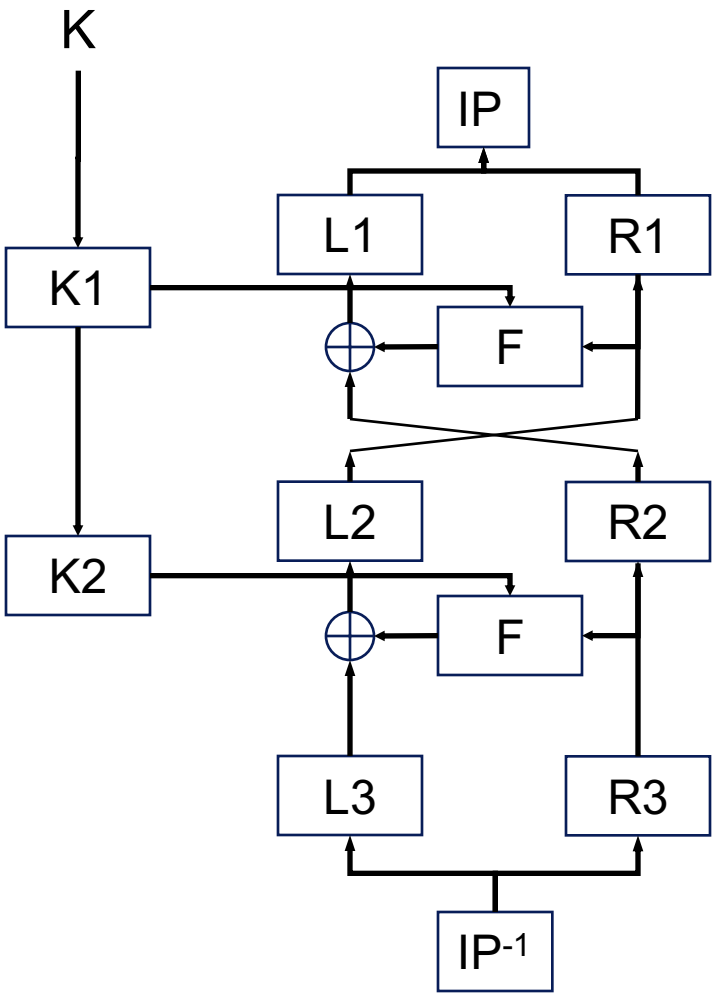
  R2=L3

  L2=L3⊕F(R3,K2)

  R1=L2

  L1=R2⊕F(L2,K1)

  M=IP^{-1}(L1,R1)



演習

- 次の転置表Pについて求めよ.
  - 1. x = 3Dの転置 P(x)
  - 2. x = C5の転置 P(x)
  - 3. Pの逆関数 P^{-1}
  - 4. $P^{-1}(3E)$

7	1	6	8	4	5	3	2

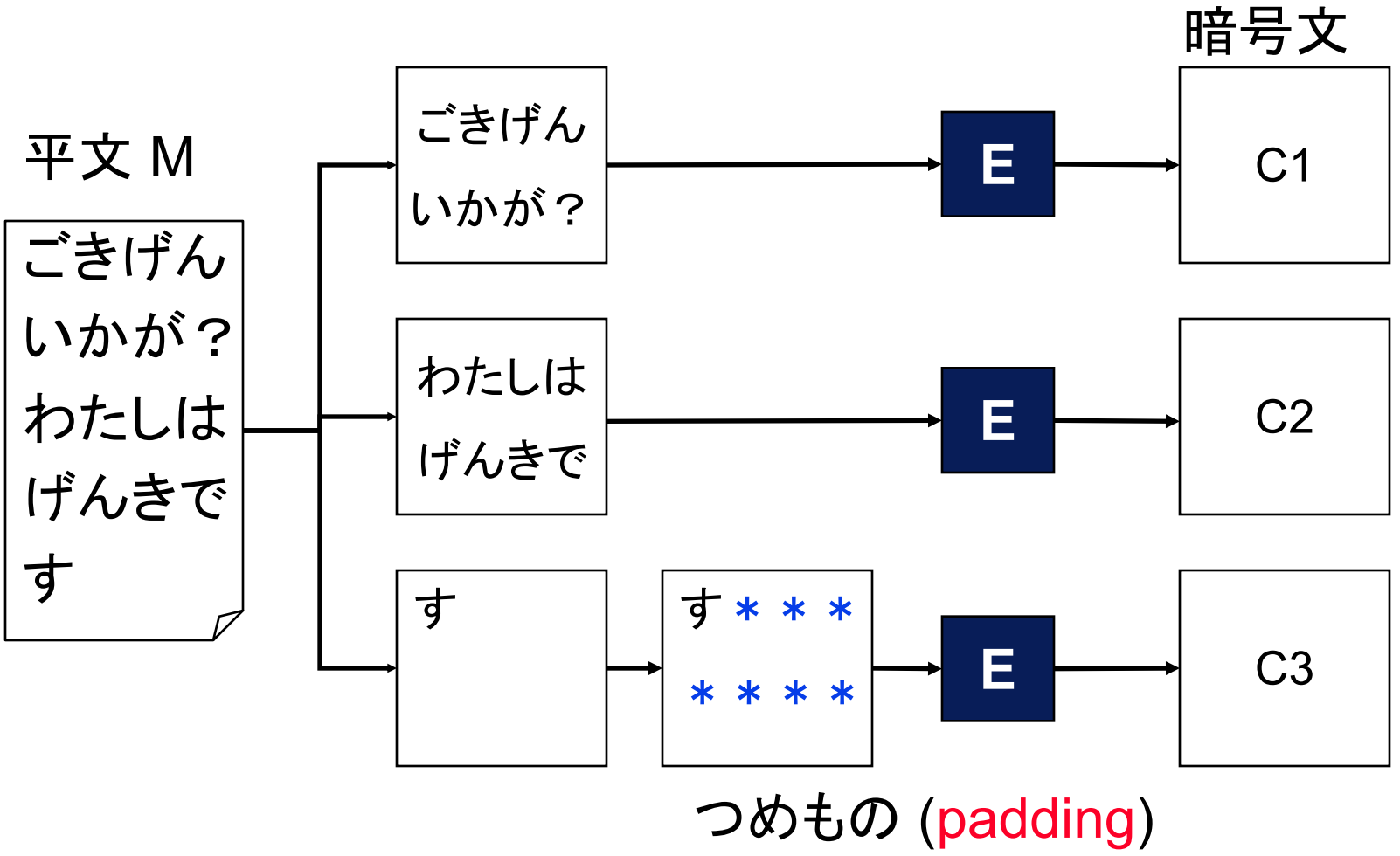
運用モード

ECB, CBC, CFB

運用モード

- ECB(Electronic Code Book)
  - ブロック単位に独立に暗号化
- CBC(Cipher Block Chaining)
  - S/MIME, SSL/TLS, IPsec
- CFB(Cipher FeedBack)
  - ストリーム暗号として利用,（OFB, CTRも同様）
- OFB(Output FeedBack)
- CTR (CounTeR mode)

1. ECB

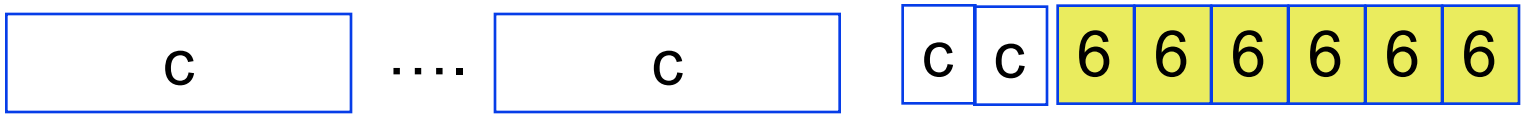

暗号文
平文 M
ごきげんいかが？わたしはげんきです
ごきげんいかが？
わたしはげんきで
す
す＊＊＊＊＊＊＊
E
E
E
C1
C2
C3
つめもの (padding)

Padding

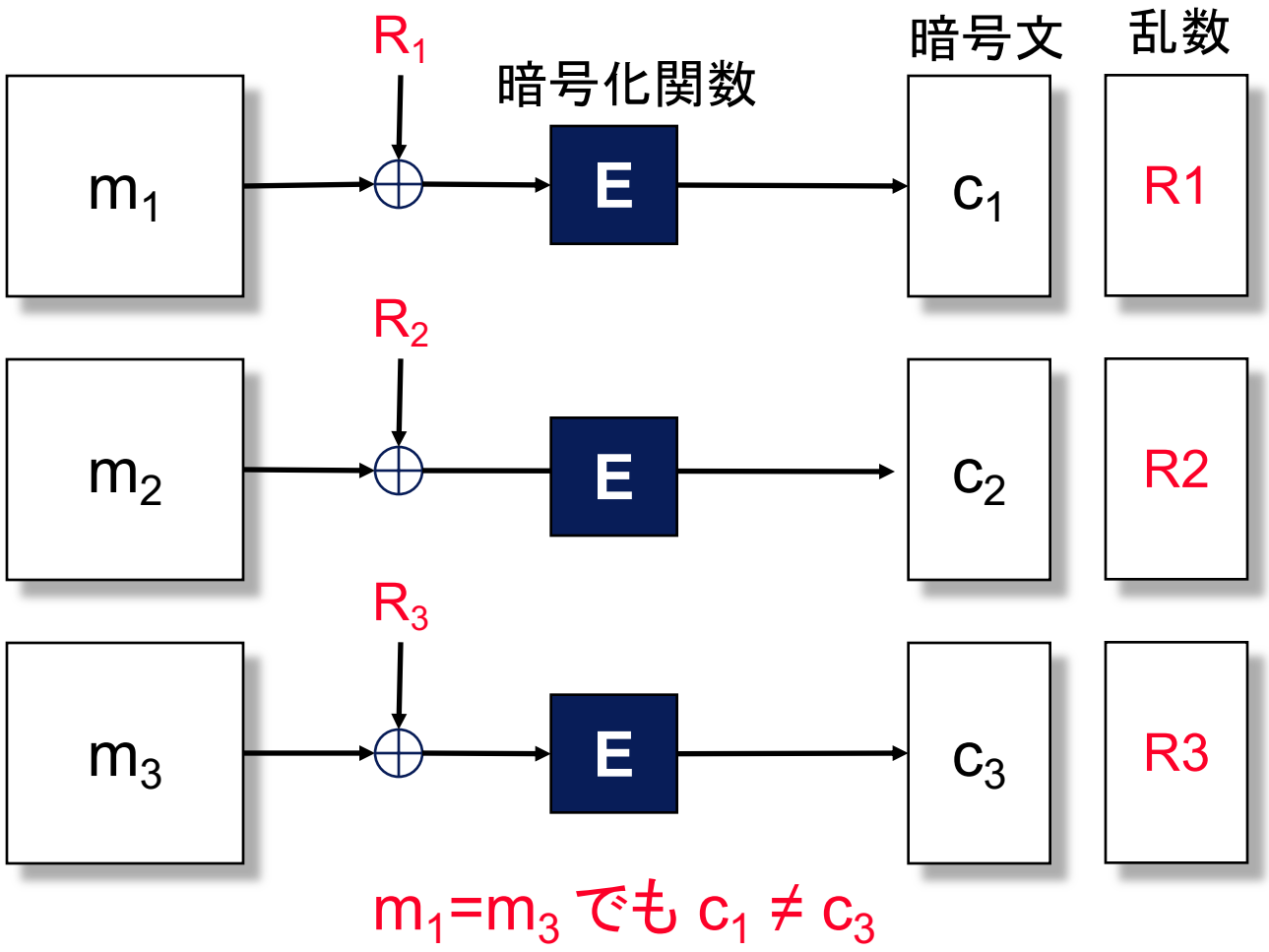
- PKCS 5
  - メッセージ長 n
  - ブロック長 b (byte)
  - パディングデータ e = b – (n mod b)をe個
- 例(DES)

  n = 50 byte

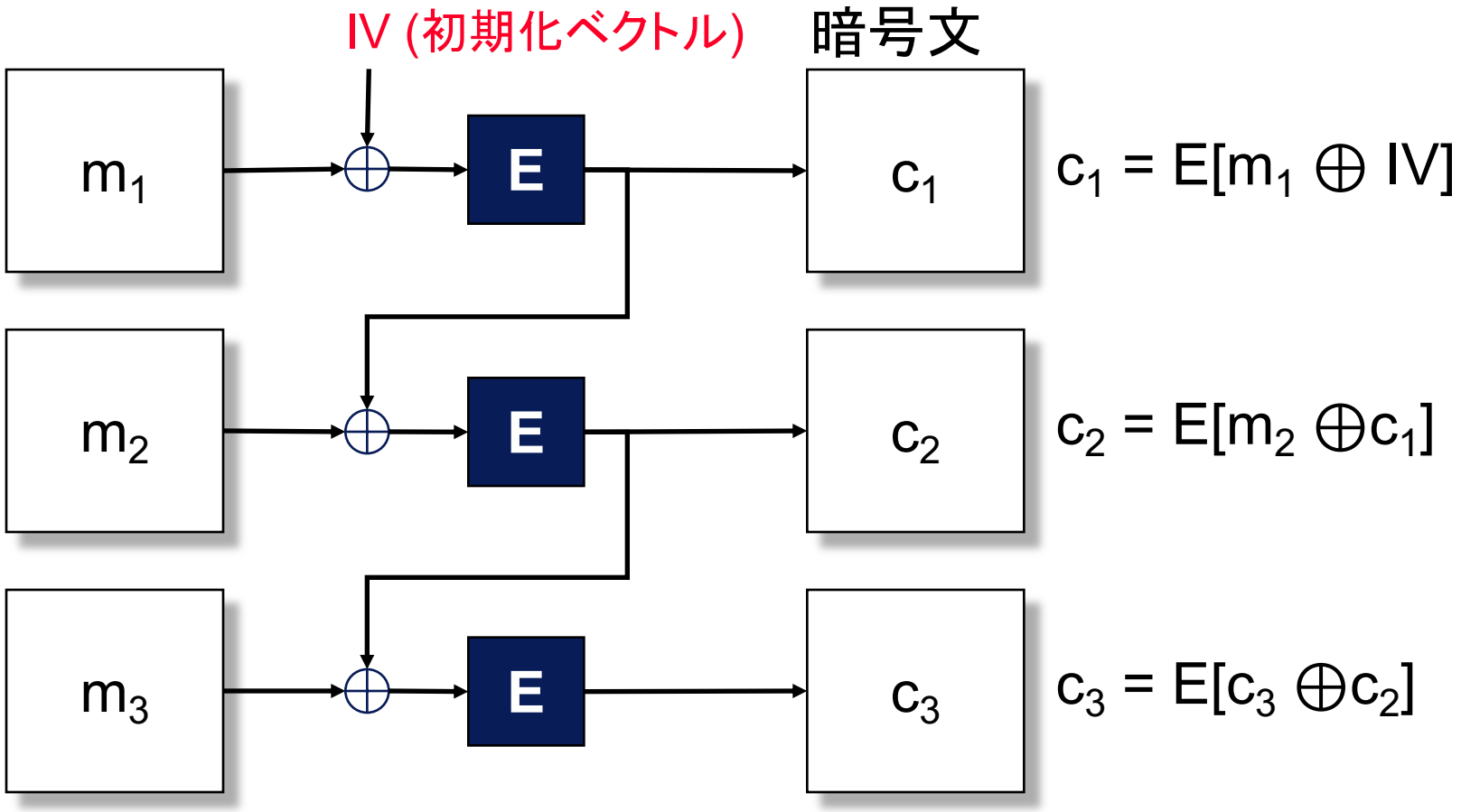
  e = 8 – (50 mod 8) = 6



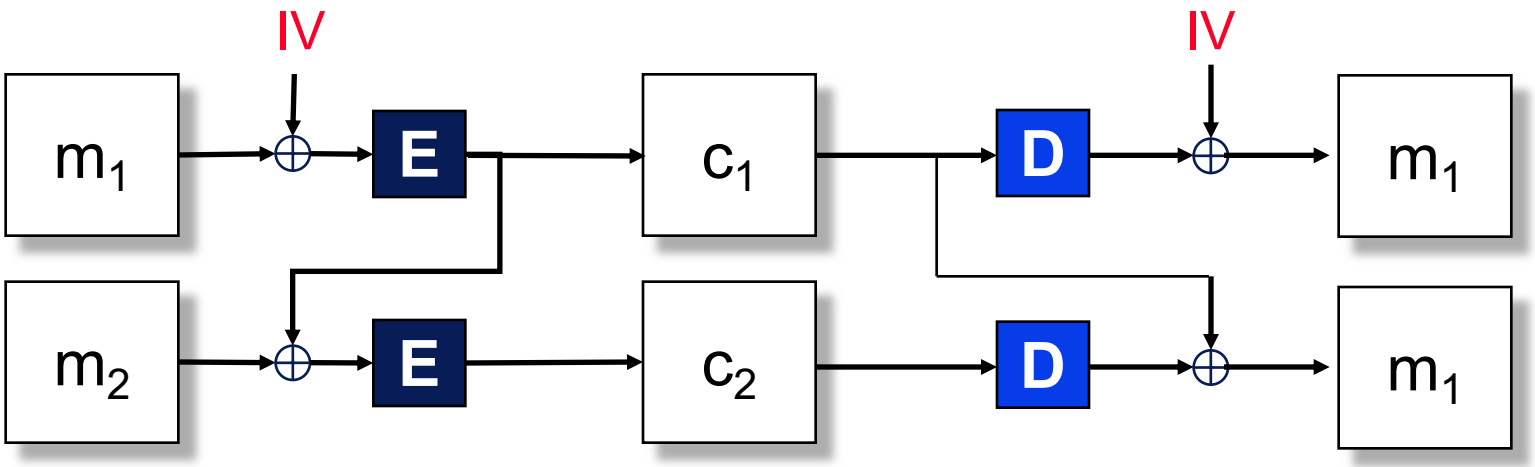
ECB with 乱数



2. CBC


IV (初期化ベクトル)
暗号文
m_1
E
c_1
$c_1 = E[m_1 \oplus IV]$
m_2
E
c_2
$c_2 = E[m_2 \oplus c_1]$
m_3
E
c_3
$c_3 = E[c_3 \oplus c_2]$

CBCの複号



暗号化

$c_1 = E[m_1 \oplus IV]$

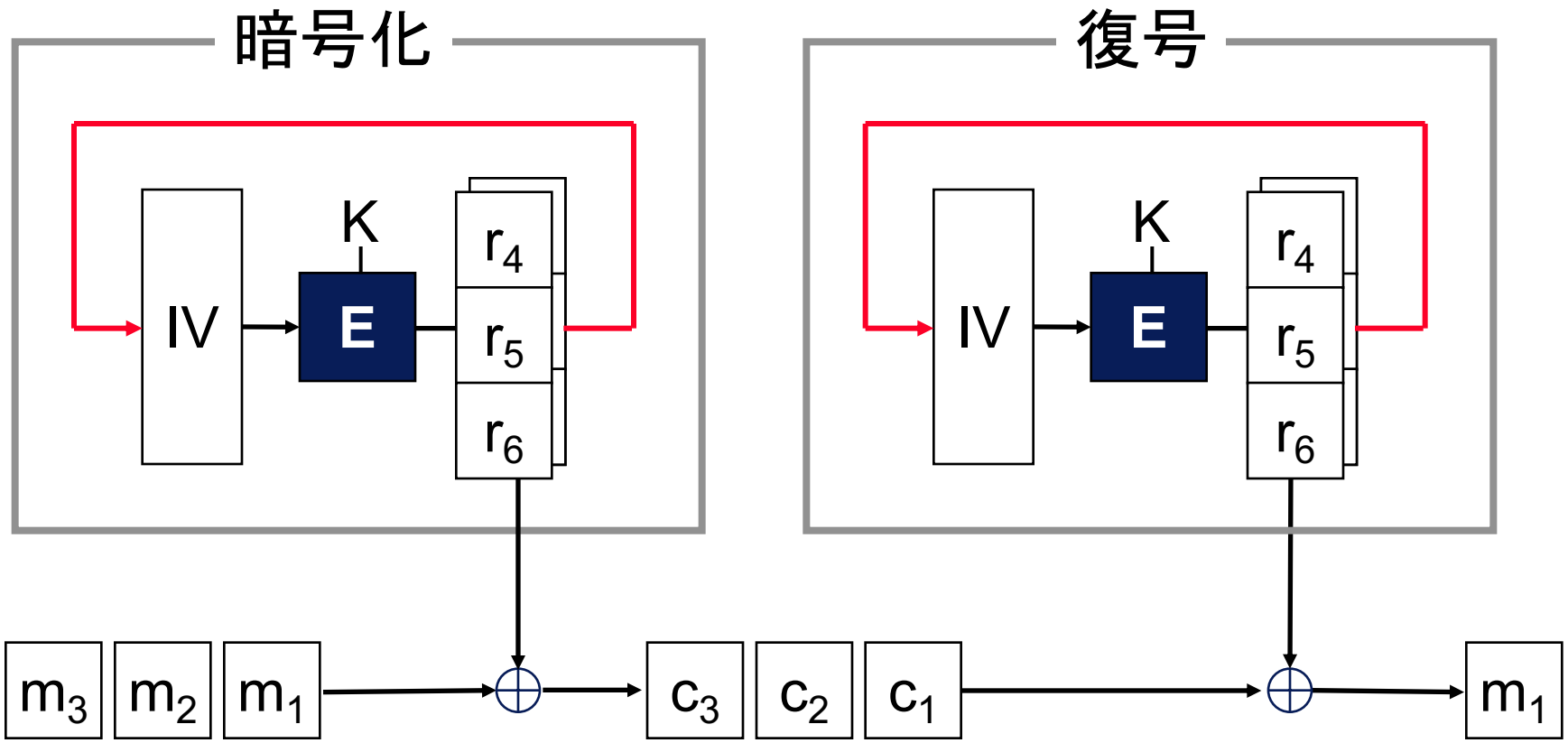
$c_2 = E[m_2 \oplus c_1]$

複号

$m_1 = D[c_1] \oplus IV$

$m_2 = D[c_2] \oplus c_1$

3. OFB



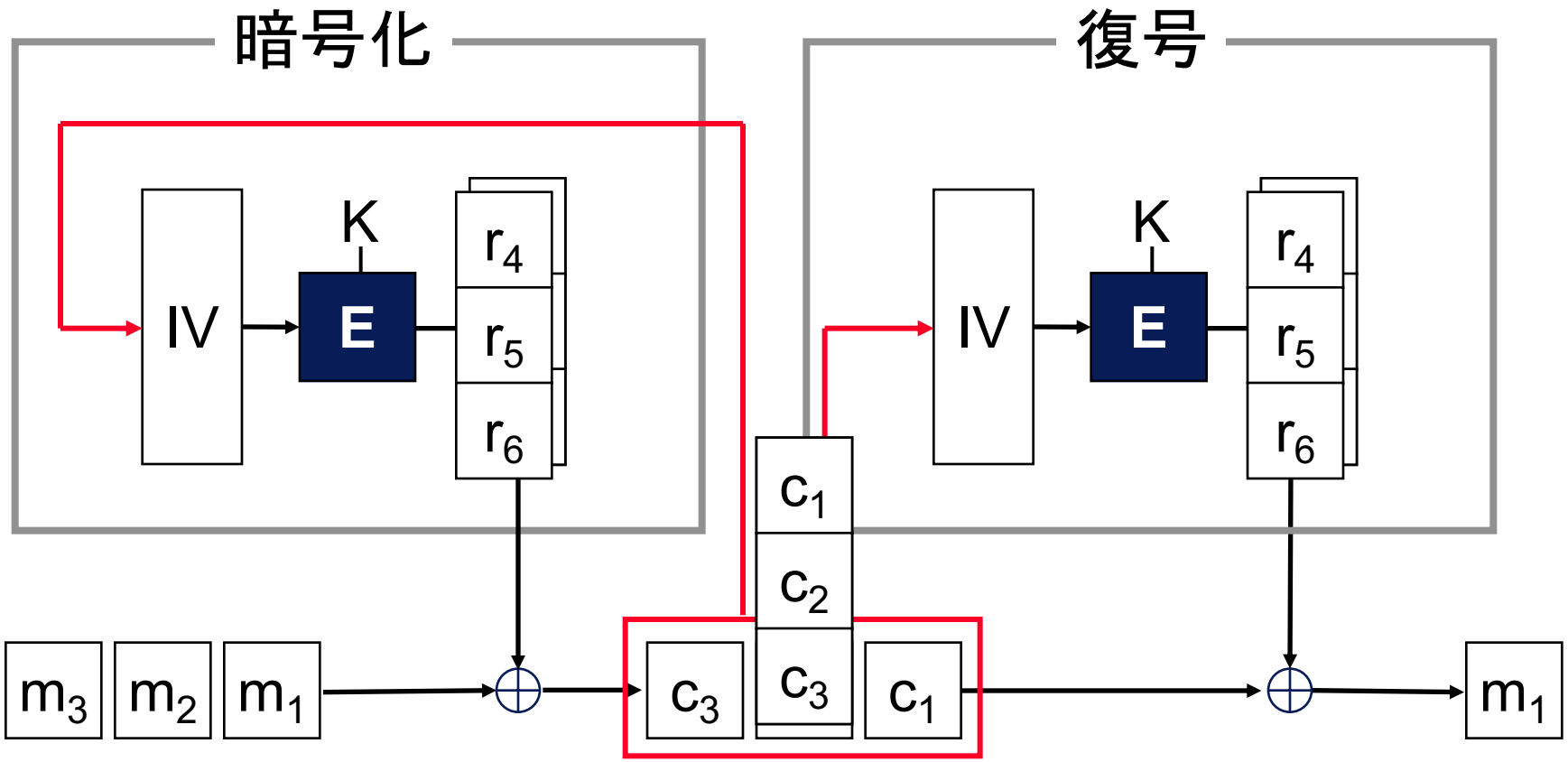
$c_1 = m_1 \oplus E(IV;r_1;r_2;r_3)$

$c_4 = m_4 \oplus E(r_1;r_2;r_3)$

$m_1 = c_1 \oplus E(IV;r_1;r_2;r_3)$

- 注意: 復号に暗号化関数Eを使う

4. CFB



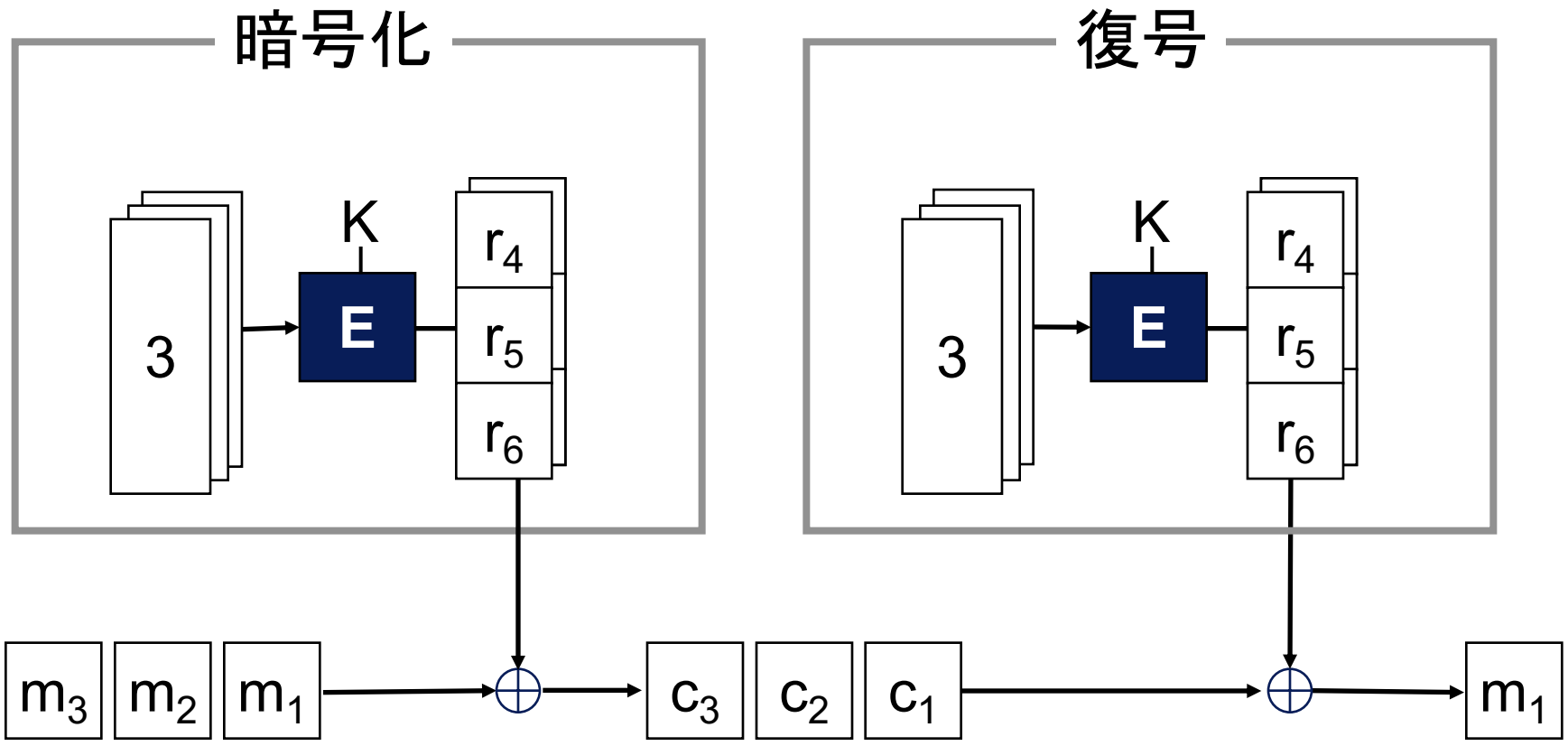
$c_1 = m_1 \oplus E(IV)$

$c_4 = m_4 \oplus E(c_1;c_2;c_3)$

$m_1 = c_1 \oplus E(IV)$

- 注意: 暗号文をEの入力とする

5. CTR



$c_1 = m_1 \oplus E(r_4)$

$c_4 = m_4 \oplus E(r_4)$

$m_1 = c_1 \oplus E(r_4)$

- 乱数r_1, r_2の事前計算可能

演習

- 1) 次の表で与えられる3ビットの暗号化関数Eを用いて，IV=1, CBCモードで暗号化したら，(C_1,C_2,C_3,C_4) = (0, 6, 5, 6)になった．平文M_1,M_2,M_3,M_4を求めよ．
- 2) 平文 M1,M2,M3,M4 = (1,1,2,3) をEをCFBモードで用いて暗号化せよ．
  ただし，IV=3，ブロック長3ビットとする．

M	0	1	2	3	4	5	6	7
E(M)	5	6	3	4	1	0	2	7

暗号解析

暗号の安全性

解読方法

暗号文のみ

既知平文攻撃
暗号文とその平文
から解析

選択平文攻撃
任意の平文と
その暗号文から解析

選択暗号文攻撃
任意の暗号文と
その平文から解析

解読者
に有利

解析技術

- 総当たり攻撃(Brute Force)
  - 鍵空間の大きさに比例　　複雑さ 2^{56}
- 差分攻撃
  - 1989 E. Biham and A. Shamir
  - 選択平文攻撃　　複雑さ 2^{47}
- 線形攻撃
  - 1993 Matsui
  - 線形近似式による最ゆう法
  - 既知平文攻撃　　複雑さ 2^{47}

DES Challenge

- 暗号破りコンテスト
  - DES 56bit
  - $10,000 (120万円)

1. 1997 96日間
   distributed.net
2. 1998 56時間
   EFF(Electronic Frontier Foundation)
3. 1999 22時間
   distributed.net & EFF

“Deep Cracker”

- 専用ハードウェア
  - EFF
  - 27枚専用ボード
  - 64個カスタムチップ
  - 探索スピード90,000,000,000 key/sec
  - お値段
    $250,000

http://www.eff.org/descracker.html

まとめ

- 暗号技術には公開鍵暗号と(　　)鍵暗号がある．完全秘匿性が保証されているのは(　　)暗号である．
- ブロック暗号の要素は，換字Substitutionと置換(　　)である．全単射である必要がある．
- 平文がブロック長の倍数でないので行う処理を(　　)という．暗号を鎖の様に適用していく運用モードを(　　)という．
- 総当たりで鍵を探す攻撃を(　　)攻撃という．