CRIPTOGRAFIA BASICA

1) Determinar cuál de los arreglos some1 o some2 es el mensaje cifrado o ciphertext.
2) Determinar cuál de los arreglos some1 o some2 es una cadena auxiliar y como se usa.
3) Obtener la password para decodificar el mensaje secreto.
4) Obtener el mensaje secreto o plaintext.
5) Decidir si el programa está completo o incompleto en algún sentido justificando.

Respuestas:

1) El arreglo some1 es el “ciphertext” o “mensaje cifrado”.

2) El arreglo some2 es una “cadena auxiliar” y sirve tanto para corroborar que la clave ingresada es correcta (función “b”) , como también para descifrar el ciphertext (función “d”).

3) Realicé la resta hexadecimal byte a byte: “some2 - X8 = KEY” para obtener la clave:

some2: 60 8e 8f 81 89 7e 82 7d 85 7a 84 55 7f 79 80 54 74 51 7f 85 7b 7e 78 4d 75 47 58 51 7c 43 53 4d
-
X8: 1f 1e 1d 1c 1b 1a 19 18 17 16 15 14 13 12 11 10 0f 0e 0d 0c 0b 0a 09 08 07 06 05 04 03 02 01 00
= ----------
KEY: 41 70 72 65 6e 64 69 65 6e 64 6f 41 6c 67 6f 44 65 43 72 79 70 74 6f 45 6e 41 53 4d 79 41 52 4d

Pasado a arreglo para incorporar al código y ser interpretado por el qemu:

0x6569646e65727041, 0x446f676c416f646e, 0x456f747079724365, 0x4d5241794d53416e

KEY: AprendiendoAlgoDeCryptoEnASMyARM

4) Mensaje secreto: YOU·WIN!MuyC3rcaDeAprob@rEst0!!!

5) Para mi el programa esta completo, en el sentido que cumple la función que se describe en un principio, ya que no es exactamente “OTP”, dado que el cifrado del mensaje no lo realiza el programa, y tampoco cumple la función de OTP de descifrado D(k⊕c) != k ⊕ c = m (siendo k “KEY”, c “ciphertext” y m some1 descifrado). El descifrado en el programa dado no lo hace utilizando la key, sino la cadena auxiliar some2. Pero como todo esto es aclarado previamente en la presentación de crypto, no veo porque decir que no esta completo de alguna forma. Ya que analizando el código y descubriendo la clave se puede descifrar el mensaje oculto, cumpliendo así el significado del nombre del algoritmo (decrypt = descifrar).