Tras seguir los pasos de un estafador, se secuestró una notebook que fue llevada al laboratorio forense para análisis. Entre los archivos de la computadora se encontró lo que parecería ser una lista de usuarios y contraseñas que uso el acusado para desarrollar sus tareas.

Contar con esa información podría permitir llegar al resto de la red delictiva, pero la misma se encuentra cifrada y el sospechoso se niega a revelar la clave.

Por suerte, los investigadores se dieron cuenta que el cifrado utilizado fue construido por el mismo sospechoso, así que suponiendo que no sería muy difícil quebrarlo, solicitan tu asistencia.

El pseudocódigo reconstruido analizando los ejecutables es el siguiente:

// Considerar los string como arreglos de caracteres ascii, x[i] es el i-esimo caracter

decrypt(key, file):

for each line in file:

c := base64\_dec(line)

k := key

p := ""

for i = 0 to length(c):

p[i] := (c[i] - k[i] - i) mod 256

k[length(k) + i] := p[i]

print(p) // linea descifrada

También se encontró en uno de los navegadores una credencial guardada que se sospecha puede estar en el archivo:

user: meltedgalloway

pass: wcS@D6d6

Se pide encontrar la clave con la que fue cifrado el archivo passfile.

Podes encontrar el adjunto en https://s3.amazonaws.com/it.challenge/level8