Crypto Analysis L01

eqbpntwemza
원래의 문자열로 변환 후 인증하시오

— Author: CodeEngn

이걸 보고 바로 카이사르가 생각났다. (사실 만만한게 카이사르)
얼마전 다른 워게임 사이트에서 사용했던 카이사르 복호화 프로그램을 사용해보기로 했다.

== Caesar_decriptor.c ==

```c
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <conio.h>

void decrypt(char *cipher_text, int key) {
    char *copied_cipher;
    int length, flag, i;

    length = strlen(cipher_text);
    copied_cipher = (char *)malloc(sizeof(char) * length);  // 복사본을 건드린다. 원본을 건드리면 다음 key값으로 복호화 안댐

    for (i = 0; i < length; i++) {
        if (cipher_text[i] == ' ') { printf(" "); continue; }   // 공백은 무시

        if (cipher_text[i] >= 'a' && cipher_text[i] <= 'z') flag = 97;
        else if (cipher_text[i] >= 'A' && cipher_text[i] <= 'Z') flag = 65;

        copied_cipher[i] = cipher_text[i] - flag;
        copied_cipher[i] = (copied_cipher[i] + key) % 26;   // key 만큼 shift
        printf("%c", copied_cipher[i] + flag);
    }
    printf("₩n₩n");
    free(copied_cipher);

    return;
}

void main() {
    char *cipher;
    int key = -1, i;

    cipher = (char *)malloc(sizeof(char) * 100000); // 암호문은 100,000 까지

    printf("==== Caesar Decrpytion ==== ₩n");
    //printf("input key (0 ~ 26)₩n");
    //printf("if you don't know key, input -1₩n");
    //printf("key = "); // 키값 입력
    //scanf("%d", &key);
    //fflush(stdin);
    printf("cipher text = ");   // 암호문 입력

    gets_s(cipher, 100000);    // visual studio에서는 보안때문에 gets()를 지원 안한다고한다.

    printf("cipher = %s₩n", cipher);

    if (key == -1) {
        for (i = 1; i <= 25; i++) {
            printf("shift %d ==================₩n", i);
            decrypt(cipher, i);
        }
    }
    else {
        printf("shift %d ================₩n", key);
        decrypt(cipher, key);
    }
    free(cipher);

    return;
}
```

== RESULT ==

```
==== Caesar Decrpytion ====
cipher text = eqbpntwemza
cipher = eqbpntwemza
shift 1 ==================
frcqouxfnab

shift 2 ==================
gsdrpvygobc

shift 3 ==================
htesqwzhpcd

shift 4 ==================
iuftrxaiqde

shift 5 ==================
jvgusybjref

shift 6 ==================
kwhvtzcksfg

shift 7 ==================
lxiwuadltgh

shift 8 ==================
```

```
shift 8 ==================
myjxvbemuhi

shift 9 ==================
nzkywcfnvij

shift 10 ==================
oalzxdgowjk

shift 11 ==================
pbmayehpxkl

shift 12 ==================
qcnbzfiqylm

shift 13 ==================
rdocagjrzmn

shift 14 ==================
sepdbhksano

shift 15 ==================
tfqeciltbop

shift 16 ==================
```

```
shift 16 ==================
ugrfdjmucpq

shift 17 ==================
vhsgeknvdqr

shift 18 ==================
withflowers

shift 19 ==================
xjuigmpxfst

shift 20 ==================
ykvjhnqygtu

shift 21 ==================
zlwkiorzhuv

shift 22 ==================
amxljpsaivw

shift 23 ==================
bnymkqtbjwx

shift 24 ==================
```

key가 18일 때 withflowers 라는 글자가 나온다.

Key : withflowers