暗号技術入門

第2章「歴史上の暗号」

暗号技術入門

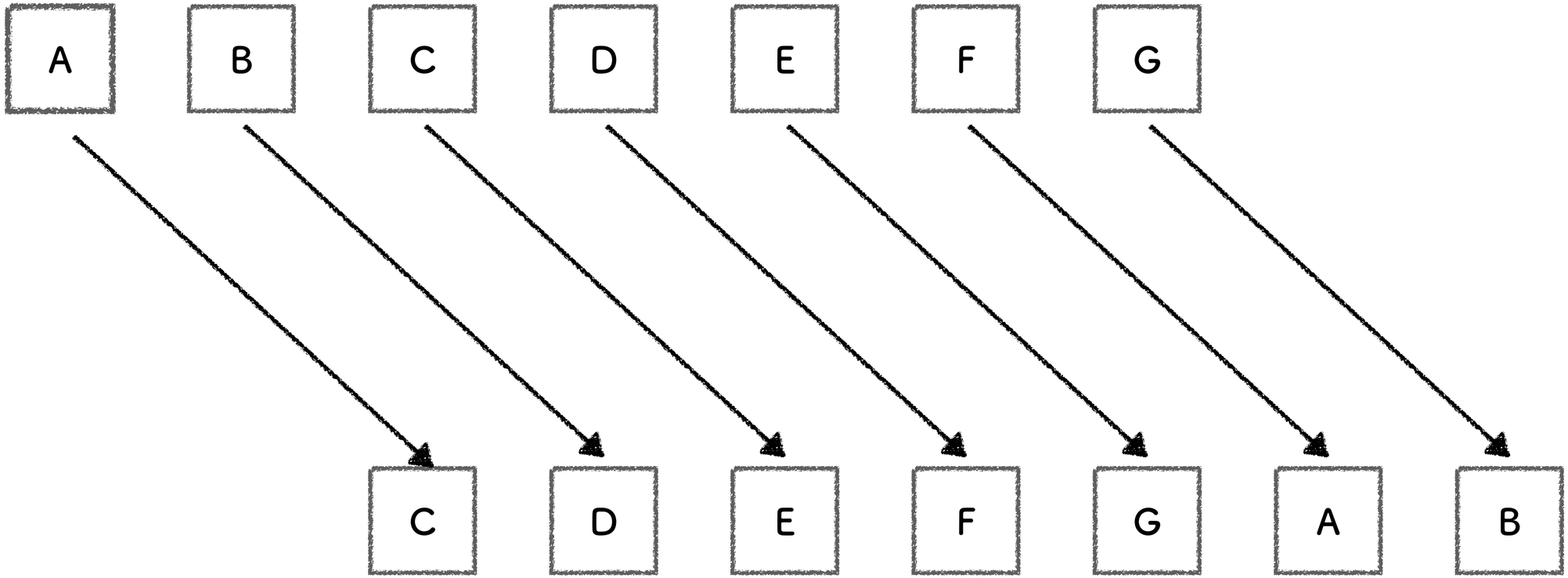
出版：SB Creative

著者：結城 浩

第三版は2015年発行。暗号化技術の基礎から丁寧に解説されており、各所で初心者にお勧めされている。改訂版ではビットコインなど最新の情報も記載。

シーザー暗号
単一換字暗号
エニグマ

シーザー暗号



ずらすやつ

シーザー暗号の復号化

・シーザー暗号では「◯文字ずらす」という情報が鍵となる。

・解読は**ブルート・フォース・アッタク**（**総当たり攻撃**）で可能。

クイズ

解読してみよう！

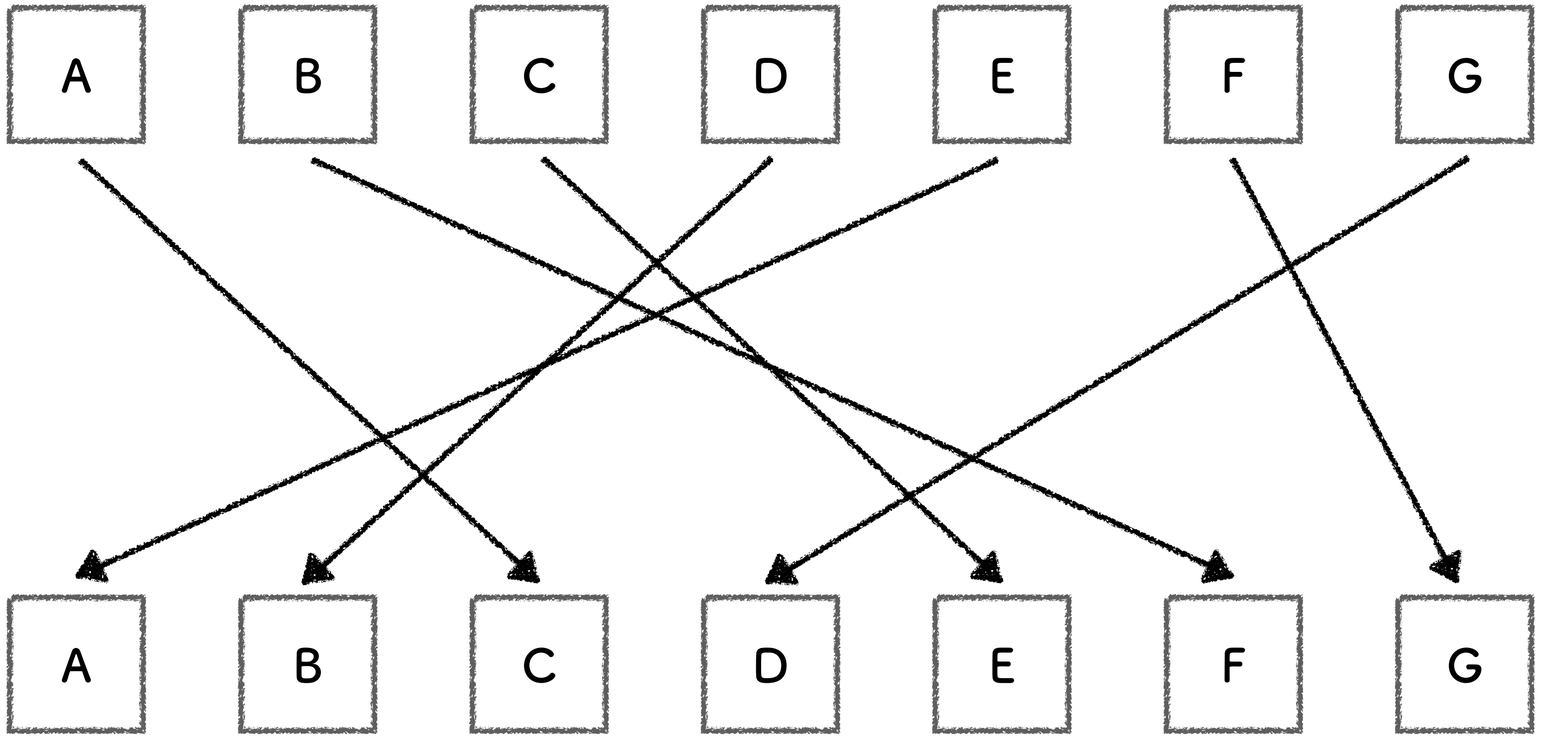
PELCGBTENCUL

クイズ

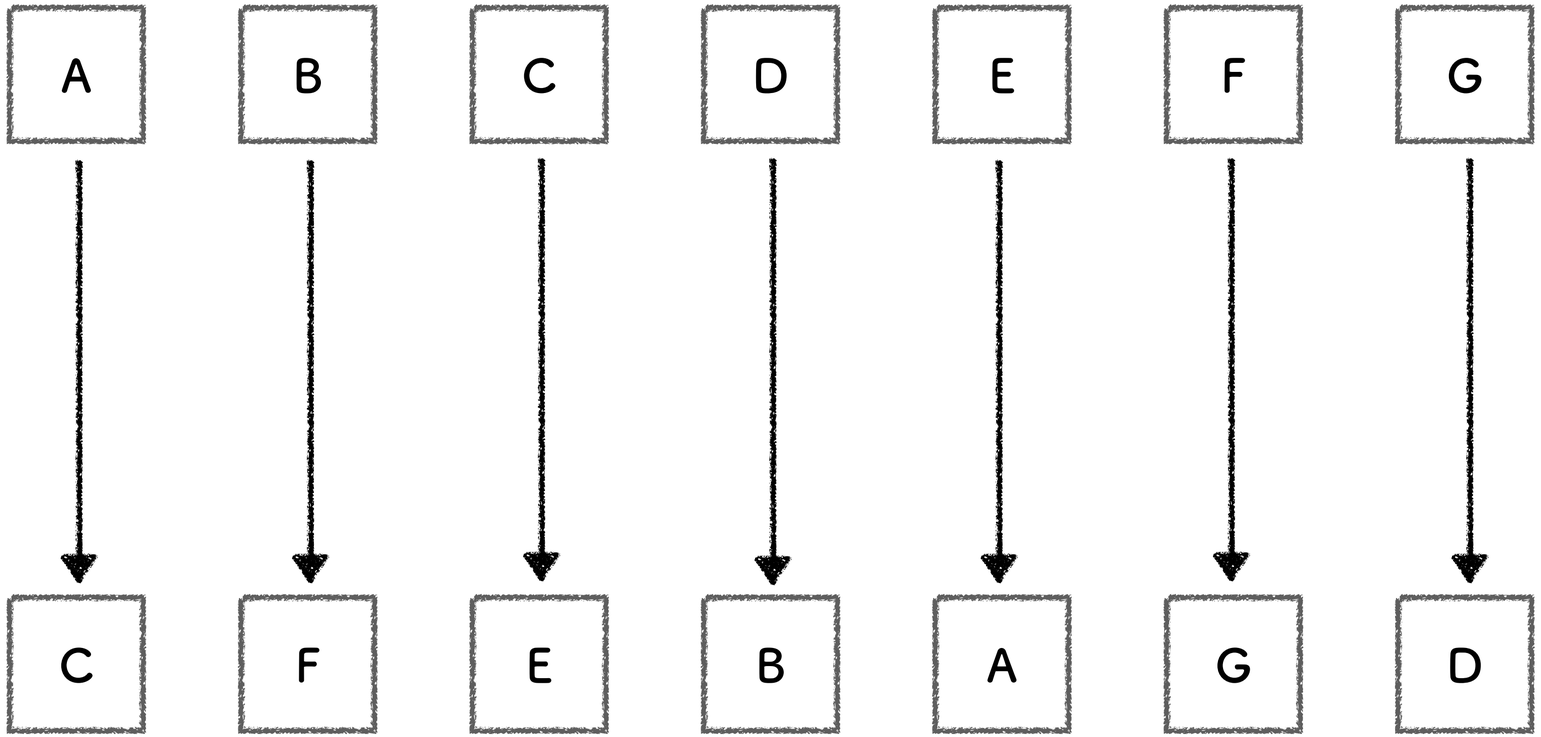
PELCGBTENCUL

```python
# seasar

# chr(64) = "@"
# chr(65) = "A"
# chr(66) = "B"

def encrypt(plain_text, shift_num):
    retval = ""
    for s in plain_text:
        # アルファベット外へ行ったら"A"まで巻き戻す
        if ord(s) + shift_num > 90:
            retval += chr(ord(s) + shift_num - 26)
        else:
            retval += chr(ord(s) + shift_num)
    return retval

# print(encrypt("CRYPTOGRAPHY",13))

def burute_force_attack(str):
    # 26回
    for i in range(26):
        ans = ""
        for s in str:
            # アルファベット外へ行ったら"A"まで巻き戻す
            if ord(s) - i < 65 :
                ans += chr(ord(s) - i + 26)
            else:
                ans += chr(ord(s) - i)

        print(f"鍵{i}で復号化 -> {ans}")

burute_force_attack("PELCGBTENCUL")
```

単一換字暗号



一対一対応を作る



一対一対応を作る

単一換字暗号の復号化

・「こうやって対応するよ」という換字表が鍵となる。

・ブルートフォースアタックは困難。流石に無理がある。

・全ての鍵の集合を**鍵空間**と呼ぶが、この暗号では鍵空間の大きさが
4兆の1000兆倍などとなり、総当たりでは困難である。

・「頻度分析」という手法を用いる。

頻度分析

・暗号文中に高頻度で出現する英文字と、そもそも一般の英文で高頻度に出現する英文字を比べる。

・詳しくは本を見よう。

エニグマ

エニグマ

・ドイツのシュルビウスにより発明された暗号機。

・ナチスドイツ時代にドイツ国防軍に採用され、改良の後、第二次世界大戦で活躍した。

・日替わりの鍵表を用いていた。

・詳しく知りたい人は本を読もう。