暗号技術入門

溝口洸熙

高知工科大学 情報学群

July 7, 2022

KOCHI UNIVERSITY OF TECHNOLOGY

目次

目次

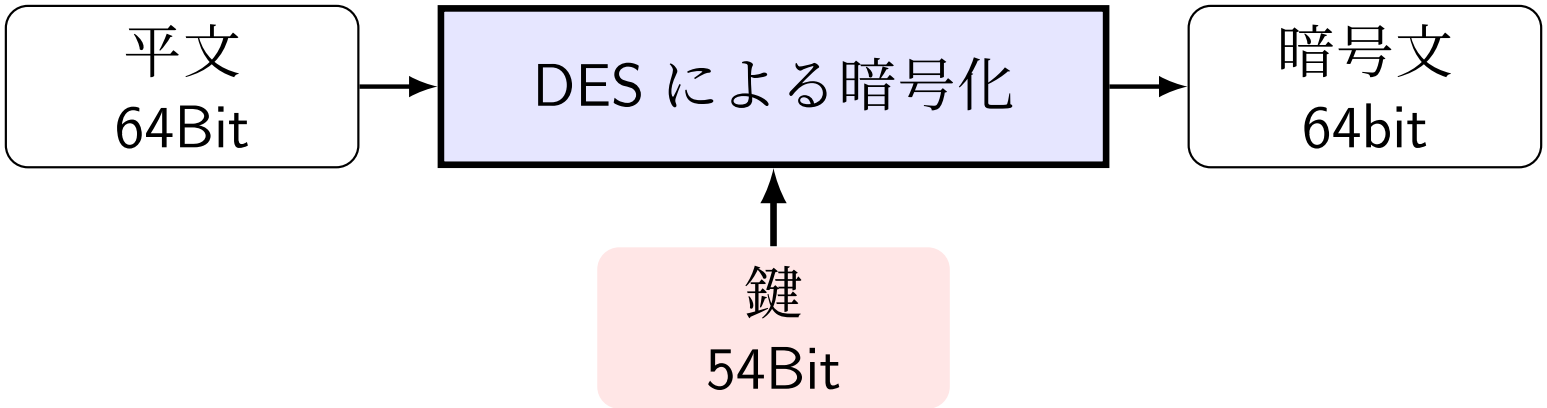
DES(Data Encryption Standard)

DES 概要

DES 暗号は，64bit の平文を 64bit の暗号文に暗号化する**対称暗号**.
鍵のビット長は，56bit.[a]

[a] 64bit だが，エラー検出の情報が 7Bit おきに 1Bit はいるので，実質的には 56Bit.

Fig1-1: 暗号化の概要



DES の構造

DES の構造

DES の基本構造は，ファイステルネットワーク.

ファイステルネットワーク

ラウンドと呼ばれる暗号化の 1 ステップを何度も繰り返すようになっている．これは，多くのブロック暗号[a] で採用されている.

[a] ビット列をまとめて暗号化する暗号アルゴリズム

DES の脆弱性

DES の脆弱性

DES は，ブルート・フォース・アタック[a] で現実的な時間内に解読されてしまう.

[a] 可能な組み合わせを全て試す解読方法.

目次

AES(Advanced Encryption Standard)

AES とは何か？

AES（Advanced Encryption Standard）は，これまで標準にあった DES に代わって，新しい基準となる対象暗号アルゴリズム.
企業や暗号学者から AES の候補として数多の対象暗号アルゴリズムがあり，その中で **Rijndael** という対象暗号アルゴリズムが 2000 年に AES として選定された.

Rijndael

Rijndael

Rijndael は，DES と同じく複数のラウンドから構成されている．DES ではファイステルネットワークという基本構造が使われていたが，Rijndael では **SPN 構造**という構造が使われている．
また，Rijndael の入力ブロックは 128 ビット（16 バイト）．

Rijndael の暗号化

Rijndael の暗号化は，4 ステップに分かれている．

処理	意味	記号 [1)]
SubBytes	バイトごとの置換	SB
ShiftRows	行シフト	SR
MixColumns	列の混合	MC
AddRoundKey	ラウンド鍵との XOR	AR

[1)] このスライドで適当に定義した．