

暗号技術入門

溝口 洸熙¹⁾

高知工科大学 情報学群

June 23, 2022



KOCHI UNIVERSITY OF TECHNOLOGY

¹⁾情報セキュリティシステム研究室

① 共通鍵暗号方式

- DES(Data Encryption Standard)
- AES(Advanced Encryption Standard)

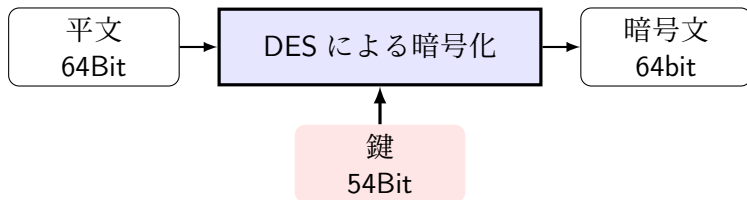
DES(Data Encryption Standard)

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

^a64bit だが、エラー検出の情報が 7Bit おおきに 1Bit はいるので、実質的には 56Bit.

Fig1-1: 暗号化の概要



DES の構造

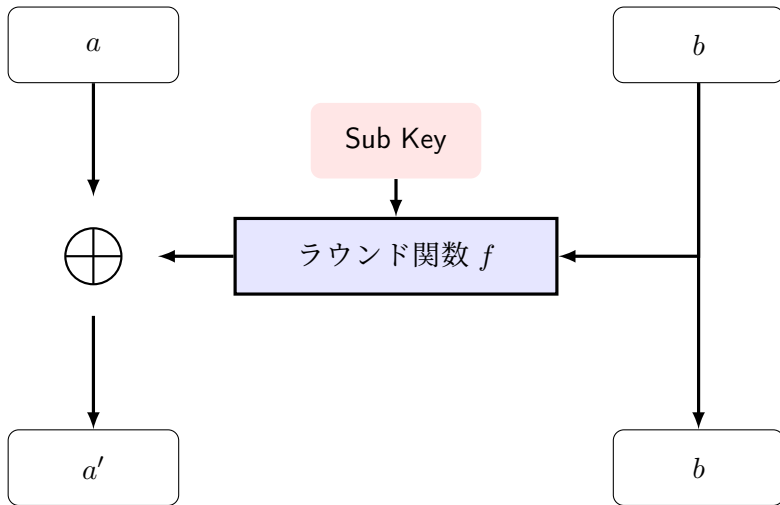
DES の基本構造は，ファイステルネットワーク。

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。ファイステルネットワークの1ラウンドをFig1-2に示す。

^aビット列をまとめて暗号化する暗号アルゴリズム

Fig1-2: ファイステルネットワークの1 ラウンド



AES(Advanced Encryption Standard)