

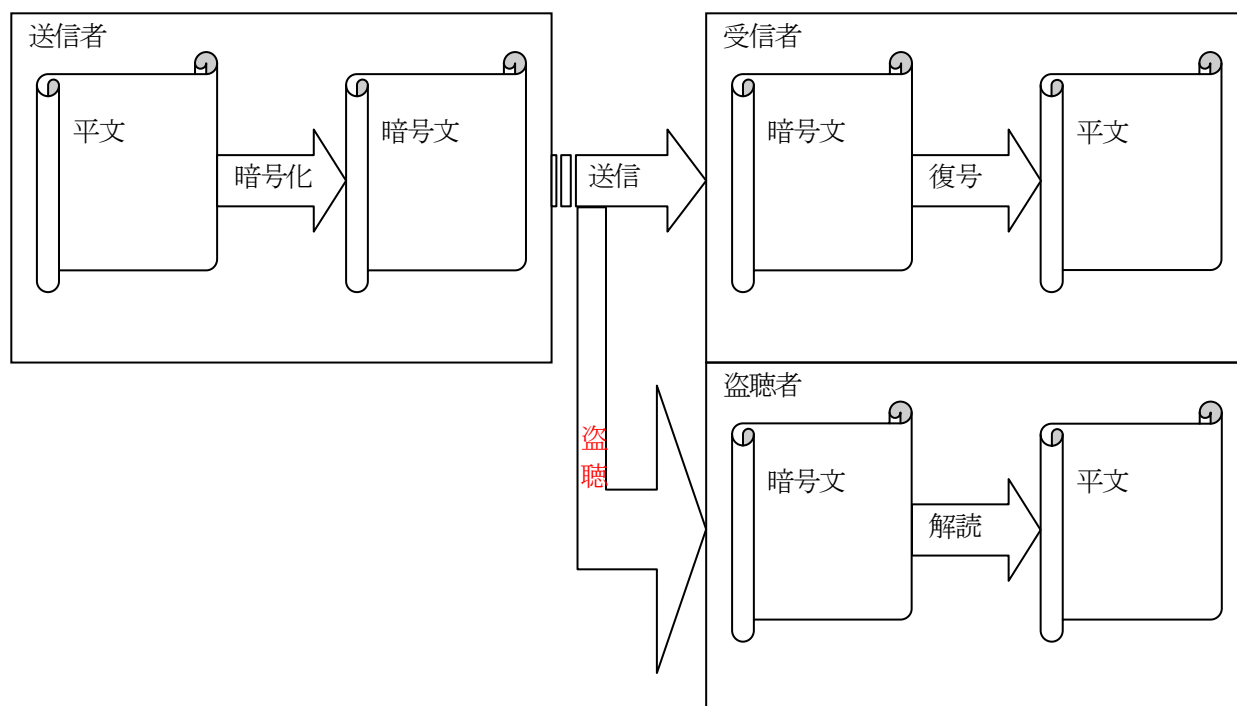
暗号

暗号通信

- ◎ ホームページの暗号規格 https など
- ◎ 電子メールの暗号規格 PGP など

暗号化していない電子メールで大切な情報を **絶対に** 送信しない。

暗号



カエサル暗号

| 平文 | 暗号化鍵＝「2つ後ろの文字に変える」 | 暗号文 |
|----|--------------------|-----|
| あ | → | う |
| い | → | え |
| う | → | お |
| え | → | か |
| お | → | き |
| か | → | く |
| き | → | け |
| ・ | | ・ |

| | | |
|---|--|---|
| ▪ | | ▪ |
| ▪ | | ▪ |

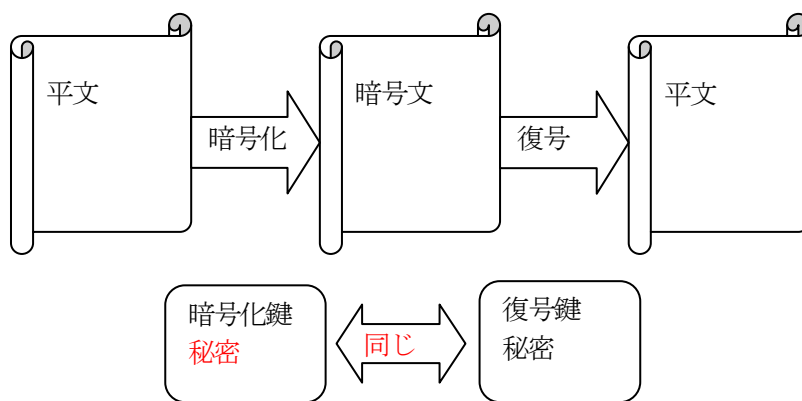
例 あんごう→ういじお

問題

暗号化鍵=「1つ後ろの文字に変える」のカエサル暗号を使ったときの暗号文「きあさ」を復号しなさい。

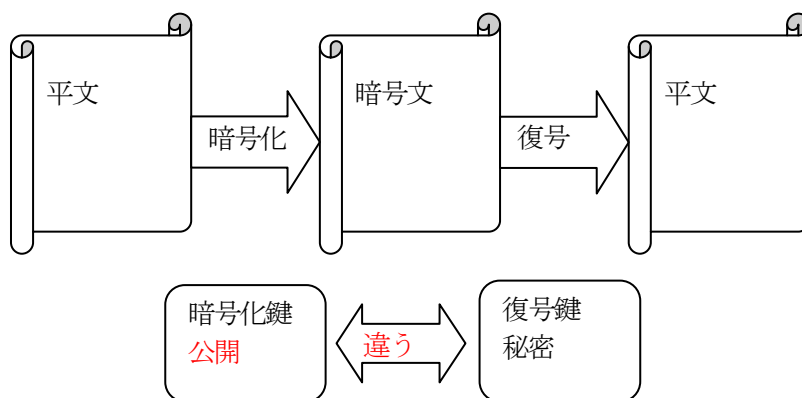
秘密鍵暗号

- ◎ 以前使用されていた暗号
- ◎ カエサル暗号は秘密鍵暗号の最も簡単なもの



公開鍵暗号

- ◎ 現在人の常識となりつつある暗号



- ◎ 公開鍵暗号理論の優れた処

暗号化鍵と復号鍵が違う⇒秘密の復号鍵は1人(受信者)だけが知っていれば良い。

暗号化鍵から復号鍵を推測することが極めて困難⇒通常 70 桁以上の素数を 2 つ使って鍵を作成する。

参考ホームページ

© 「サルにもわかる RSA 暗号」 <http://www.maitou.gr.jp/rsa/>