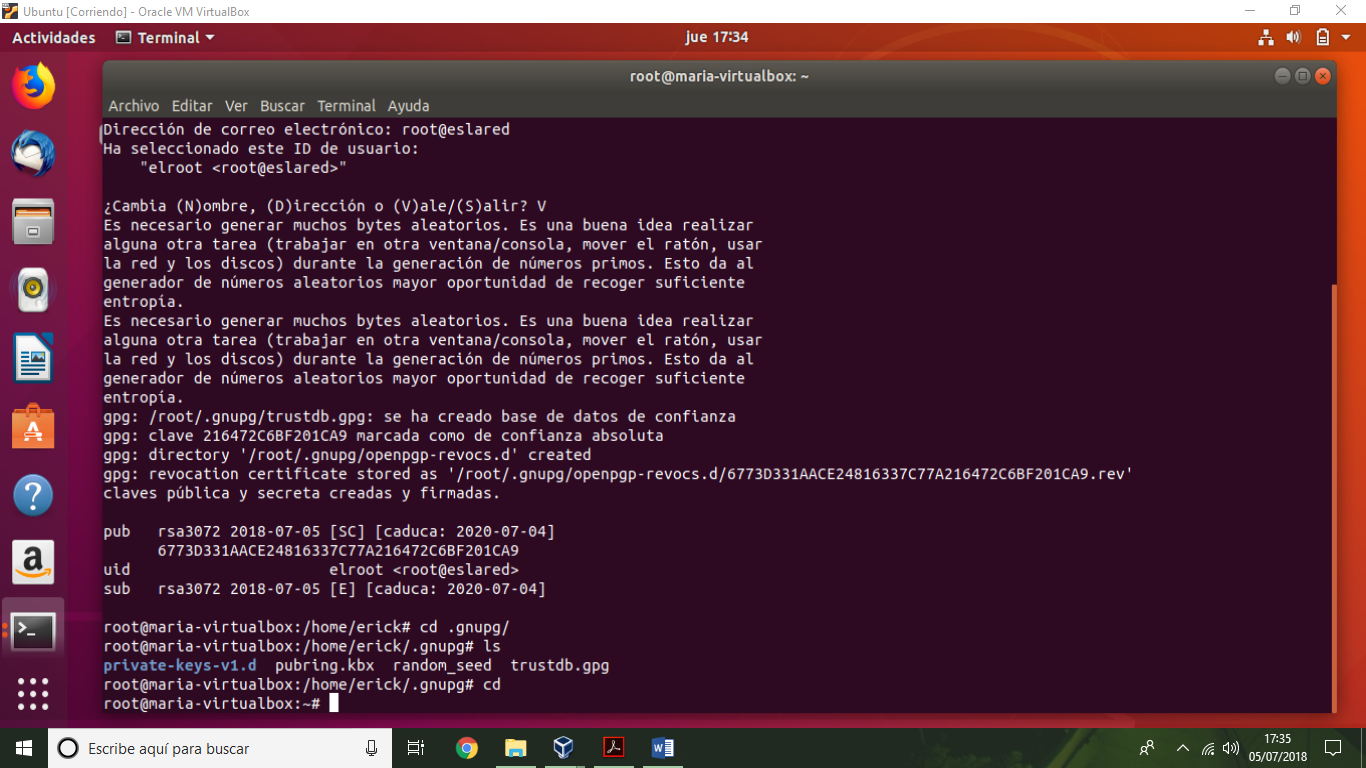
***Laboratorio 2***

***Cedeño, María 2-737-2336***

*PRIMERA PARTE*

1. **Se crean las claves *Privadas y Públicas***





1. **Se verifica la ruta de las claves que se crearon**

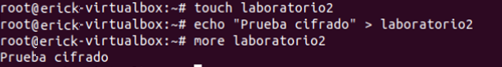




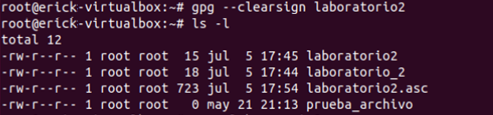
1. **Se vuelve al directorio anterior**



1. **Creación del archivo root con frase añadida**



1. **Se le asigna una firma al archivo root que se creó**

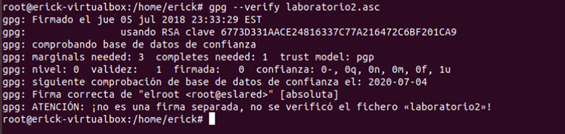




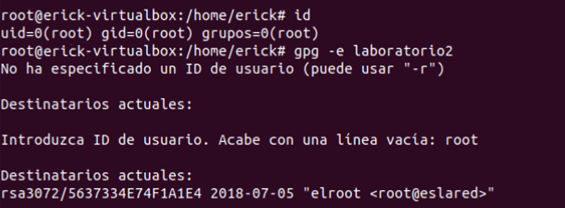
1. **Modificación del archivo firmado**



1. **Verificar la firma del archivo que contiene el mensaje**



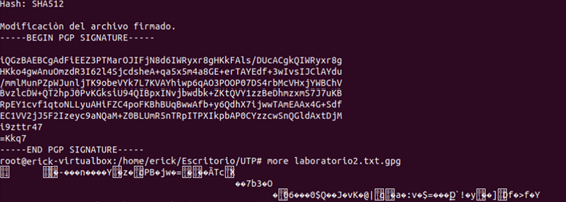
1. **Se obtiene la información del archivo firmado. Datos comprobados y obteniendo la clave RSA**
2. **Se cifra el archivo root que se creó**



1. **Se muestra el contenido del archivo que se cifro en el paso anterior**

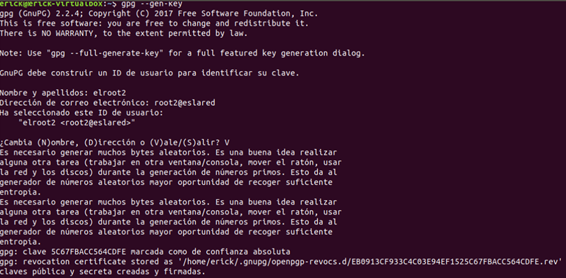


1. **Se firma el archivo cifrado que se obtuvo en el paso anterior y se muestra el contenido del mismo**



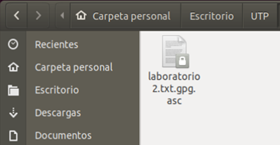
*SEGUNDA PARTE*

1. **Se crean las llaves para el usuario del ubuntu**

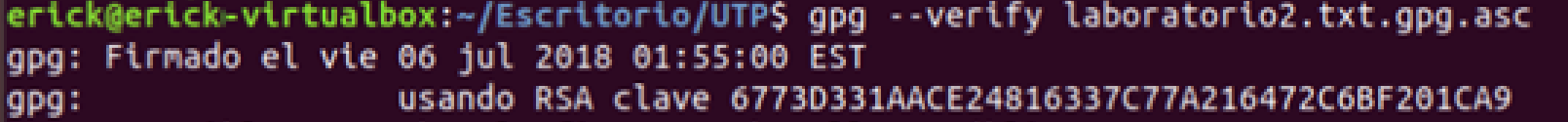


*TERCERA PARTE*

1. **Se copia hacia el subdirectorio personal del usuario Ubuntu el archivo cifrado y firmado que creó en la primera parte**



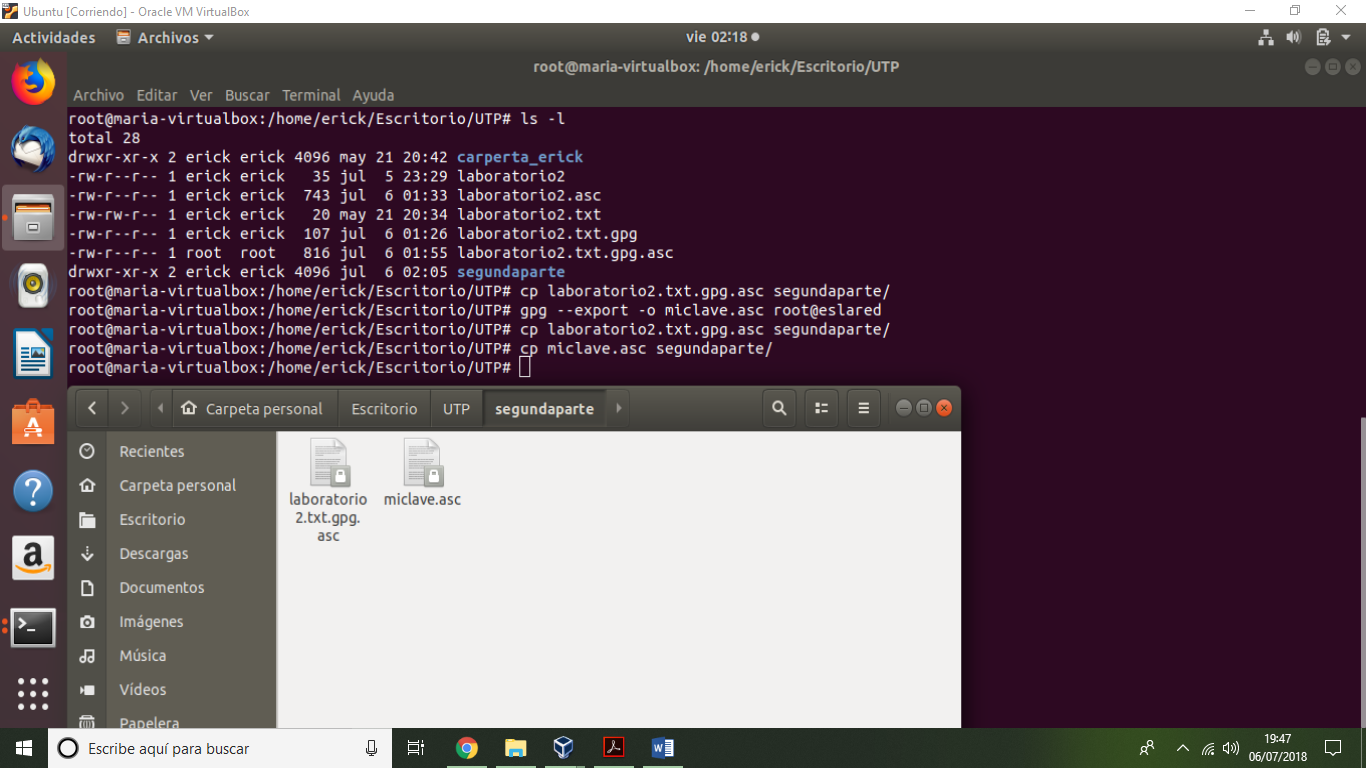
1. **Se verifica nuevamente la firma del archivo copiado.**



1. **Se exportan las llaves públicas del llavero.**

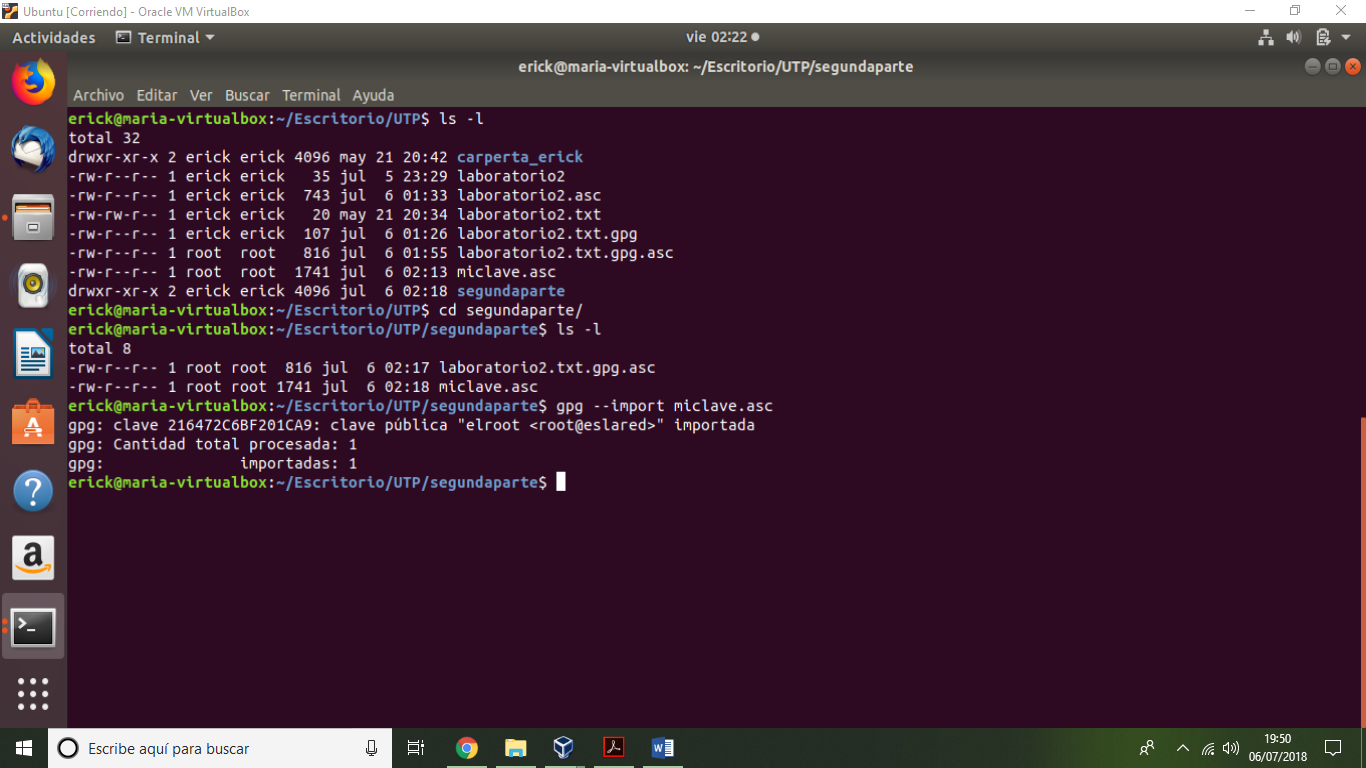


* **Se copia las llaves públicas de su llavero.**

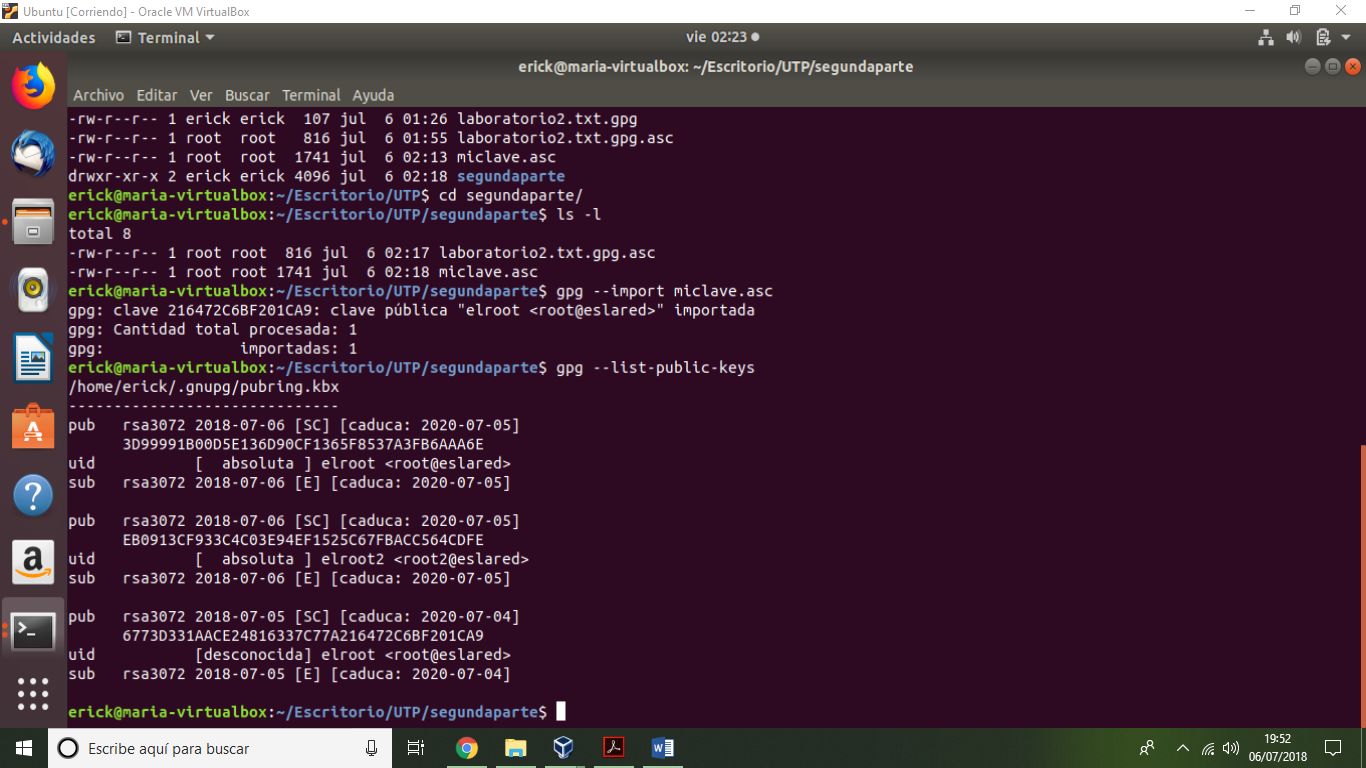


***CUARTA PARTE***

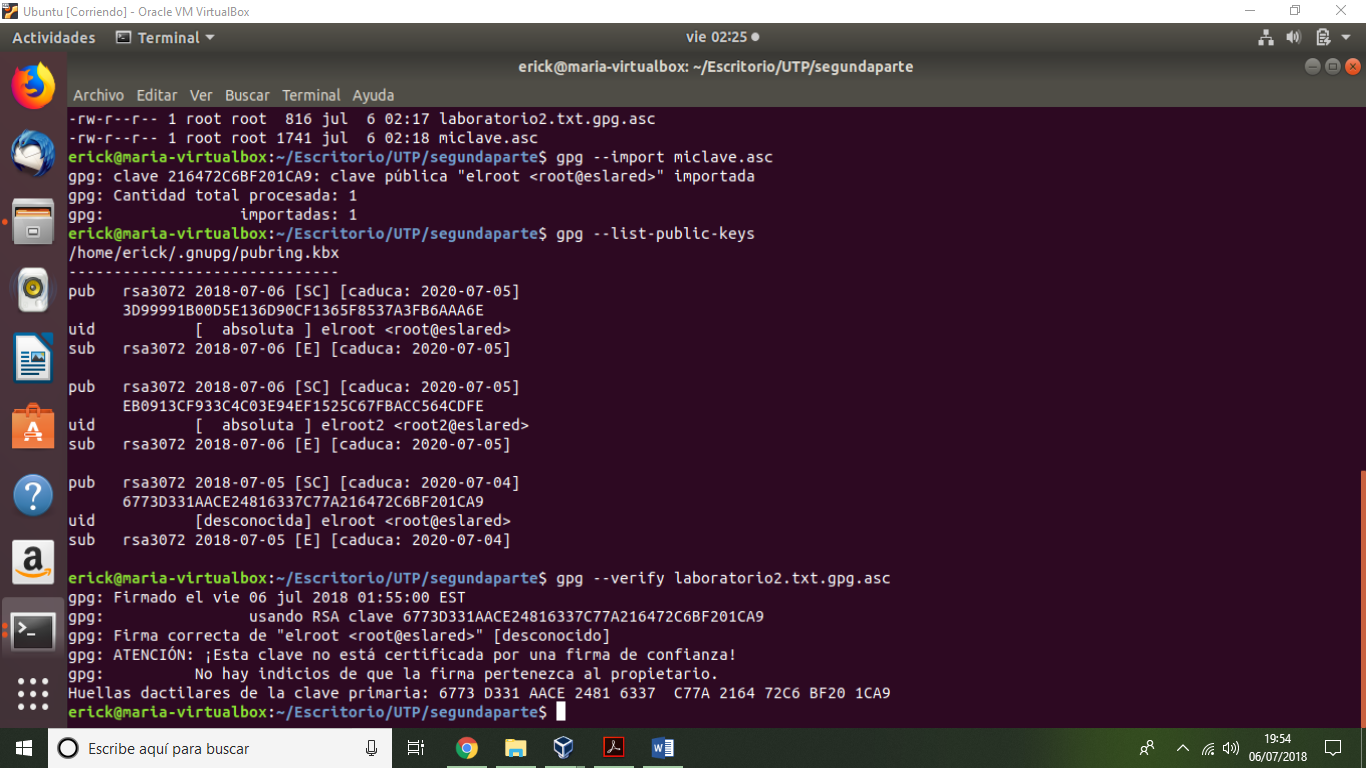
1. **Se importa las llaves públicas del usuario root hacia el llavero del usuario ubuntu.**



1. **Se lista el contenido del llavero del usuario**

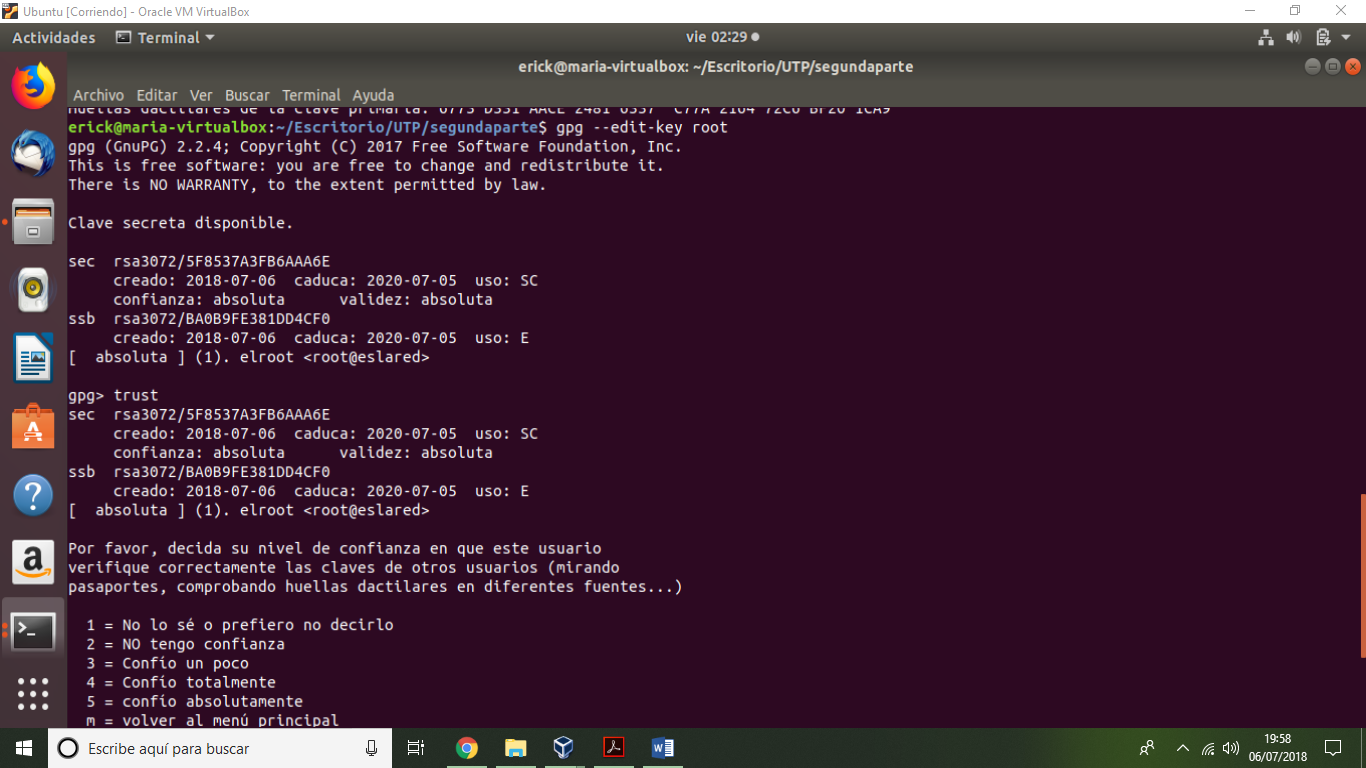


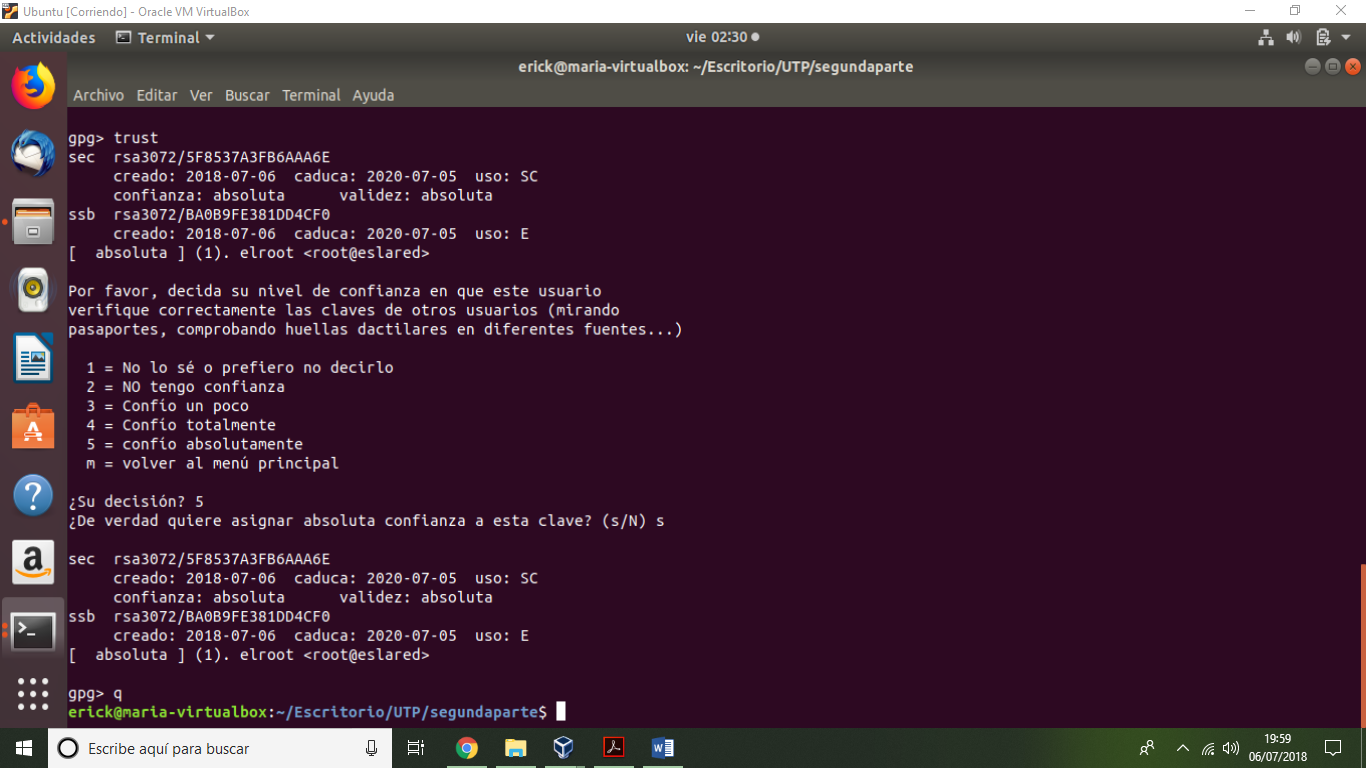
1. **Se verifica la firma del archivo**



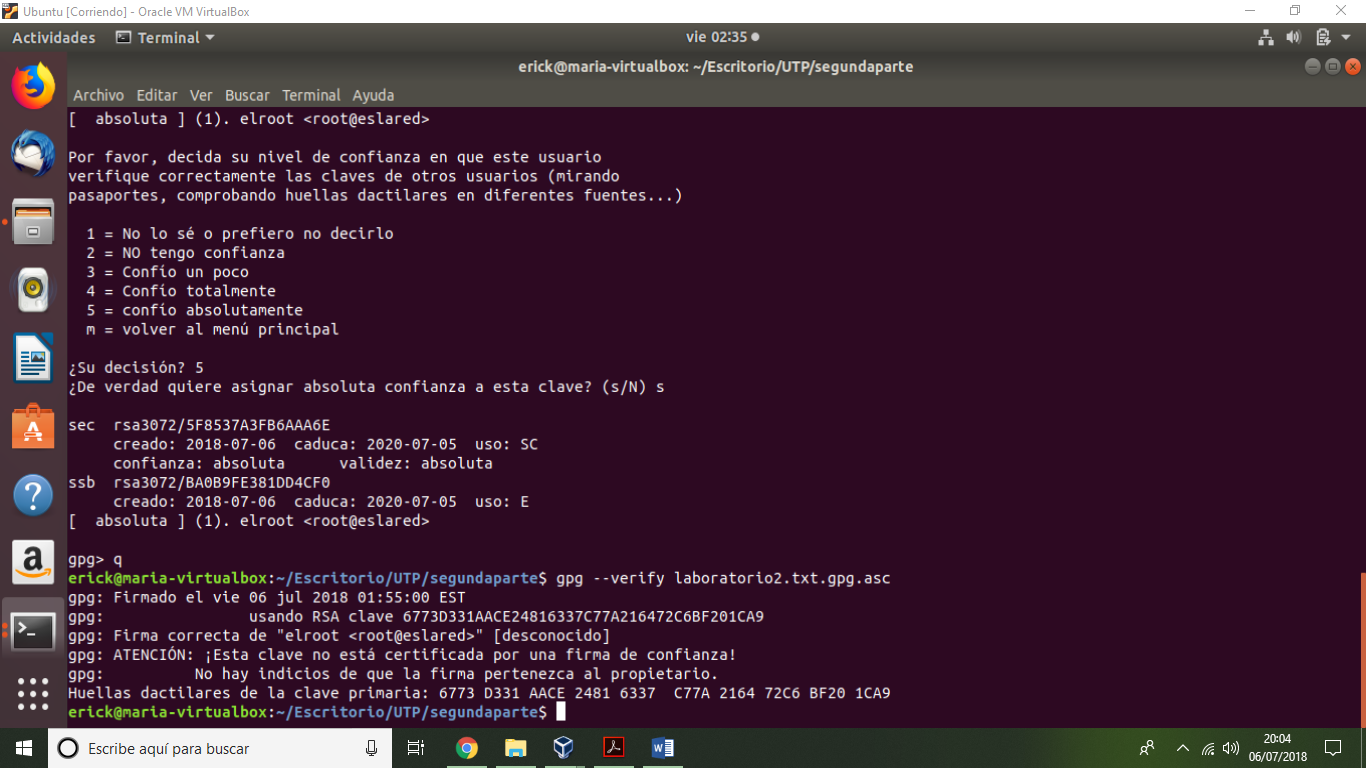
PUNTO 5

1. **Se Cambia el nivel de confianza de la clave del usuario root dentro del llavero del usuario Ubuntu**





PUNTO 6



*QUINTA PARTE*



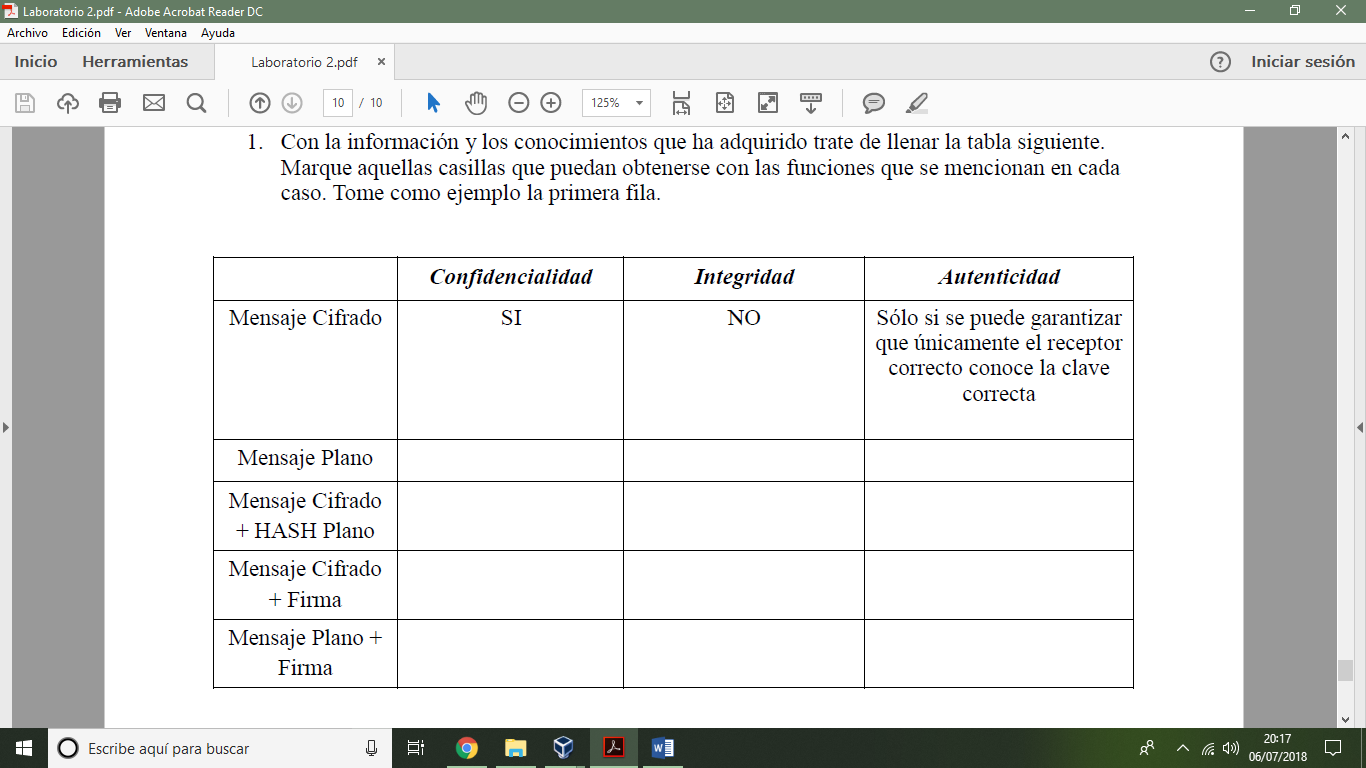
PUNTO 2

Para cifrar un mensaje cuyo destino sea otro usuario utilice el comando

* $ gpg -e **nombredelarchivo**

*ULTIMA PARTE*

1. Con la información y los conocimientos que ha adquirido trate de llenar la tabla siguiente. Marque aquellas casillas que puedan obtenerse con las funciones que se mencionan en cada caso. Tome como ejemplo la primera fila.



Solo si tiene la clave correcta

Únicamente el receptor puede verlo si tiene la clave

Únicamente el receptor puede verlo si tiene la clave correcta

Cualquiera persona puede ver el mensaje

Si

Si

Si

No

No

Si

Si

Si

2. Su respuesta sería la misma si nos refiriésemos solo a criptografía de clave simétrica? ¿Por qué?

Sí, porque solo se puede ver si se tiene la clave para obtener el mensaje original que se encripto.