Procedimiento de cifrado y descifrado de archivos mediante GPG, sin interacción, protegiendo la llave mediante partición de secretos

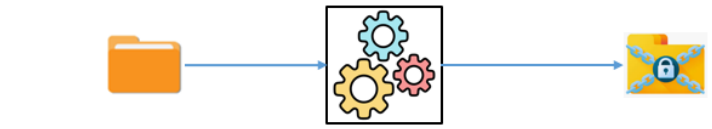
Necesidad:

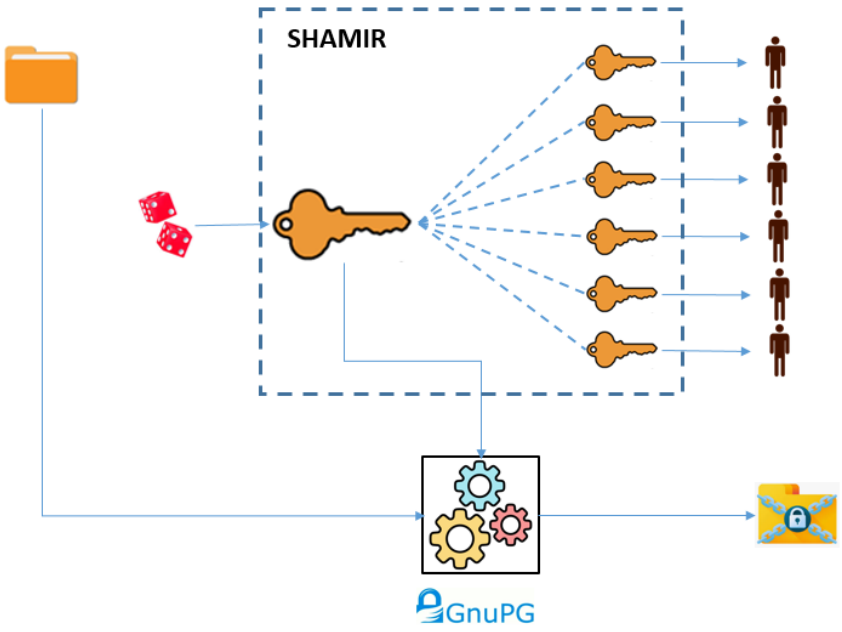
Realizar el cifrado de archivos mediante GPG usando esquema de cifrado simétrico pero en el que se requiere que la custodia de la llave no recaiga en una sola persona.

Propuesta:

Emplear el procedimiento de secreto compartido de Shamir (https://dev.to/francotel/como-compartir-un-secreto-desglosando-el-metodo-de-adi-shamir-para-la-seguridad-de-datos-4fbg) en el que el secreto original se "partirá" en "n" componentes, requiriendo una cantidad n-1 para la reconstrucción del secreto original.

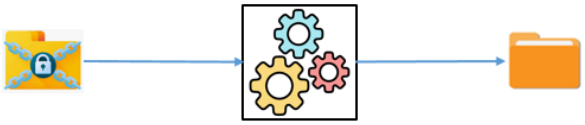
Mediante el script se generará en primera instancia la llave original de manera aleatoria, posteriormente se "partirá" en 6 componentes (ejemplo del script), posteriormente el archivo se cifra y se borra el original.

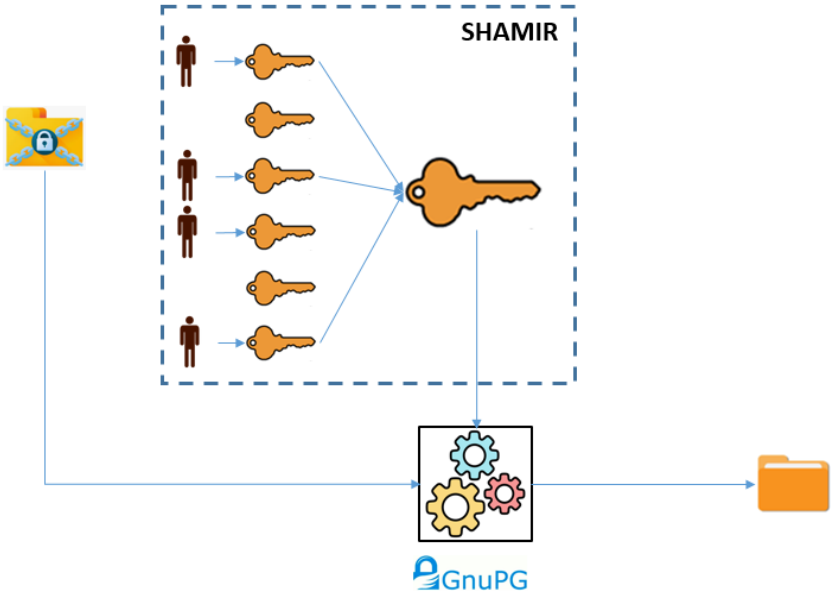




Procedimiento de cifrado y descifrado de archivos mediante GPG, sin interacción, protegiendo la llave mediante partición de secretos

En el proceso de descifrado, se requiere introducir "mínimo" el número de componentes configurado (4 para el ejemplo) con lo que se regenera la llave original y se realiza el proceso de descifrado.





Script para cifrado

Su uso será: #<script.sh> <archivo a cifrar con todo y extensión>

```
#!/bin/bash
clear
echo
echo "Generacion de llave aleatoria"
echo
uno=`date +%N`
dos=`date +%s`
tres=`echo $(($RANDOM))`
cuatro=$uno$dos$tres
cinco=`echo $cuatro | sha256sum | awk '{print $1}'`
sleep 4
echo "Termino de generarse la llave aleatoria"
echo
echo "La llave aleatoria es"
echo
```

```
echo $cinco
echo
echo "Split en 6 partes de esta llave aleatoria"
echo
seis=`echo $cinco | ssss-split -t 4 -n 6 -q -w Token`
#echo $cinco > llave.txt

i=0
for share in $seis; do
   echo "$share" > secretos/"$(basename "Secretos")-share-$i.txt"
   cat secretos/$(basename "Secretos")-share-$i.txt >> llaves.txt
   i=$((i+1))
done
echo
sleep 4
echo "Proceso de Split terminado"
echo
echo "Inicia proceso de cifrado"
echo

echo -n "$cinco" | gpg \
  --batch --yes \
  --armor --cipher-algo AES256 \
  --pinentry-mode loopback \
  --passphrase-fd 0 \
  --symmetric "$1"

Echo
rm $1
sleep 4
echo "Proceso de cifrado terminado"
```

Procedimiento de cifrado y descifrado de archivos mediante GPG, sin interacción, protegiendo la llave mediante partición de secretos

Script para descifrado

Su uso será: #<script.sh> <archivo a cifrar con todo y extensión>

```
#!/bin/bash
clear

#Nombre sin extension
nombre=$1
nombre2=${nombre%.*}


echo "Etapa de regeneración de llave..."
echo
echo "Solicitud de partes..."
echo
script -c 'ssss-combine -t 4 -Q' llave-regenerada.txt
llave=`cat llave-regenerada.txt | grep -v \- | grep -v WARNING | grep -v Script | tr -d '[[:space:]]'`
echo
echo "Llave regenerada"
#echo "La llave es:"
#echo $llave
echo
echo "Ahora inicia proceso de recuperación de secreto"
echo
#echo "Copiar y pegar la llave generada y dar Enter"
echo

gpg \
  --batch \
  --yes \
  --pinentry-mode loopback \
  --passphrase "$llave" \
  --output "$nombre2" \
  --decrypt "$1"


rm llave-regenerada.txt
rm $1
echo "El secreto ha sido recuperado"
```