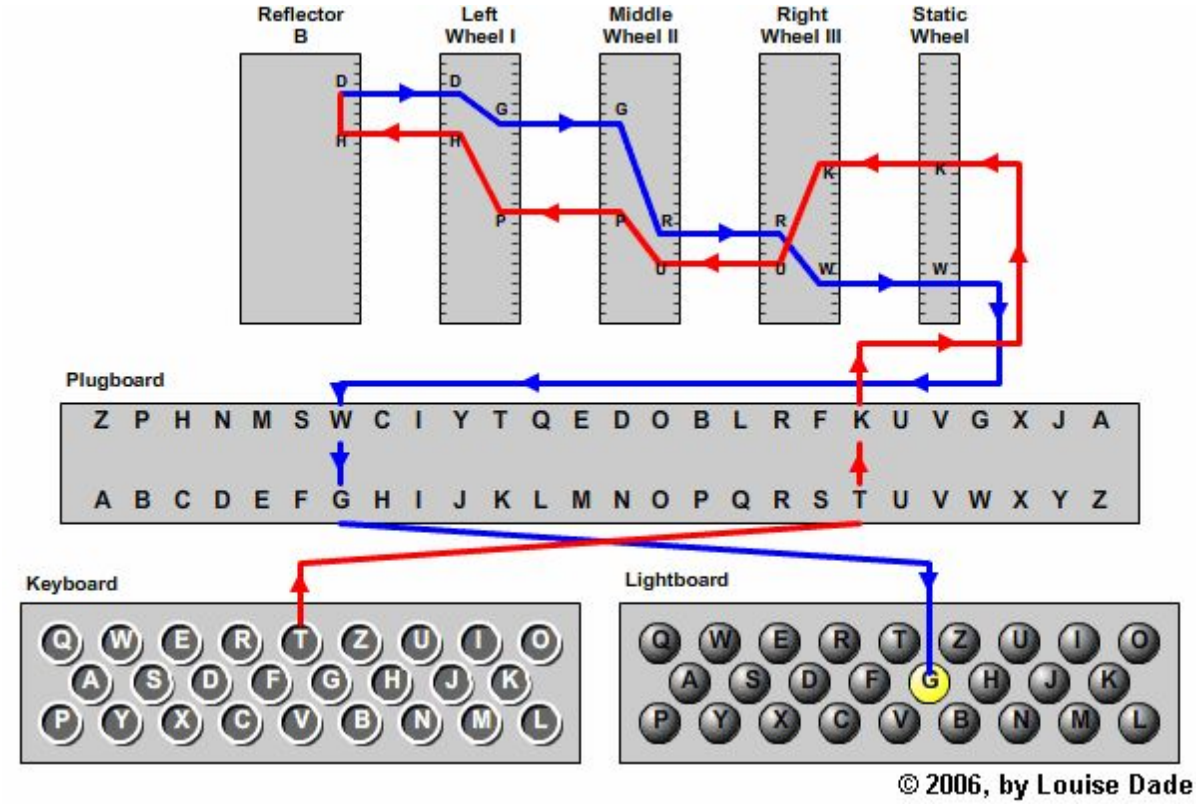
TCC341 - Trabalho 01

Introdução

Em criptografia, uma cifra de substituição é um método que opera de acordo com um sistema pré-definido de substituição, no qual as letras de uma mensagem de texto são substituídas por outras formando um texto cifrado. As cifras de substituição são decifradas pela substituição inversa. Uma cifra de substituição é diferente de uma cifra de transposição, na qual, as letras da mensagem de texto são rearranjadas numa ordem diferente e habitualmente complexa, mas não modificadas. Famosas cifras de substituição são a Cifra de Cesar e a Máquina Enigma.



Objetivo

O seu objetivo nesse trabalho é implementar uma cifra de substituição que funcione de forma parecida com a Cifra de Cesar e a Enigma. Assim como na Cifra de Cesar, sua chave será um número inteiro pelo qual você deve andar a direita da letra atual. Note que esse número pode ser muito maior que 26 (o número total de letras) dando a volta várias vezes no alfabeto até encontrar a letra que será substituída. Ao substituir a letra você deve, assim como na enigma, mudar sua chave, somando o valor da nova letra à chave atual (o A tem valor 1, o B valor 2 e assim até o Z com valor 26).

Por exemplo, ao encriptar a palavra CHANDELIER com a chave inicial 1 teríamos:

- C + 1 = D, como D vale 4 a nova chave será 1 + 4 = 5
- H + 5 = M, como M vale 13 a nova chave será 5 + 13 = 18
- A + 18 = S, como S vale 19 a nova chave será 18 + 19 = 37
- N + 37 = Y, como Y vale 25 a nova chave será 37 + 25 = 62
- D + 62 = N, como N vale 14 a nova chave será 62 + 14 = 76
- E + 76 = C, como C vale 3 a nova chave será 76 + 3 = 79
- L + 79 = M, como M vale 13 a nova chave será 79 + 13 = 92
- I + 92 = W, como W vale 23 a nova chave será 92 + 23 = 115

- E + 115 = P, como P vale 16 a nova chave será 115 + 16 = 131
- R + 131 = S, como S vale 19 a nova chave será 131 + 14 = 150

Para decriptar, devemos fazer o algoritmo inverso, sempre recalculando a chave da mesma maneira. Assim, para a palavra DMSYNCMWPS e chave inicial 1 teríamos:

- D - 1 = C, como D vale 4 a nova chave será 1 + 4 = 5
- M - 5 = H, como M vale 13 a nova chave será 5 + 13 = 18
- S - 18 = A, como S vale 19 a nova chave será 18 + 19 = 37
- Y - 37 = N, como Y vale 25 a nova chave será 37 + 25 = 62
- N - 62 = D, como N vale 14 a nova chave será 62 + 14 = 76
- C - 76 = E, como C vale 3 a nova chave será 76 + 3 = 79
- M - 79 = L, como M vale 13 a nova chave será 79 + 13 = 92
- W - 92 = I, como W vale 23 a nova chave será 92 + 23 = 115
- P - 115 = E, como P vale 16 a nova chave será 115 + 16 = 131
- S - 131 = R, como S vale 19 a nova chave será 131 + 14 = 150

Lembre-se de que todas as contas (somas e subtrações) são feitas como num relógio. Note que o operador % em C retorna o resto da divisão e não o módulo, ou seja, ele pode retornar números negativos e você deve corrigir isso. Além disso, não há limite para o tamanho da mensagem, logo, o valor da chave pode ser somado até que o máximo de um inteiro seja atingindo. Você deve impedir que isso ocorra.

Seu programa deve realizar a encriptação ou decriptação de uma mensagem, sem tamanho pré-definido, apenas de letras maiúsculas de A a Z. Nenhum outro símbolo ou caracter deverá ser encriptado, logo espaços devem ser mantidos, assim como números, quebras de linha e qualqur outro caracter encontrado. Nenhuma letra terá acento. O fim da mensagem é dado por um '#'.

Entrada e Saída

Seu programa deve começar perguntando para o usuário se ele quer encriptar ou decriptar uma mensagem. Após isso, ele deve pedir o valor da chave incial que deve ser um inteiro. Finalmente, seu programa deve encriptar ou decriptar a mensagem que será digitada até que o símbolo '#' seja entrado. Lembre-se de que somente letras maiúsculas devem ser encriptadas/decriptadas, todos os outros caracteres devem ser mantidos. Veja os exemplos a seguir para saber o padrão das frases que devem ser impressas e como a leitura deve ser realizada.

Exemplos

Nos exemplos abaixo a cor azul representa a entrada que deve ser lida pelo seu programa e a cor vermelha, a saída que deve ser gerada pelo seu programa na saída padrão.

Exemplo 1:

Digite D para decriptar e E para encriptar

E

Digite o valor da chave

10

Digite o texto

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG.#

DVO PJHJB UFIZQ ZIA NMRMC BKEW VFI YMYW YIJ.

Exemplo 2:

Digite D para decriptar e E para encriptar

D

Digite o valor da chave

10

Digite o texto

DVO PJHJB UFIZQ ZIA NMRMC BKEW VFI YMYW YIJ.#

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG.

Exemplo 3:

Digite D para decriptar e E para encriptar

E

Digite o valor da chave

100

Digite o texto

THREE RINGS FOR THE ELVEN-KINGS UNDER THE SKY,

SEVEN FOR THE DWARF-LORDS IN THEIR HALLS OF STONE,

NINE FOR MORTAL MEN DOOMED TO DIE,

ONE FOR THE DARK LORD ON HIS DARK THRONE.

ONE RING TO RULE THEM ALL. ONE RING TO FIND THEM,

ONE RING TO BRING THEM ALL AND IN THE DARKNESS BIND THEM.#

PTXIR WKAUB QQK XJQ HWDQQ-EHUID JMPGA DVO RBR,

DTESU HYA DVO CYBUD-NEMLM PK BRGRS BWEJA XM MAWSC,

OYCW UYA WVURQS MRS BODFDG DC UUL,

HOU QQK XJQ GKMS MCID SK PGX GKMS UDRGMQ.

RII EAGG AW WWKO SZWB RUP. IQY KMEC SG EMEZ PTKD,

JSC SCKO QC SBUUI EXST BOD WGD ME PTK UMQAEAPF UWYN RXST.