

Original encrypted string:QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALDDecrypt with shift -3 :THE

D:\GoogleDrive\SchoolDocs\College\Fall 2016\CS252\cesar_cypher\cesar.s

.global decrypt

decrypt:

```
stmfd sp!,{v1-v6, lr}
mov v1,a1 @copy pointer address , a1 will be overwritten
mov v2,a2 @copy what we move by, will be overwritten
bl strlen @get the length of a string into a1
add a1,a1,#1 @account for null byte
mov v4,a1 @move the stringlength to a1 for counting
bl malloc @allocate memory to make a new string
mov v5,#0 @need an iterator for adding to the string

loop:
ldrb v6,[v1],#1 @load in characters from argument string arg#
subs v6,v6,#65 @use A as the zero point for manipulation
bmi pushb @space or some other char that is less than A (0,65)
subs v6,v6,v2 @shift by the second argument given
bpl pushb
add v6,v6,#26 @went to far back, loop back to end of alphabet
```

```
pushb:
cmp v6,#26 @see if we went too far ahead
subge v6,v6,#26 @if we did then subtract a bit
add v6,#65 @add to get us back into the proper ascii space
strb v6,[a1,v5] @write out character
add v5,v5,#1 @increment position counter
subs v4,v4,#1 @decrement loop counter
bne loop @continue if loop counter isn't zero
ldmfd sp!,{v1-v6, pc}

.end
```

D:\GoogleDrive\SchoolDocs\College\Fall 2016\CS252\cesar_cypher\cesar.c

/* decrypt the string encrypted via revised Caesar shift */

#include <stdio.h>

extern char * decrypt(char * encrypt, int shift) ;

void main(int argc, char * argv[])

```
{
char * result ; /* pointer to decrypted string */
char encrypt[] = "QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD" ;
//char encrypt[] = "D";
int i = -3 ;
printf( "Original encrypted string:%s\n", encrypt ) ;
result = decrypt( encrypt,i ) ;
printf( "Decrypt with shift %d :%s\n", i, result ) ;
}
```