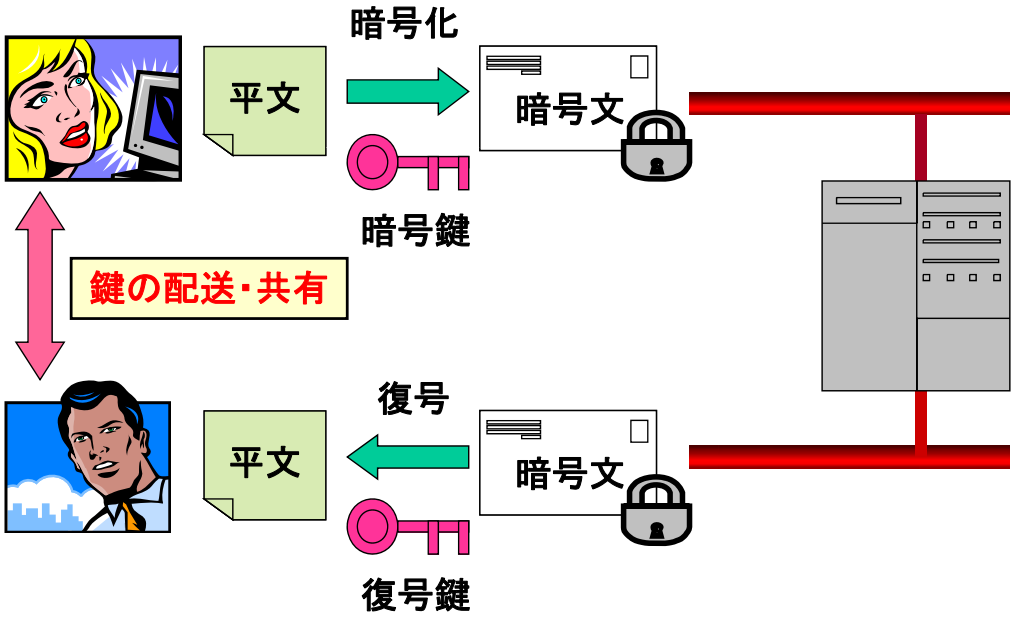
暗号技術　－共通鍵暗号方式－

- 共通鍵暗号方式
- DES (Data Encryption Standard)
- 暗号攻撃
- DESからトリプルDES（T-DES）へ
- AES (Advanced Encryption Standard)
- ブロック暗号の使い方

共通鍵暗号／秘密鍵暗号

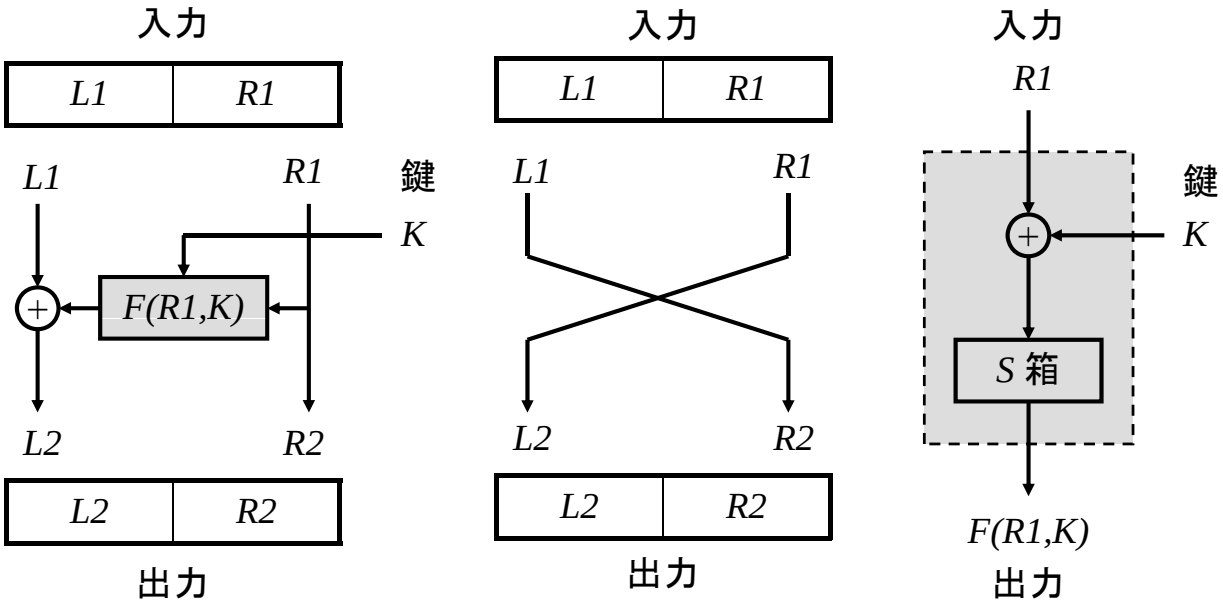
- 暗号鍵＝復号鍵　⇒　鍵の配送問題
- 転置式暗号、換字式暗号、・・・・
- DES (Data Encryption Standard) 暗号



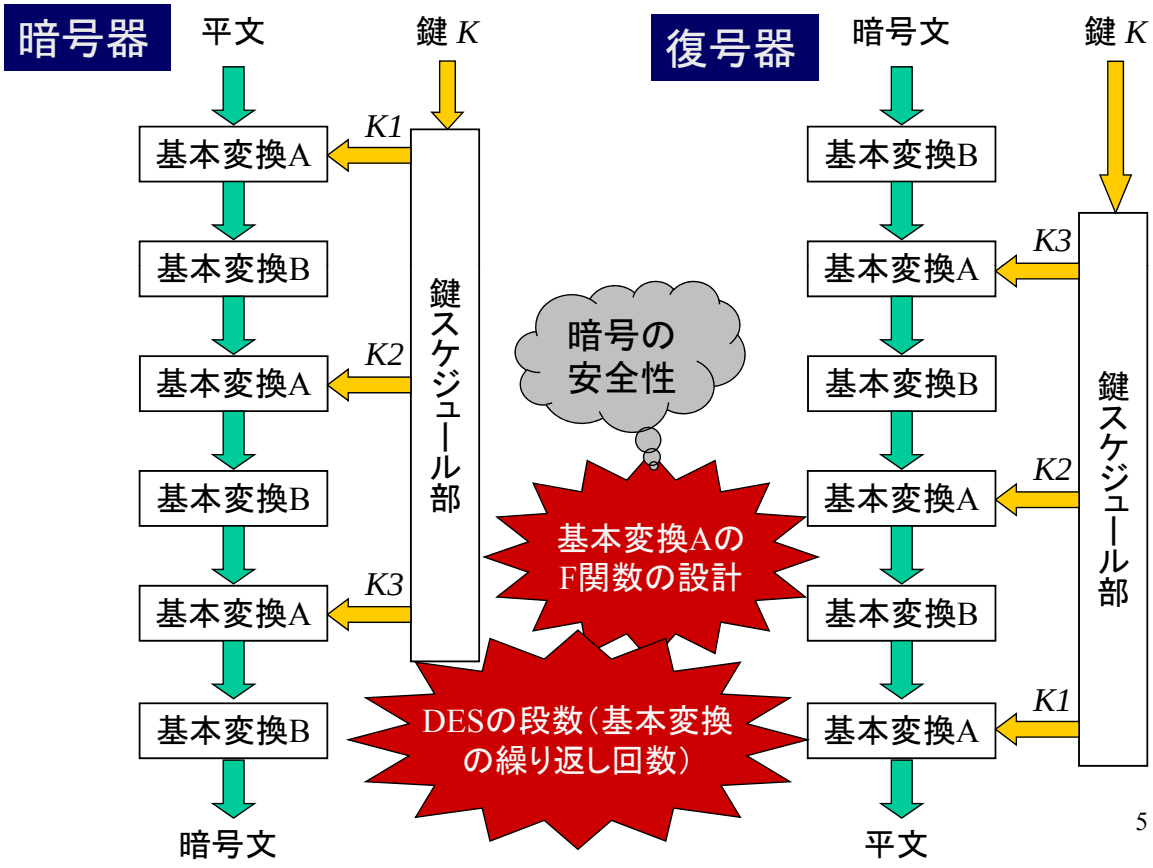
DES（Data Encryption Standard, データ暗号化規格）

- 1974年：IBMにより開発される。
- 1977年：アメリカ連邦政府の標準暗号となる。
- ブロック暗号（*n* ビットブロック暗号）
  平文 64 or 128 ビット ⇒ 暗号文 64 or 128 ビット
- 鍵（鍵長 56 ビット） ⇒ 鍵スケジュール部で副鍵をつくる。
- 暗号のしくみを完全に公開 ⇒ 従来の暗号のイメージを完全に変える。「暗い」暗号から「明るい」暗号へ。ネットワーク暗号、現代暗号の幕開け。
- フェイステル型暗号 ⇒ 基本変換AとBを繰り返す構造をもつ。
- 繰り返し型ブロック暗号

DES (Data Encryption Standard) 暗号（1）



DES (Data Encryption Standard) 暗号（2）



暗号解読（1）

- 既知平文攻撃

「同じ鍵で暗号化された平文と暗号文の対がいくつか攻撃側の手にわたるという状況」

- 暗号文攻撃

「同じ鍵で暗号化された暗号文がいくつか攻撃側の手にわたるという状況」

既知平文攻撃を想定すべき。
既知平文攻撃に耐えるなら、暗号文攻撃にも耐える。

暗号解読（2）

暗号に高い安全性が要求される場合には、

- 選択平文攻撃

「攻撃側が勝手に選んだ平文に対して、同じ暗号鍵で暗号化した暗号文が入手できるという状況（攻撃側にとって極めて都合のよい平文と暗号文の対が入手できるという状況」⇒ 既知平文攻撃の（防御側にとって）ほぼ最悪の場合

- 選択暗号文攻撃

「攻撃側が勝手に選んだ暗号文（もちろん、攻撃側が解読の対象とする暗号文以外の暗号文）に対し、それに対応する平文が得られるという状況」

DES暗号の攻撃（選択平文攻撃）

✓ あらゆる平文に対応する暗号文を求め、平文と暗号文の対応表を作る。

⇒ 対策：平文を長くする。例えば、64ビットとすれば、現在の記憶装置の技術ではこの攻撃は不可能。

⇒将来は？ 記憶装置の進歩・・・いつまでも安全ではない！

✓ 鍵の全数探索

1990年代後半～

「鍵長56ビットのDESはもはや安全ではない！」

⇒ 全数探索攻撃がコンピュータとネットワークの進歩で1日以内で可能。

⇒ 対策：鍵を長くする。例えば、80ビット程度にすれば、現状では不可能。

⇒ 将来は？ コンピュータの進歩・・・いつまでも安全ではない！

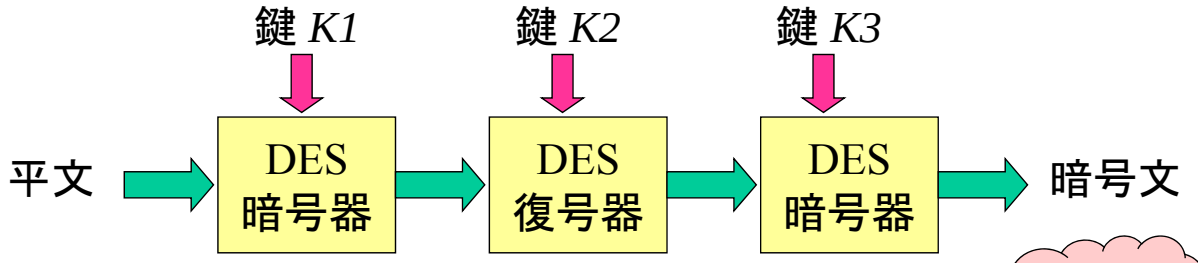
✓ 差分攻撃法（差分解析法）

⇒ 平文の変化に対して、各段の出力ビットの変化の確率がちょうど0.5とはならず、多少偏ることがあることを利用して鍵の一部を推定する攻撃法

⇒ 対策：DESの段数、S箱の設計

T-DES（トリプルDES）

DESを3回繰り返して用いる（DESの中継暗号）。



鍵 *K1*, *K2*, *K3* 独立 ⇒ 3鍵T-DES（鍵長168ビット）

当面は安全

鍵 *K1*=*K3*, *K2* ⇒ 2鍵T-DES（鍵長112ビット）

（ 鍵 *K1*=*K2*=*K3* ⇒ DES（鍵長56ビット））

（Q) なぜ繰り返し回数を2回にしないのか？
（A) 2回だと中間一致攻撃や差分攻撃を受けるから。

AES（Advanced Encryption Standard, 先端暗号化規格）

- 1997年　米国連邦政府がDESの後継暗号として公募
- 2001年　ベルギーの研究者が発明した暗号「ラインドール（Rijndael）」を米国連邦政府標準暗号に制定

AES暗号（ラインドール暗号）の特徴

- 鍵の長さ: 128ビット、192ビット、256ビット（選択）
- 128ビットブロック暗号（平文・暗号文：128ビット）
- 繰り返し型ブロック暗号
- SPN（Substitution（換字）-Permutation（置換） Network）型暗号
- 差分攻撃法など、これまでに知られている各種の攻撃に耐え得るように設計

ブロック暗号の使い方（1）

A)　ECB方式（Electronic Code Book、電子符号帳）

「単に nビットの平文をそのまま暗号化する。」

送るべき平文がランダムになっていないと危険！

例えば、普通の言語や音声・画像をそのまま暗号化する場合

✓ 日本語　漢字　2バイト／文字

⇒ 64ビットDESでは漢字4文字単位で暗号化

✓ 画像　8ビット／画素

⇒ 64ビットDESでは8画素単位で暗号化

64ビットに現れる組合せの数が限られてしまう！

ブロック暗号の使い方（2）

送るべき平文がランダムになるように改良

B)　CBC方式（Cipher Block Chaining）

C)　CFB方式（Cipher Feedback）

D)　カウンタ方式／OFD方式（Output Feedback）

送り側も受け側も、全く同じしくみで同じ擬似ランダム系列を発生させ、送り側では平文に加えて暗号文をつくり、受け側では受け取った暗号文に加えて平文を得る。