1　シーザー暗号

広義の暗号は秘密通信全般を指す。これに対して、文字を他の文字に変換し、直接見ても、わからないようにする狭義の暗号の歴史は、かなり昔にさかのぼる。そして確実な史実であり、現在まで影響を及ぼしている最初のものは、シーザー暗号である。(中略) これは、各文字を、アルファベット順に一定の間隔だけずらした文字に変換する方式であり、その間隔が鍵字に相当する。最初の A が移される文字を鍵字と考えてよい。たとえば、鍵字が D ならば、B は E、C は F、・・・に移される。これは、きわめて初歩的な暗号であり、ローマ時代には、ともかく現在では熟練者なら「一目で読んでしまう」といわれる。しかし、これが現在慣用の暗号の鍵である。
暗号の数理　一松信著　ブルーバックス　33 頁

1.1　シーザー暗号 ceasar.c

```
/*
  シーザー暗号 (Ceasar Cipher)
  ceasar.c
*/
#include <stdio.h>

int main()
{
  int code[6];
  int i;

  code[0] = 'H';
  code[1] = 'e';
  code[2] = 'l';
  code[3] = 'l';
  code[4] = 'o';
  code[5] = '\0';

  for(i = 0; i < 5; i++){
    printf("%c", code[i]);
  }
```

```
  printf("->\n");

  for(i = 0; i < 5; i++){
    printf("%c", code[i] + 5);
  }

  return 0;
}
```