**２年 プログラミング基礎＆演習I（2024年7月17日（水））**

**文字列の応用（**Caesar暗号）

　通信などで送られる文書データを他人が読めないようにすることを「暗号化」と呼び，暗号化された文書データを元の状態に戻すことを「復号化」と呼ぶ．暗号化される前の文書データを「平文（ひらぶん）」と呼び，暗号化された文書データを「暗号文」と呼ぶ．

　暗号化には，様々なアルゴリズムがあるが，単純な暗号化方式としては，平文を構成する個々の文字の文字コードを，何らかの規則によって他の文字コードに変換することである．この変換に使用される数値データを「鍵」と呼ぶ．この方式の暗号化のアルゴリズムの中ではCaesar暗号が有名である．Caesar暗号は，平文の文字コードに特定の数を加えることで暗号化し，暗号文の文字コードから同じ数を引くことで復号化する．例えば，「kisarazu」を鍵1で暗号化すると，「ljtbsbav」となる．

参考文献： サイモン シン，青木薫訳「暗号解読(上)(下)」，新潮文庫，2007．

**第17回課題**

課題番号 No0717\_1.c **(要チェック)**

|  |
| --- |
| 鍵1で暗号化された「lpvtfotbjlpvuboptijjob」を復号化して画面に出力するプログラムを作成せよ．暗号文は文字列として，あらかじめプログラムに書き込むことにする．例えば、次のようにchar型配列を宣言することになる．  　char cyphertext[] = “lpvtfotbjlpvuboptijjob”; |

課題番号 No0717\_2.c

|  |
| --- |
| Caesar暗号方式で，平文「hayakukoikoinatsuyasumi」を暗号化して画面に出力するプログラムを作成せよ．平文は文字列として，あらかじめプログラムに書き込むことにする．例えば、次のようにchar型配列を宣言することになる．  　char plaintext[] = “hayakukoikoinatsuyasumi”;  　鍵の値はユーザーがキーボードから入力できるようにすることとする． |

超発展10(chohatten10.c)

|  |
| --- |
| 換字式暗号で英小文字が数字に暗号化されている．これを解読するプログラムを作成せよ．以下に暗号文を示す．  　ただし，スパイによって以下のことが判明している．  ・元の文章は高専に関するものである．  ・すべて同様の暗号化の方法をとっている．  ・あるアルファベットは，2桁の数字に置き換えられている．  (1)667050865286364666584674385846665846485846507860625860748666665846  (2)665846507860728648584878625838587074866666584680785046  (3)6858467258464858707884864886707066466686706678704886707066466686706678704858707884866858467258466658467486666686 |