



Instituto Politécnico Nacional



Unidad Profesional Interdisciplinaria en Ingeniería y
Tecnologías Avanzadas

Seguridad de Redes

Profesor. Polanco Montelongo Francisco Antonio

Alumno: Hernández Guzmán Bryan Alexis

Grupo: 3TV4

Práctica: Cifrado y Descifrado con RC4

Introducción:

RC4 es un esquema de cifrado de flujo (no basado en bloques) simétrico.

Fue diseñado por Ron Rivest (la R de RSA) en 1987. Originalmente era secreto, pero se filtró en 1994 a través de una lista de correo.

Es un esquema de cifrado extremadamente simple y puede implementarse en software de forma muy eficiente. Esto lo ha convertido en uno de los esquemas de cifrado más utilizados del mundo.

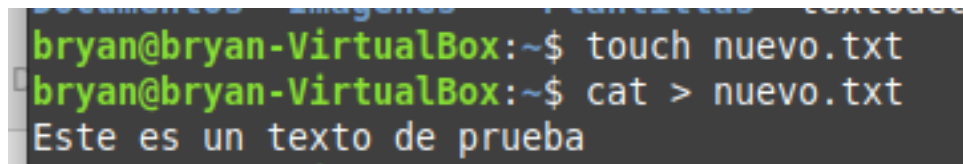
Sin embargo, RC4 hace tiempo que no es considerado un algoritmo seguro. RC4 es conocido por ser el mismo esquema de cifrado usado por WEP (Wired Equivalent Privacy), sistema criptográfico totalmente roto hoy en día.

Menos conocido es que RC4 es usado aún en aproximadamente la mitad de las transmisiones TLS que ocurren en el mundo actualmente, desde para consultar tu correo hasta para establecer transferencias bancarias.

Hoy en día el interés por el RC4 parte de querer conocer hasta qué punto está roto y cómo de vulnerables son los sistemas que lo utilizan.

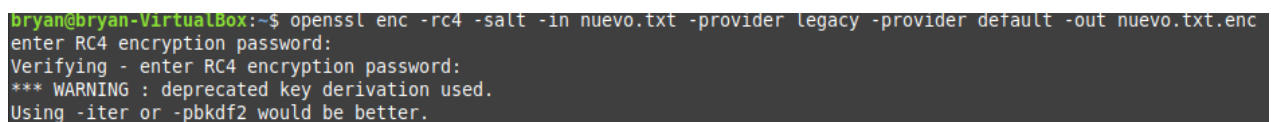
Elaboración:

Primeramente, creamos un archivo .txt y escribimos un texto:



```
bryan@bryan-VirtualBox:~$ touch nuevo.txt
bryan@bryan-VirtualBox:~$ cat > nuevo.txt
Este es un texto de prueba
```

Procedemos a cifrar nuestro archivo con RC4, nos pedirá una contraseña para poder descifrarlo más adelante:



```
bryan@bryan-VirtualBox:~$ openssl enc -rc4 -salt -in nuevo.txt -provider legacy -provider default -out nuevo.txt.enc
enter RC4 encryption password:
Verifying - enter RC4 encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

Procedemos a visualizar su contenido:

```
bryan@bryan-VirtualBox:~$ cat nuevo.txt.enc
Salted 0#%00T00$0
q?0F6"fvr0:02)0S00M0bryan@bryan-VirtualBox:~$ ls
Descargas  Imágenes  nuevo.txt.enc  textodecod.txt  Vídeos
Documentos Música    Plantillas    texto.txt        Warpinator
Escritorio nuevo.txt  Público       texto.txt.enc
```

Como se puede observar, no podemos visualizar su contenido, así que procederemos a descifrarlo:

```
bryan@bryan-VirtualBox:~$ openssl enc -rc4 -d -in nuevo.txt.enc -provider legacy -provider default -out nuevodecod.txt
enter RC4 decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bryan@bryan-VirtualBox:~$ cat nuevodecod.txt
```

Procederemos a visualizar nuevamente su contenido para comprobar si está correcto

```
bryan@bryan-VirtualBox:~$ cat nuevodecod.txt
Este es un texto de prueba
bryan@bryan-VirtualBox:~$
```

Conclusiones:

Dentro de mis observaciones puedo entender el por qué el cifrado es muy útil actualmente, sin embargo, se puede observar que actualmente no es muy seguro, pero como método de aprendizaje es muy bueno, dentro de las complicaciones que pude encontrar fueron unas librerías que no estaban dentro de mi maquina virtual, para esta práctica se utilizó Linux mint, sin embargo pude realizarla en otro sistema operativo de otra distribución y fue más fácil de llegar al resultado final.

Referencias:

https://ntrrgc.me/attachments/Cifrado_RC4/#:~:text=RC4%20es%20un%20esquema%20de,software%20de%20forma%20muy%20eficiente.