EJERCICIOS CRIPTOGRAFÍA

Prerrequisitos

Busca información sobre el paquete hash-identifier en Kali y comprueba si lo tienes instalado. En caso que no lo esté, instálalo.

Crea un fichero de texto llamado "ejercicio\_crypto.txt" en la ruta $HOME/Crypto con este texto:

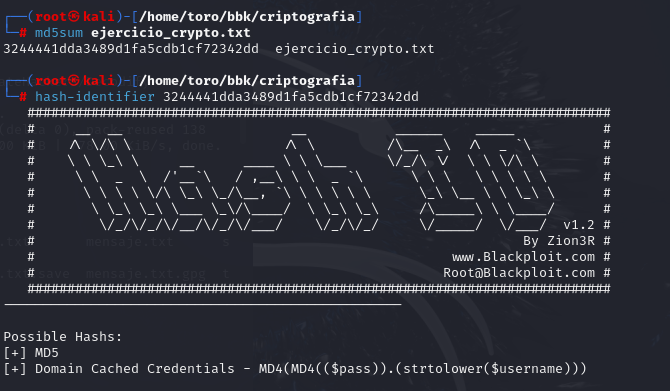
b2pvIGltcG9ydGFudGUgcXVlIGNvZGlmaWNhciBubyBlcyBsbyBtaXNtbyBxdWUgY2lmcmFy



Ejercicios - Funciones hash

1.Crea un hash MD5 del fichero ejercicio\_crypto.txt.

2.Comprueba con hash-identifier el resultado con el hash obtenido. ¿Acierta en la predicción del tipo de hash? SI!



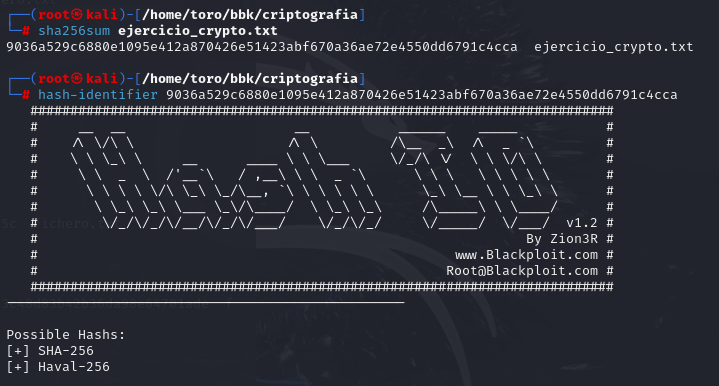
3.Crea un hash SHA-1 del fichero ejercicio\_crypto.txt.

4.Comprueba con hash-identifier el resultado con el hash obtenido. ¿Acierta en la predicción del tipo de hash? SI!



5.Crea un hash SHA-256 del fichero ejercicio\_crypto.txt.

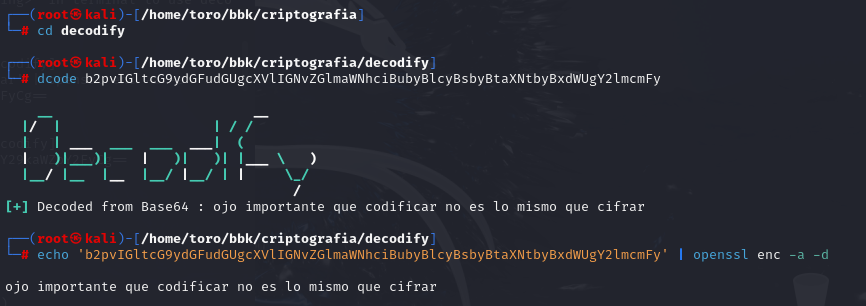
6.Comprueba con hash-identifier el resultado con el hash obtenido. ¿Acierta en la predicción del tipo de hash? SI!



Ejercicios - Codificación

7.Comprueba la cadena de texto que contiene el fichero. ¿Qué formato es? Base64!

Utiliza la herramienta Decodify para identificarla y una vez identificada intenta decodificarla utilizando openssl.

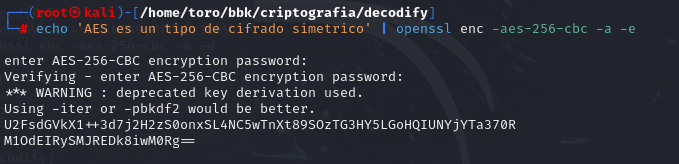


8.Codifica el texto "No metemos gente en criptas" en el mismo formato usando openssl.

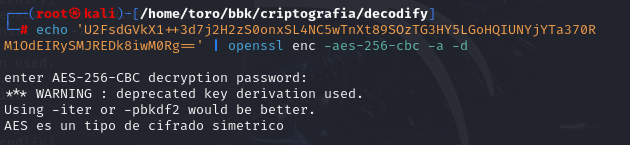


Ejercicios - Cifrado simétrico

9.Cifra el texto "AES es un tipo de cifrado simetrico" con AES-256 Cipher (aes-256-cbc) y con password "AES".

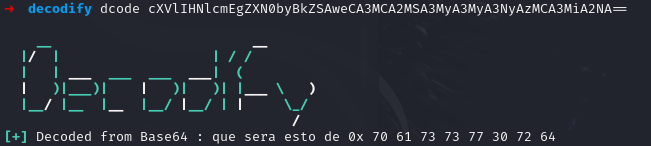


10.Descifra el resultado del ejercicio anterior con su password para recuperar el contenido.



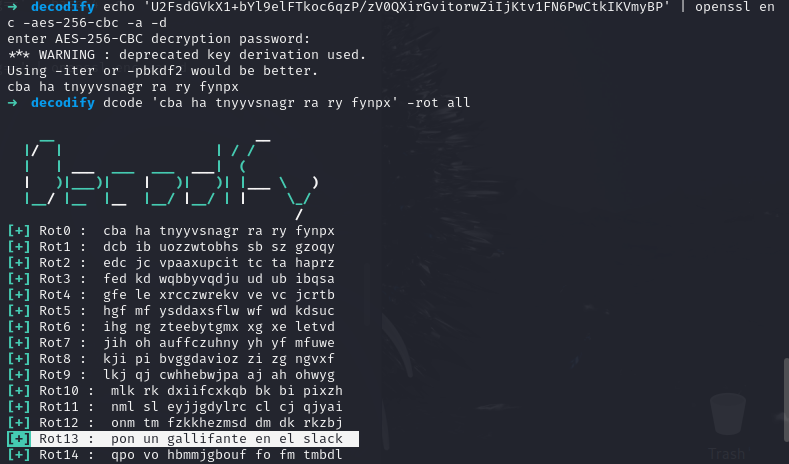
11.Descifra la cadena de texto indicada con la clave oculta AES 256 siguiente:

Clave oculta: cXVlIHNlcmEgZXN0byBkZSAweCA3MCA2MSA3MyA3MyA3NyAzMCA3MiA2NA==



70 - 61 - 73 - 73 - 77 - 30 - 72 – 64 = p – a – s – s – w – 0 – r – d

Cadena de texto: U2FsdGVkX1+bYl9elFTkoc6qzP/zV0QXirGvitorwZiIjKtv1FN6PwCtkIKVmyBP



(Opcional) Ejercicios - Cifrado asimétrico

12.Genera una clave privada RSA 2048 y guardala en un fichero privada.pem usando openssl.



13.Genera una clave pública (publica.pem) desde la clave privada anterior usando openssl.



14.Cifra el archivo "ejercicio\_crypto.txt" usando la clave PRIVADA RSA 2048 y guardalo como prueba.rsa



15.Descifra el archivo prueba.rsa usando la clave PRIVADA RSA 2048 y comprueba el contenido.

