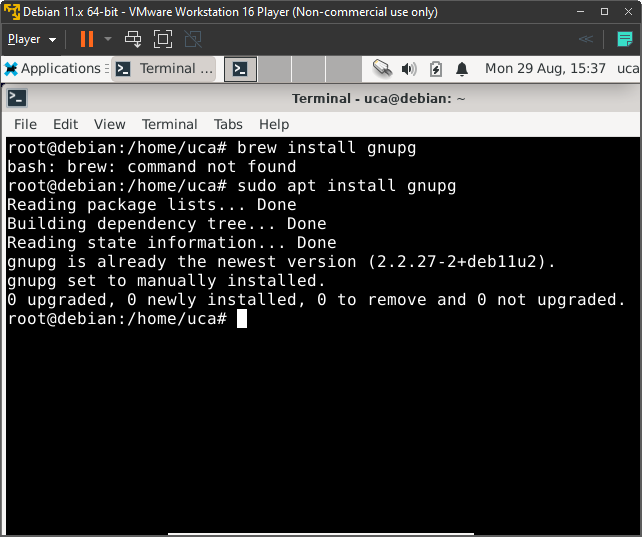
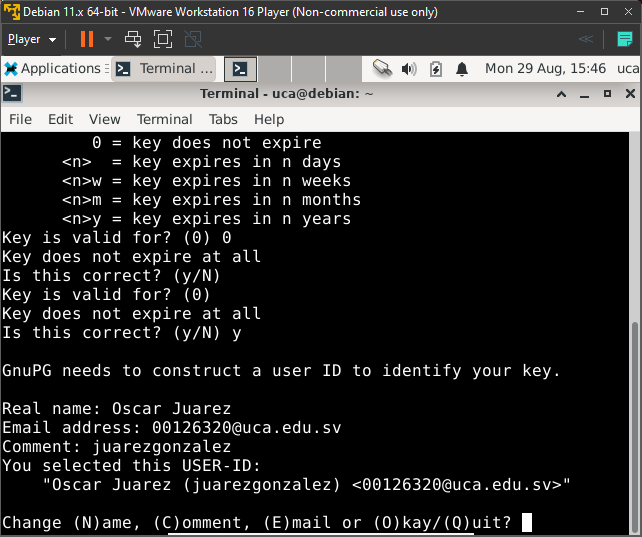
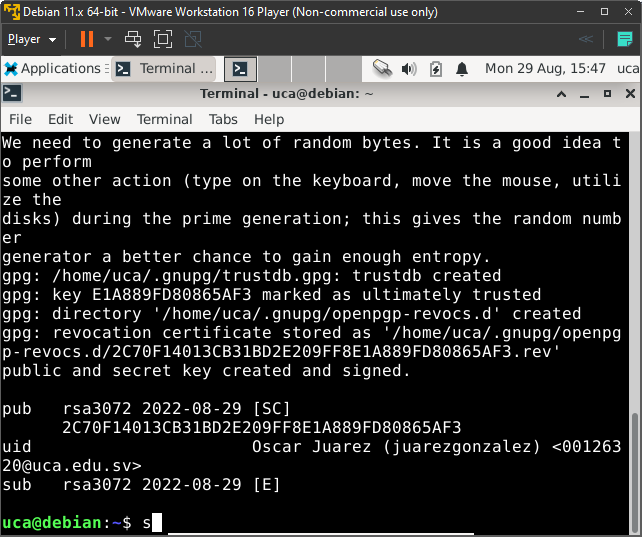
# Instalando GPG



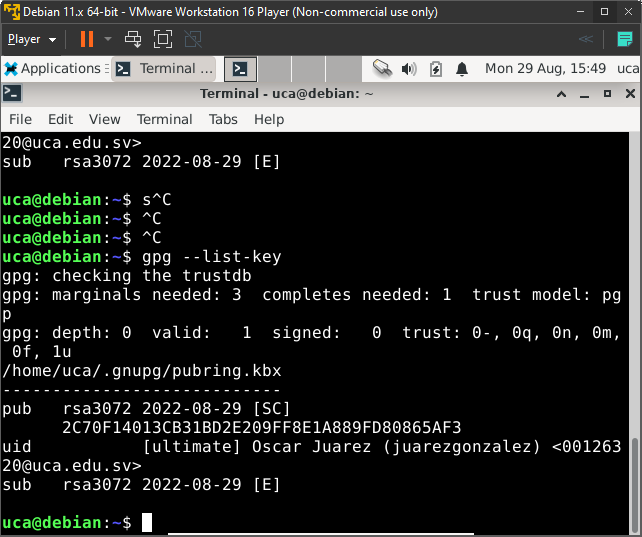
# Generar clave gpg --full-generate-key

# 

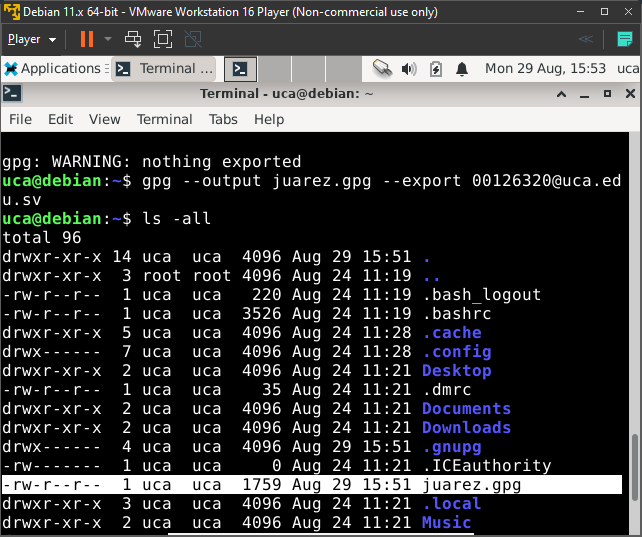




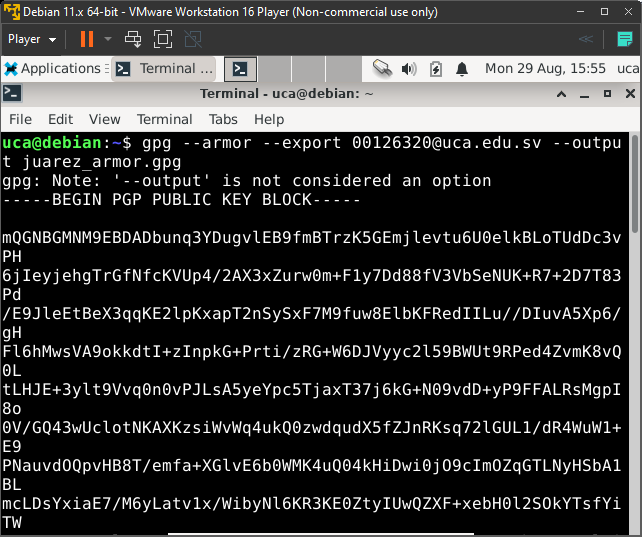
# USANDO GPG -KEY-LIST



# Exportando las claves a binario con gpg --output juarez.gpg --export 00126320@uca.edu.sv



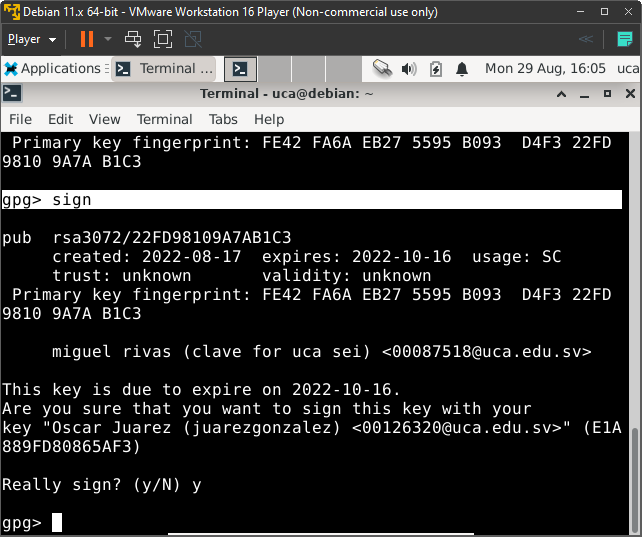
# Usando gpg --armor --export [00126320@uca.edu.sv](mailto:naldana@uca.edu.sv) para exportar la clave publica

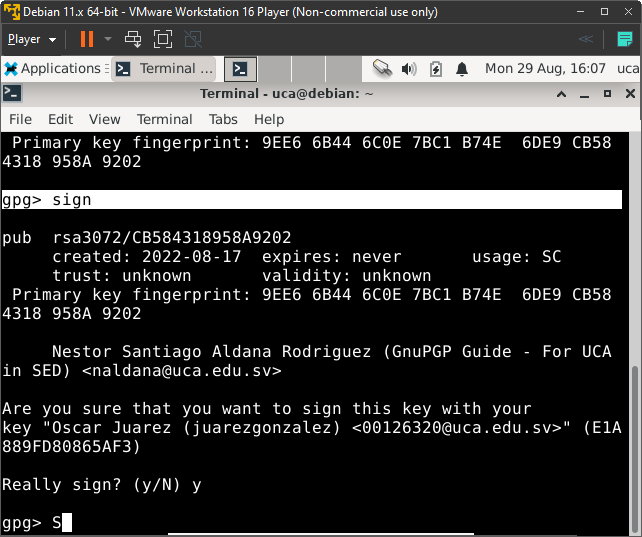


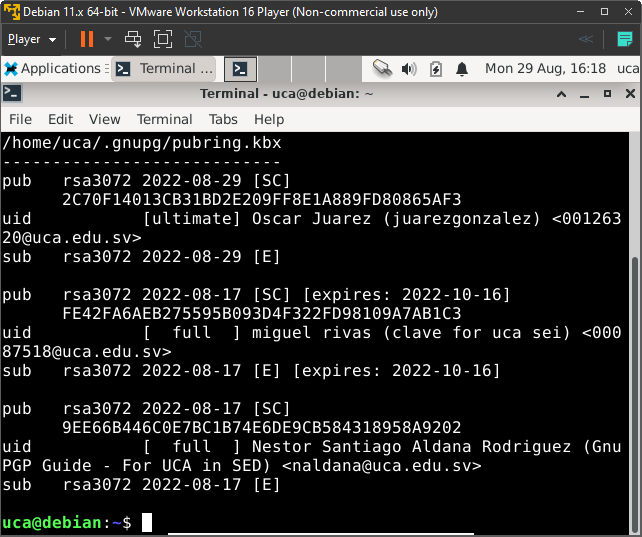
# Exportando mi llave privada

# Importando llave publica Miguel y Nestor

# Firmando llaves importadas

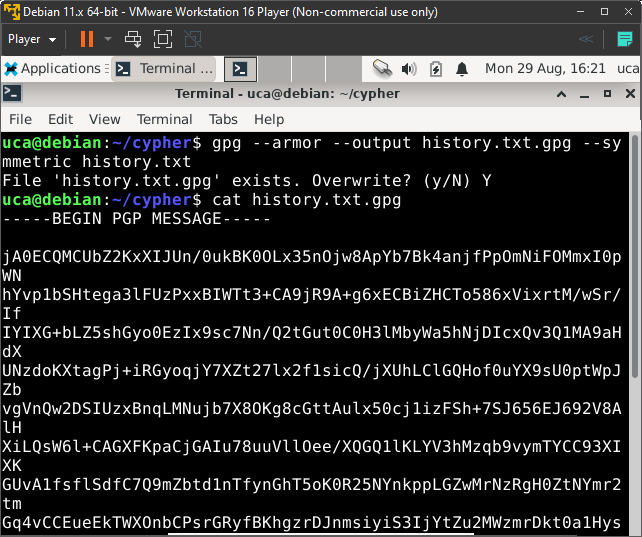




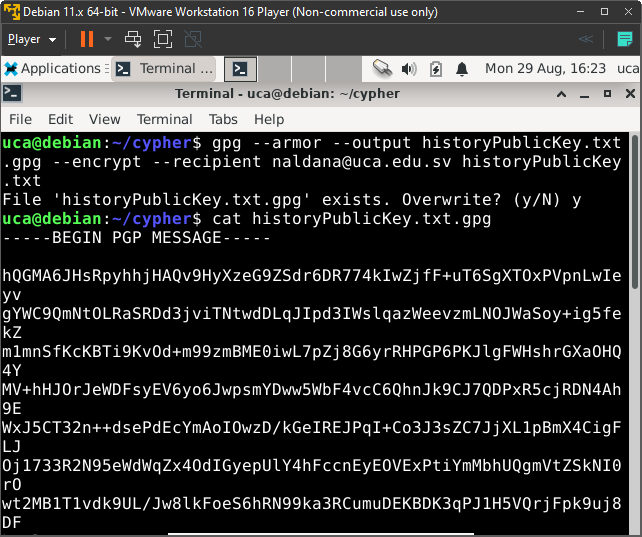


# Cifrado simétrico

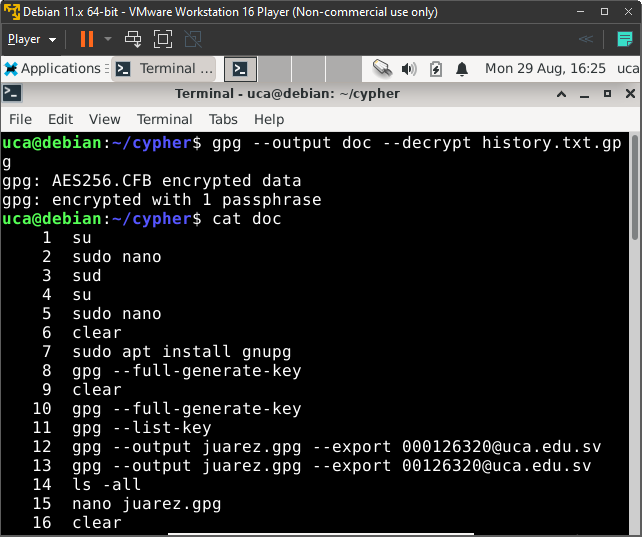
# 



# Cifrado asimétrico



# Descifrado mensaje con cifrado simétrico



# ¿Cuál es el punto más débil de PGP?

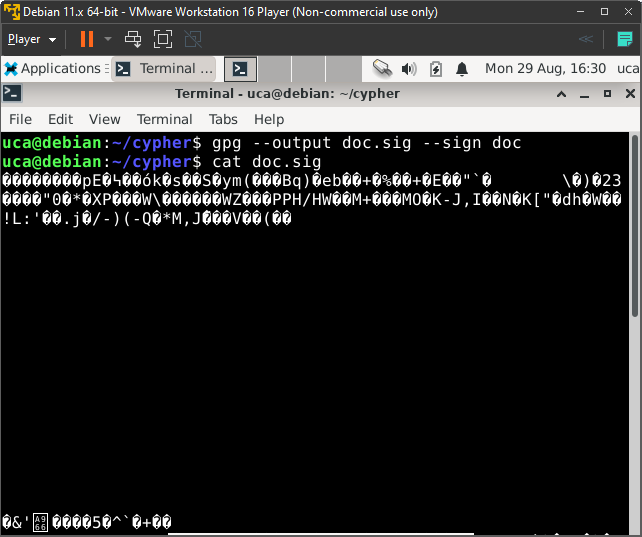
Compartir las claves entre personas

# ¿Cuándo es conveniente utilizar solamente cifrado simétrico?

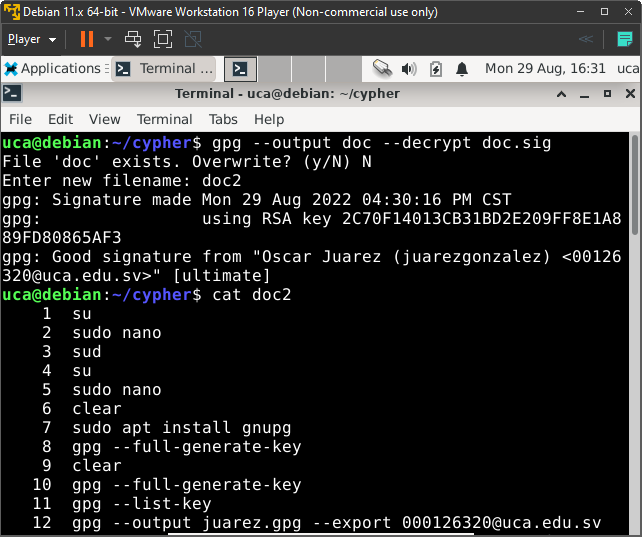
Es necesario una unica llave, puede ser muy eficaz porque no experimenta ningún retraso de tiempo significativo como resultado del cifrado y descifrado.

# Firmando documento

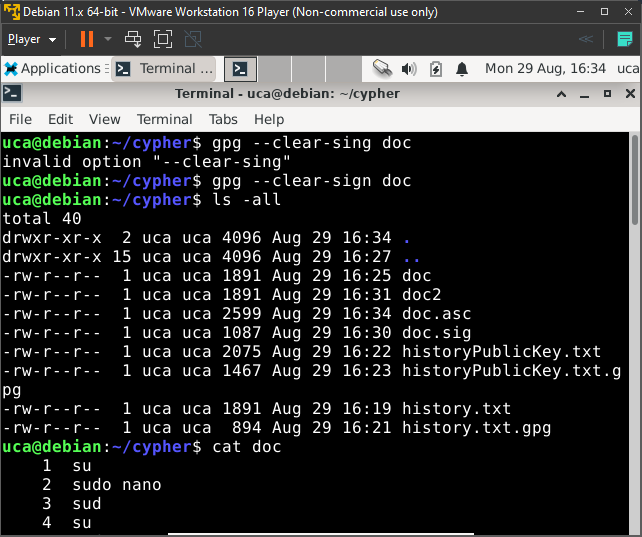
# Firmando documento



# Descifrado documento firmado



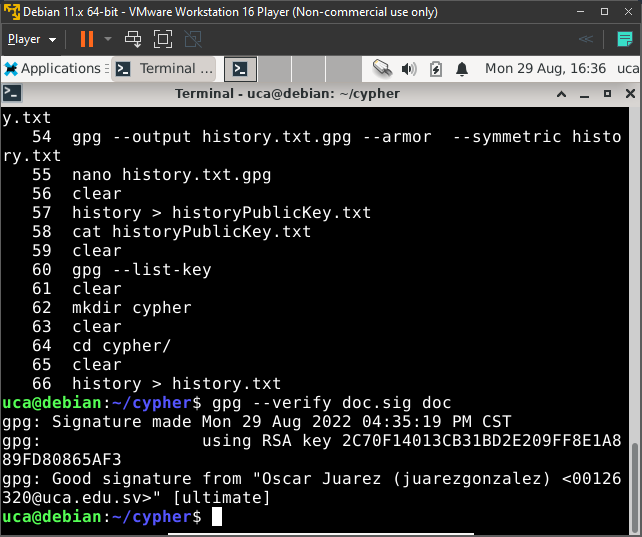
# Quitando la firma al documento



# Usando firmas desacopladas

# 

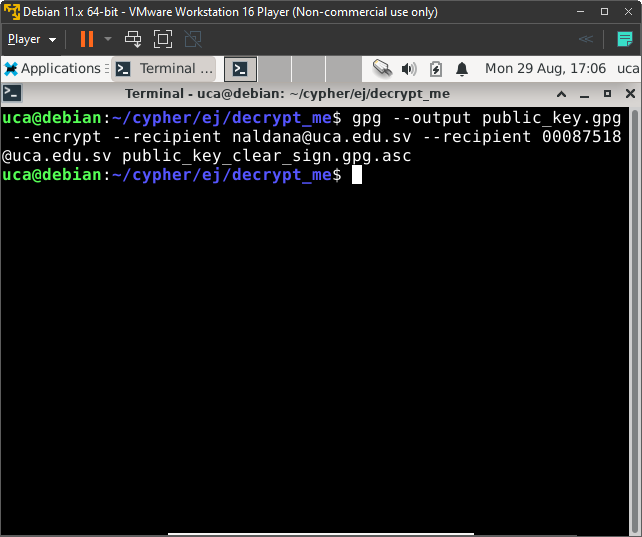
# Verificando firmas desacopladas

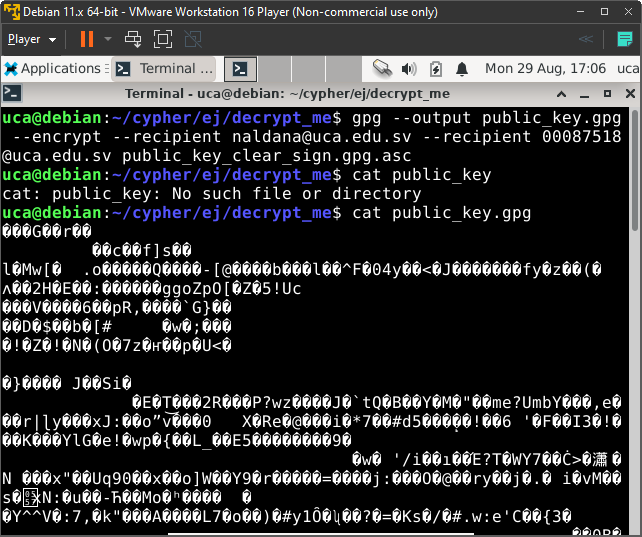


# EJERCICIO

1. Sí lo hice pero no tomé capturas, son 6 documentos con el mismo nombre public\_key\_XXXX

# Encriptando con recipientes Miguel Y Nestor.





# Agregando a git y haciendo commit

