平成17年9月30日

リスク工学特別演習

共通鍵ブロック暗号の変遷

4班

植竹　聡　　岡山 麻裕子　　田中　永

指導教員　　片岸一起　　繆　瑩

本日のアジェンダ

Ⅰ　本発表の位置付けなど（植竹）

Ⅱ　DESの解読された経緯について（岡山）
(Data Encryption Standard)

Ⅲ　AESの特徴について（田中）
(Advanced Encryption Standard)

本演習の目標

グループ課題

秘密鍵暗号と公開鍵暗号の考え方について概観せよ。

特にDES暗号とRSA暗号について素人に分かるように説明せよ。

同一テーマで、DES、RSA、楕円曲線暗号について発表済(H14年度)

本テーマにおけるグループ目標

共通鍵暗号について概説し、専門家でない人に理解してもらう

分野の特性上、改良などは短期間では難しい・・・

調査的な内容であるが、ポイントを初心者にわかりやすく説明する。

今回の位置付け

前回の発表

共通鍵暗号の初歩から最新の標準暗号までを広く概説

今回の発表

中間発表で指摘されたポイントに絞った詳細な説明

最終レポート

本発表と中間発表をフォローアップし、総合的にまとめた報告とする

今回のポイント

導入･基礎→ポスターなど

- DESの解読された経緯について
- AESの特徴について

具体例を用い、初心者にも
分かるように詳細に説明

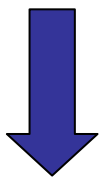
Ⅱ章
DESの解読方法と現在の動向

目次

- DESとは
- DESが破られた経緯
  - 線形解読法
  - 鍵の全数探索
- 現在のDESの動向

DESとは

- DES（Data Encryption Standard）
  - **１９７７年アメリカ合衆国商務省標準局が連邦政府関係の非機密だが取り扱い注意データ用標準暗号として制定**
  - **約２０年間標準暗号として使われていたが、近年その安全性が問題視**



DESが破られた経緯と動向について調べる

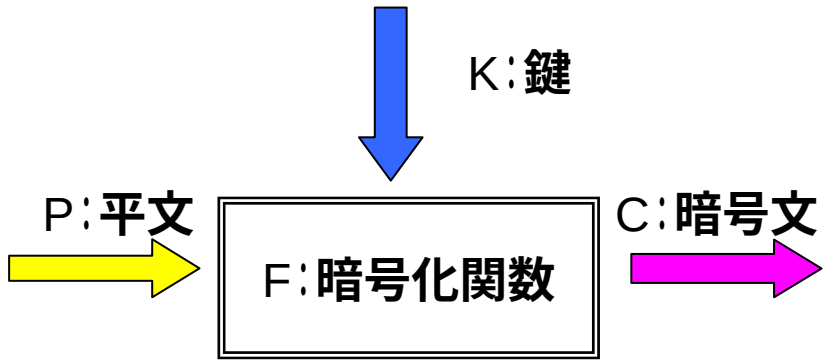
DESが破られた経緯

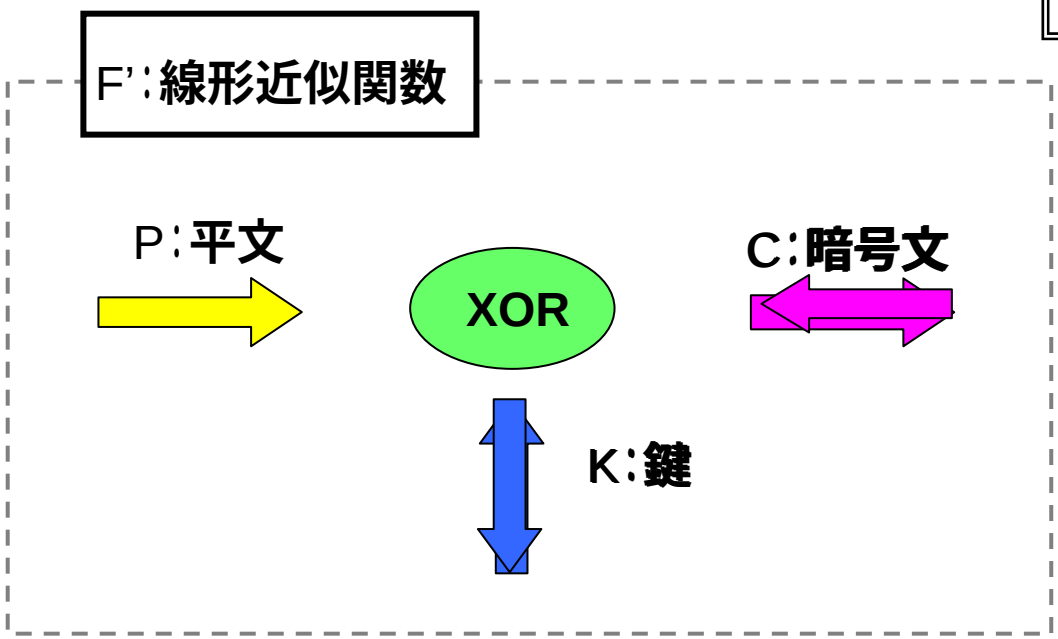
- １９９０年代から解読手法が盛んに研究される
- 差分解読法
  - １９８９年BihamとShamirが発表
  - 選択平文アタック
  - 事前に対策がとられていたためDES自体は破られていない
- 線形解読法
  - １９９３年に松井充が考案
  - 既知平文アタック
  - DES初の解読例
    （１９９４年　１２台のWS、2^{43}ブロックの平文-暗号文対で５０日）
- 鍵の全数探索
  - 最も単純で効率の悪い方法
  - １９９７～９９年、RSA　Security社がDES解読コンテストを開催

線形解読法

•平文と対応する暗号文から鍵を求める。

•暗号化関数を部分的に近似したものを
解読することにより、計算量を減らす



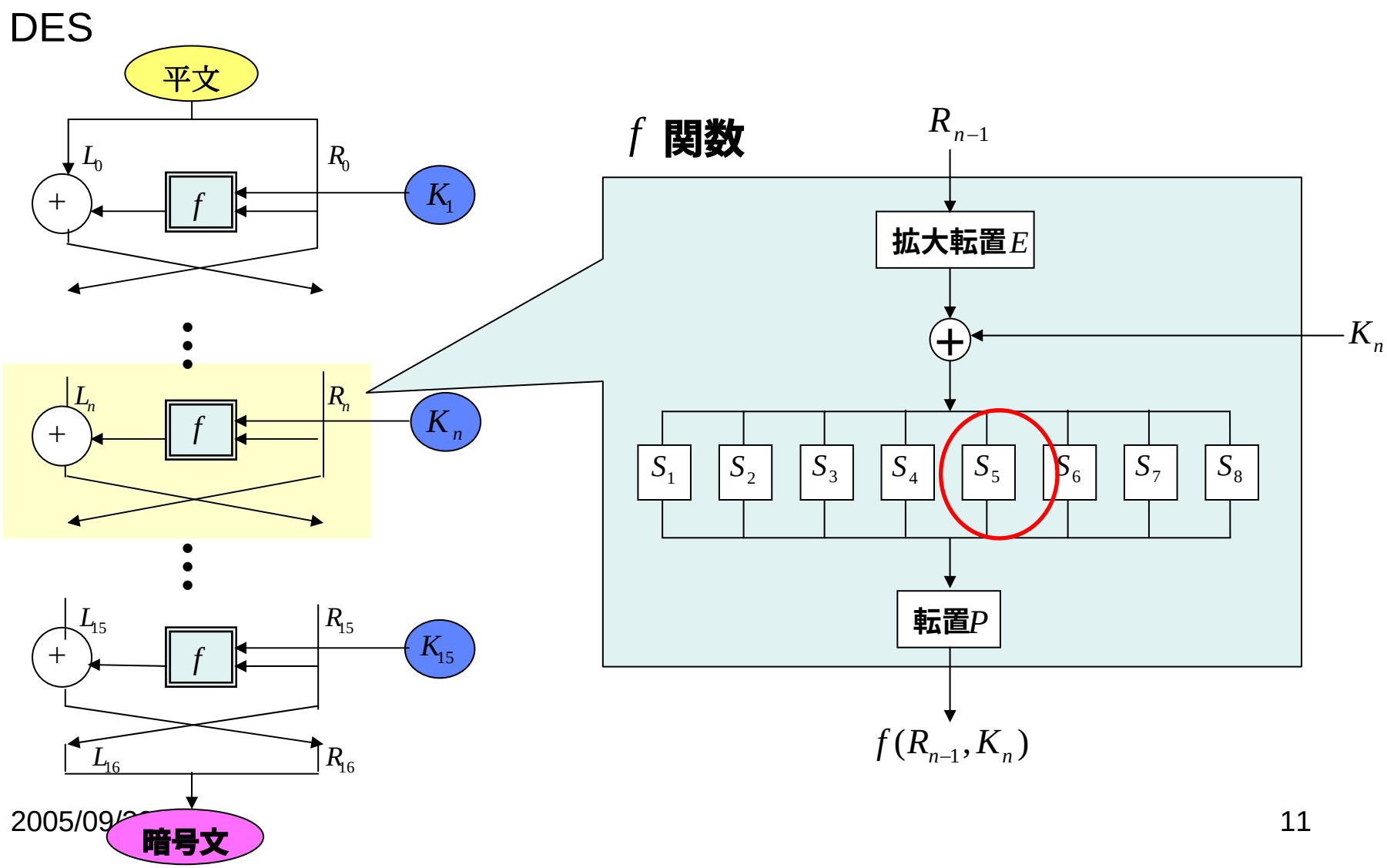


P	C	K
1	1	0
0	1	1
1	0	1

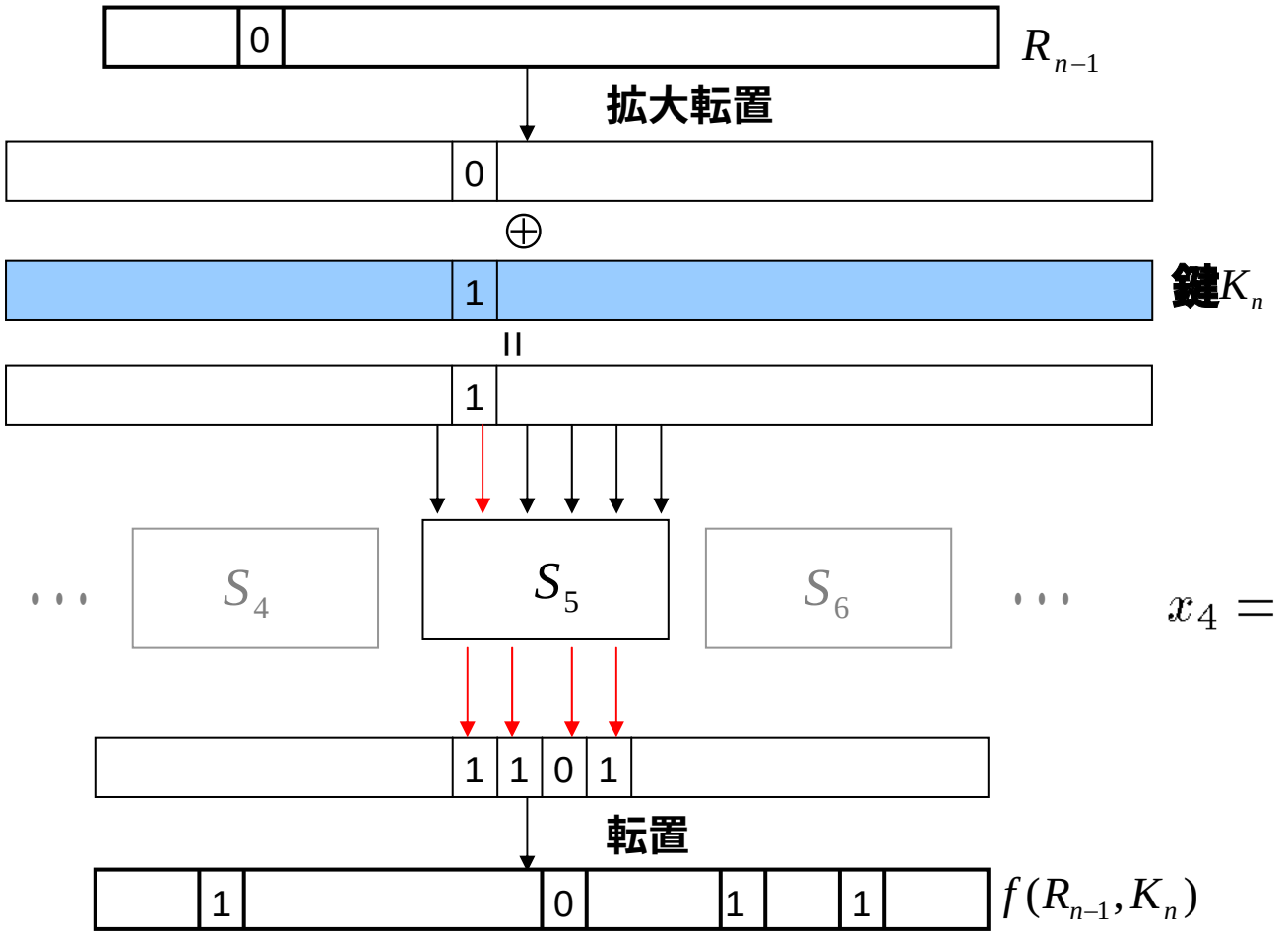
Kが0の確率 ・・・ 1／3
Kが1の確率 ・・・ 2／3

•成立確率が高い線形近似式を選ぶ
•確率を求めるために多数の平文-暗号文対が必要

DESの構成


DES
平文
L_0
R_0
K_1
L_n
R_n
K_n
L_{15}
R_{15}
K_{15}
L_{16}
R_{16}
暗号文
f 関数
R_{n-1}
拡大転置E
K_n
S_1 S_2 S_3 S_4 S_5 S_6 S_7 S_8
転置P
$f(R_{n-1}, K_n)$

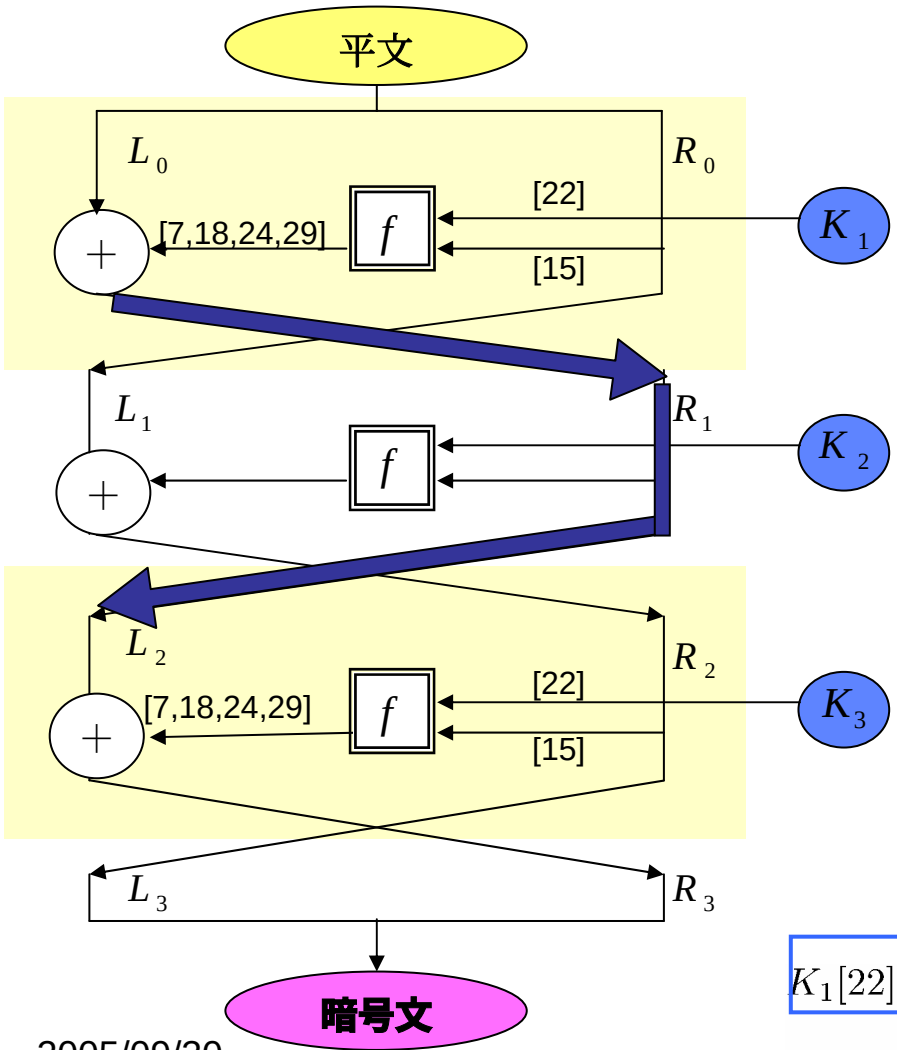
最良表現



$$x_4 = y_0 \oplus y_1 \oplus y_2 \oplus y_3$$

$$R_{n-1}[15] \oplus K_n[22] = f(R_{n-1}, K_n)[7, 18, 24, 29]$$

3段DESの例



1段目と3段目を最良表現で表す

$$K_1[22] = R_0[15] \oplus f(R_0, K_1)[7,18,24,29]$$
$$= R_0[15] \oplus L_0[7,18,24,29] \oplus R_1[7,18,24,29]$$

$$K_3[22] = R_2[15] \oplus f(R_2, K_3)[7,18,24,29]$$
$$= L_3[15] \oplus R_3[7,18,24,29] \oplus L_2[7,18,24,29]$$
$$= L_3[15] \oplus R_3[7,18,24,29] \oplus R_1[7,18,24,29]$$

鍵

$$K_1[22] \oplus K_3[22]$$
$$= R_0[15] \oplus L_0[7,18,24,29] \oplus L_3[15] \oplus R_3[7,18,24,29]$$

平文　　暗号文

鍵の全数探索

- **可能性のある鍵** $2^{56} = (72{,}057{,}594{,}037{,}927{,}936)$ **を全て試す方法**（**力ずく、最も単純だが時間がかかる方法**）

- **解読コンテスト**（DES Challenge）
  １９９７～１９９９年、RSA Security**社が開催**

  コンテスト問題 ： DES**により暗号化された暗号文**
  平文テキスト ： **誰にも知られていないテキスト**
  （**メッセージ・ヘッダ** The secret message is :）
  秘密鍵 ： **コンテスト生成ソフトウェアがランダムに作成し、破壊したものを使用**（**コンテスト管理者も未知**）

DES Challenge

時期･勝者	解読時間	
１９９７年1月 DES Challenge Ⅰ Rocke Vercerらのグループ	９６日	約7万台のPC ※ 7billion keys per second “Strong cryptography makes the world a safer place”
１９９８年2月 DES Challenge Ⅱ-1 Distributeted.net	４１日	約5万台のPC ※ 34billion keys per second “Many hands make light work”
１９９８年7月 DES Challenge Ⅱ-2 EFF (Electronic Frontier Foundation)	５６時間	$25,000で作成した解読専用マシン 88billion keys per second “It’s time for those 128-,192-,and 256-bit keys”
１９９９年1月 DES ChallengeⅢ Distributeted.net	２２時間	DES専用解読マシン＋ 約１０万台のPC ※ 250billion keys per second “See you in Rome (second AES Conference, March 22-23,1999)”

※インターネット上のパソコンのCPUのアイドル時間を使用

現在の動向

- **安全性が問題視**
  - **５６ビットの鍵長⇒短時間で全数探索可能**
- **DESの後継**
  - T-DES (**１９９８～**)
  - AES (**２００１～**)　**・・・III章**
- **DESの標準暗号取り下げ** (**２００４**)

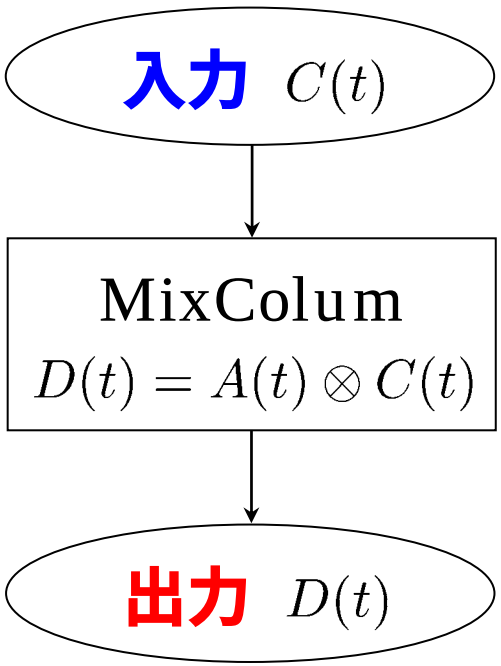
III章

Advanced Encryption Standard による暗号化

目次

- **有限体 $GF(2^8)$ 上の演算**
- MixColumn**処理の流れ**
- **まとめ**

処理の流れ



入力：(c_5 , c_6 , c_7 , c_8)

$$A(t) = (03)_{16}t^3 + (01)_{16}t^2 + (01)_{16}t + (02)_{16}$$

出力：(d_5 , d_6 , d_7 , d_8)

とすると

$$d_5 = 02c_5 \oplus 01c_6 \oplus 01c_7 \oplus 03c_8$$
$$d_6 = 03c_5 \oplus 02c_6 \oplus 01c_7 \oplus 01c_8$$
$$d_7 = 01c_5 \oplus 03c_6 \oplus 02c_7 \oplus 01c_8$$
$$d_8 = 01c_5 \oplus 01c_6 \oplus 03c_7 \oplus 02c_8$$

有限体 $GF(2^8)$ 上の演算

加 算

◆ $(00110101)_2$ と $(01100011)_2$ の加算

$(00110101)_2 \oplus (01100011)_2$ を考えればよい.

$$
\begin{array}{r}
00110101 \\
\oplus\ 01100011 \\
\hline
01010110
\end{array}
$$

加算

||

排他的論理和

有限体 $GF(2^8)$ 上の演算

乗 算 (1/3)

◆ **$(01)_{16} = (00000001)_2$ との乗算**

$(00110101)_2 \times (00000001)_2$ を考える.

$$
\begin{array}{r}
00110101 \\
\times\ 00000001 \\
\hline
00110101 \\
00000000 \\
\vdots \\
\hline
00110101
\end{array}
$$

$(01)_{16} = (00000001)_2$ との乗算

||

通常の演算で1を掛ける

有限体 $GF(2^8)$ 上の演算

乗 算 (2/3)

◆ **$(02)_{16} = (00000010)_2$ との乗算**

$(00110101)_2 \times (00000010)_2$ **を考える.**

$$
\begin{array}{r}
00110101 \\
\times\ 00000010 \\
\hline
00000000 \\
00110101 \\
\vdots \\
\hline
01101010
\end{array}
$$

$(02)_{16} = (00000010)_2$ との乗算

||

1ビット左にシフト

有限体 $GF(2^8)$ 上の演算

乗 算 (3/3)

◆ $(03)_{16} = (00000011)_2$ との乗算

$(00000011)_2 = (00000010)_2 \oplus (00000001)_2$ のように分解できる.

つまり, 任意の値 m との演算を考えた場合,

$m \times (03)_{16} = m \times (02)_{16} \oplus m \times (01)_{16}$ と言える.

$(03)_{16} = (00000011)_2$ との乗算

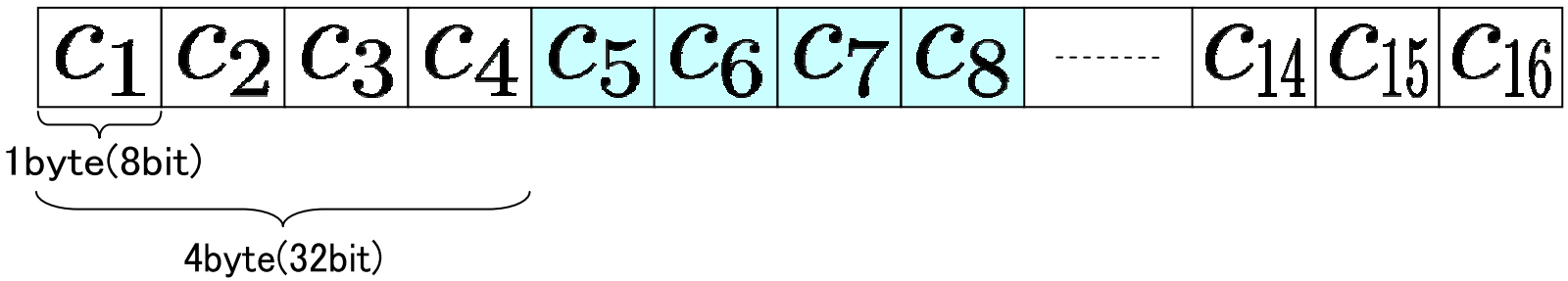
||

$(02)_{16}$ との乗算とXOR

※ XOR : 排他的論理和

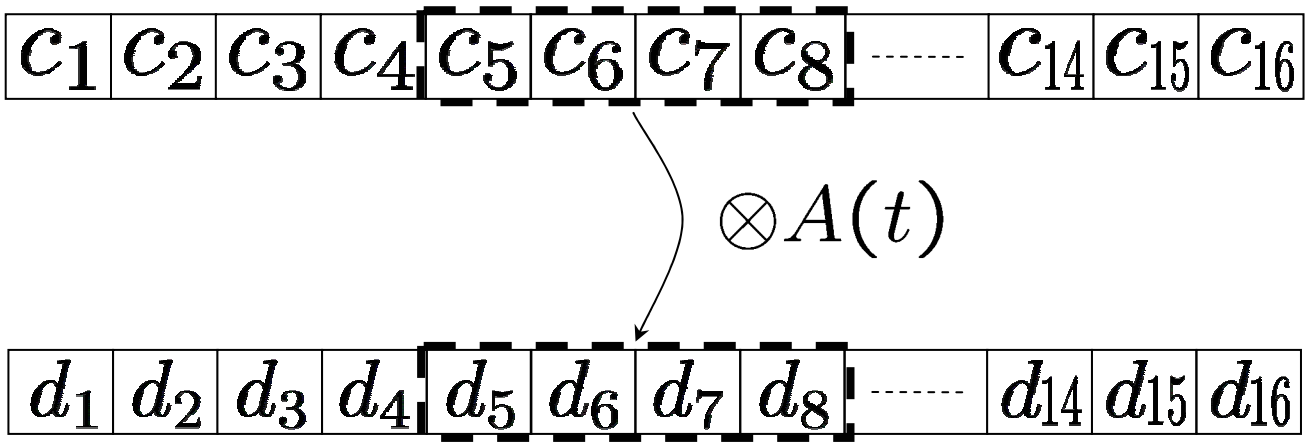
MixColumns

処理の流れ (1/7)



1byte**ずつ区切り，4つのブロック** (4byte) **ごとに演算による変換を行う．**

処理の流れ (2/7)



$$d_5 = 02c_5 \oplus 01c_6 \oplus 01c_7 \oplus 03c_8$$
$$d_6 = 03c_5 \oplus 02c_6 \oplus 01c_7 \oplus 01c_8$$
$$d_7 = 01c_5 \oplus 03c_6 \oplus 02c_7 \oplus 01c_8$$
$$d_8 = 01c_5 \oplus 01c_6 \oplus 03c_7 \oplus 02c_8$$

処理の流れ (3/7)

入力 (c_5, c_6, c_7, c_8)

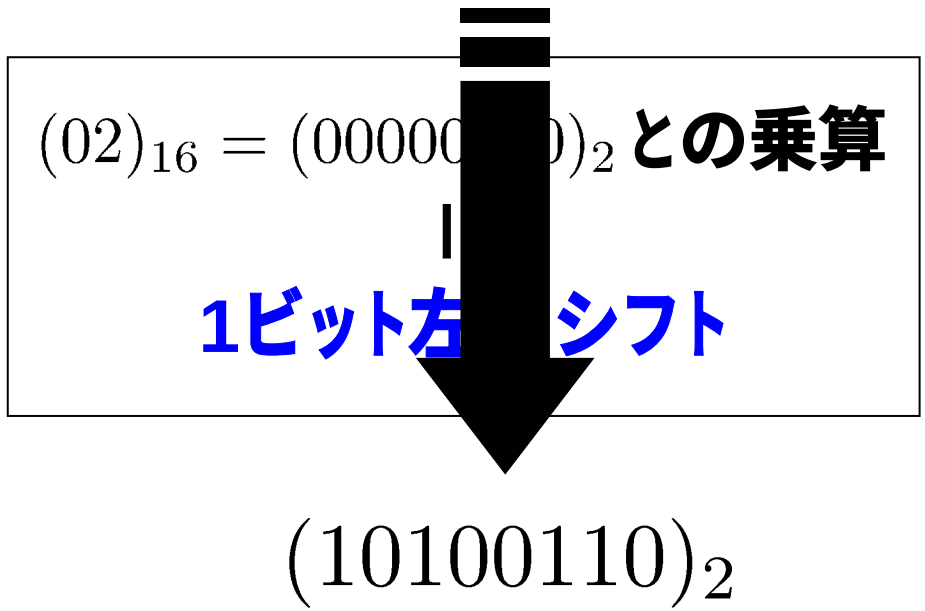
$= (01010011, 00111001, 00011010, 00111110)$

としたときの， $d_5 = 02c_5 \oplus 01c_6 \oplus 01c_7 \oplus 03c_8$ **の演算結果を求める過程を示す．**

MixColumns

処理の流れ (4/7)

$$02c_5 = (02)_{16} \times (01010011)_2$$



$$(10100110)_2$$

処理の流れ (5/7)

$$01c_6 = (01)_{16} \times (00111001)_2$$

$(01)_{16} = (00111001)_2$ **:の乗算**

||

通常の演算で1を掛ける

$$01 \quad)_2$$

$$= (00011010)_2$$

処理の流れ (6/7)

$$03c_8 = (03)_{16} \times (001$$
$$= (0$$
$$= (0$$
$$= (01000010)_2$$

$$\begin{array}{r} 01111100 \\ \oplus\ 00111110 \\ \hline 01000010 \end{array}$$

$.110)_2$

$(03)_{16} = (0000($

2

$(02)_{16}$との乗算とXOR

MixColumns

処理の流れ (7/7)

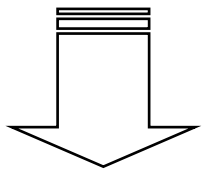
$$d_5 = 02c_5 \oplus 01c_6 \oplus 01c_7 \oplus 03c_8$$
$$= (10100110)_2 \oplus (00111001)_2 \oplus (00011010)_2 \oplus (01000010)_2$$

$$\begin{array}{r} 10100110 \\ 00111001 \\ 00011010 \\ \oplus\ 01000010 \\ \hline 11000111 \end{array}$$

$$d_5 = (11000111)_2$$

まとめ

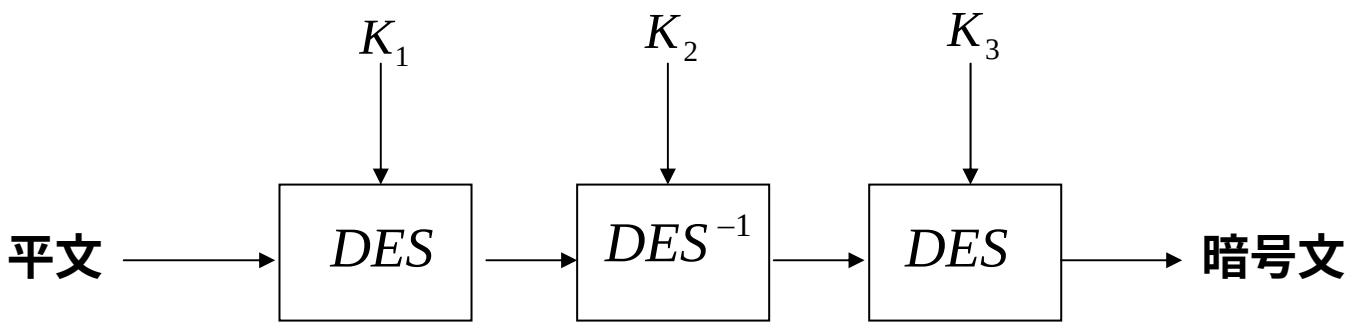
- 住民基本台帳ネットワークシステムや電子申請といった個人情報を含めた情報の電子化
- 企業でも大量の情報を扱っている．



各自が情報の取り扱いやセキュリティについて，ある程度の知識を持つ必要がある

Triple-DES

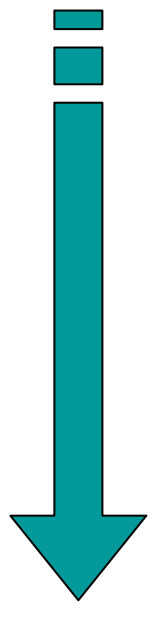
- DES**からの移行が容易**
- DES**処理を3回繰り返すため処理効率が悪い**



$K(K_1, K_2, K_3)$ ：168ビット
$K_1 = K_3$ ：112ビット
$K_2 = K_3$ ：DES

暗号解読のためのアタック法

- 暗号文アタック
  - 十分な暗号文が与えられている場合
- 既知平文アタック
  - いくつかの平文と対応する暗号文対が与えられている場合
- 選択平文アタック
  - 任意の平文に対して暗号文が与えられている場合
- 選択暗号文アタック
  - 任意の暗号文に対して対応する平文が与えられている場合



排他的論理和の計算

X	Y	X XOR Y
0	0	0
0	1	1
1	0	1
1	1	0

同じ値の組み合わせでは結果は0
異なる値の組み合わせでは1