Universidad de Alcalá

Kevin van Liebergen Ávila

Práctica 2
Explotación de la herramienta JCrypTool (iii)

Máster en ciberseguridad

Asignatura: Criptografía aplicada

2020

Mediante el uso de la herramienta JCrypTool, se pretende que el alumno utilice las posibilidades del cifrador de bloque AES, tales como

- cifrado y descifrado
- diversos tamaños de clave
- diversos modos de relleno
- claves manuales o generadas automáticamente

1 Introducción

Para desarrollar la práctica, podemos seguir aproximadamente este guión. En primer lugar arrancamos la herramienta en las máquinas del laboratorio, después de presentarnos, tecleando dentro de un Terminal:

```
/usr/local/jcryptool/JCrypTool &
```

A continuación pasamos a desarrollar los distintos apartados propuestos.

2 AES

2.1 Abrir un fichero vacío con Text editor. Escribir algún texto sobre el que vayamos a trabajar.

El texto sobre el que vamos a trabajar aparece en la imagen 1.

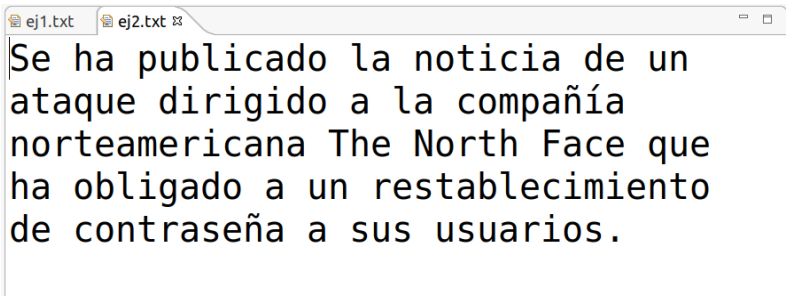

Figure 1: Texto sobre el que trabajaremos

2.2 Seleccionar la vista Default y, dentro de la ventana Crypto Explorer, la pestaña `Algorithms`.

Una vez se ha realizado lo ordenado, la ventana *Crypto Explorer* debe aparecer como en la imagen 2.

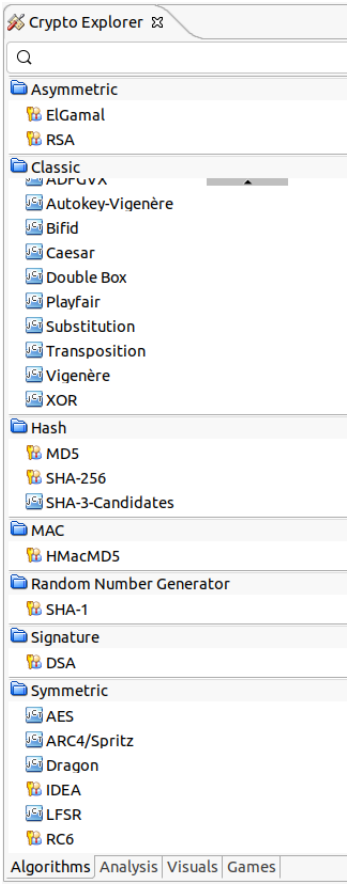

Figure 2: Ventana *Crypto Explorer*

2.3 Crear una identidad nueva y su clave simétrica asociada:

a) Seleccionar en la barra de menú la opción Algorithms → Keystore.

Desde la barra de menú nos aparece un desplegable en **Algorithms** donde se puede seleccionar la opción `Keystore`

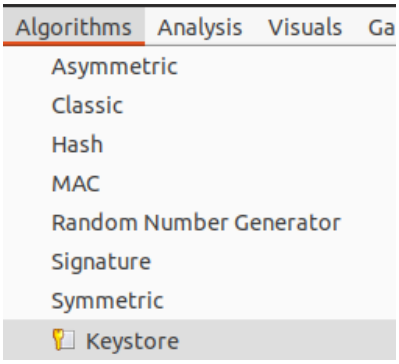

Figure 3: Keystore

b) Crear una identidad nueva, pulsando con el botón derecho sobre la ventana Keystore.

Cuando pulsamos con el click derecho nos aparece una pestaña como la de la figura 4 y cuando pulsamos sobre `New Contact` nos aparece una pestaña como la de la imagen 5 en el que especificaremos un nombre.

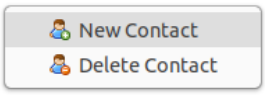

Figure 4: Click derecho

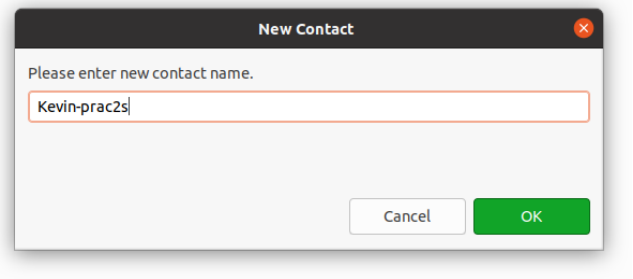

Figure 5: Nombre del nuevo contacto

c) Crear para esa identidad una nueva clave simétrica, seleccionando el icono de una sola llave situado a la derecha de la barra de menú de la ventana Keystore. Elegiremos la clave de tipo AES con el tamaño deseado. Observemos que se ha de proteger mediante una contraseña.

Pulsando en el icono de una sola llave a la derecha del todo donde se lee `New Secret Key` (figura 4) aparece una nueva pestaña (imagen 7) donde podemos elegir el tipo de algoritmo, la longitud de la clave y la contraseña que protege la clave.

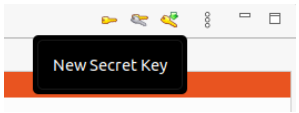

Figure 6: New Secret Key

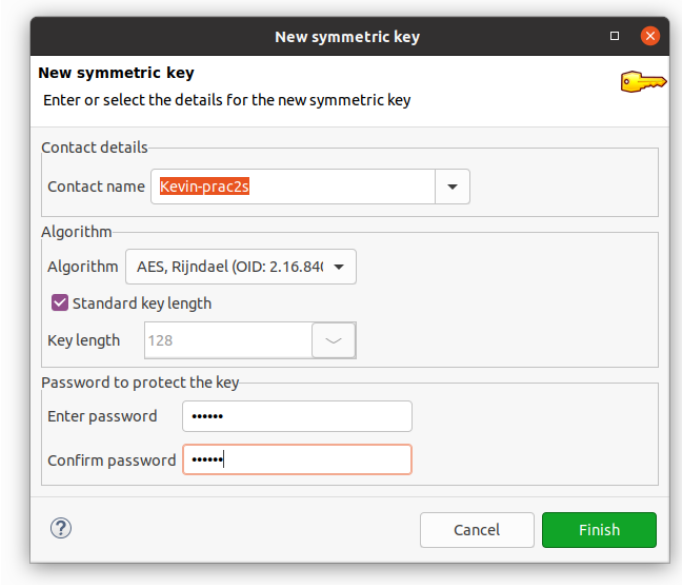

Figure 7: New Symmetric Key

2.4 En la ventana Crypto Explorer, seleccionar Symmetric → AES.

Seleccionando donde se ha indicado nos debe aparecer una pestaña como la de la figura 8.

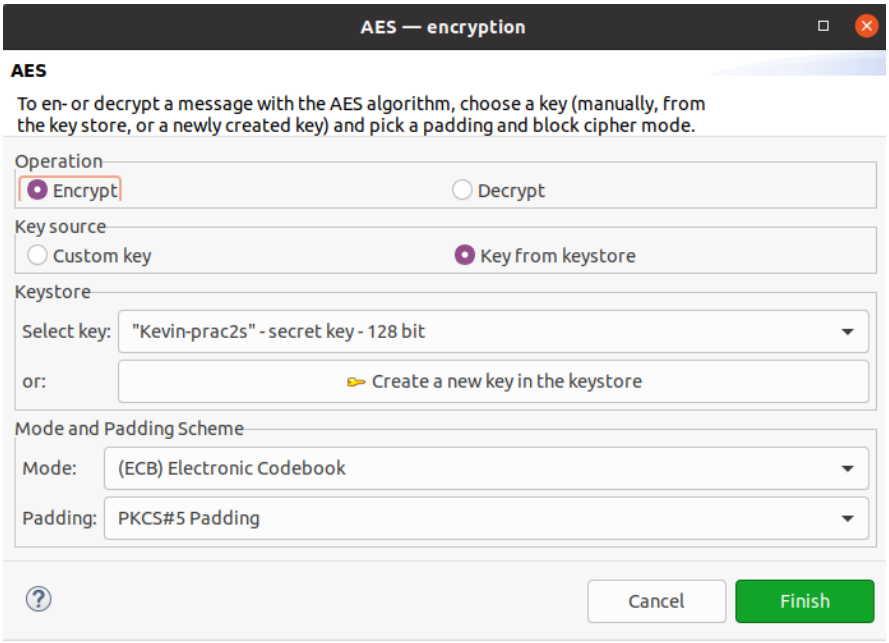

Figure 8: Pestaña AES

2.5 Elegir una clave, que puede ser manualmente introducida, o seleccionada del Keystore, con lo que podemos usar la que acabamos de crear en el paso anterior

La clave se ha elegido automáticamente y es la que hemos creado anteriormente como se muestra en la figura 8.

2.6 Seguir las indicaciones para cifrar y descifrar. Si hemos elegido, en particular, la clave almacenada en el Keystore, el sistema nos pedirá la contraseña mediante la cual se ha protegido al crearla. Compruébes que los procesos se realizan correctamente y al descifrar se recupera el texto claro original.

Se ha Cifrado como se ha comentado e ingresando la contraseña por la cual se ha protegido la clave, se ha cifrado mediante Electronic Code Book y como padding PKCS #5 Padding, el mensaje cifrado correspondiente es el que aparece en la imagen 9.

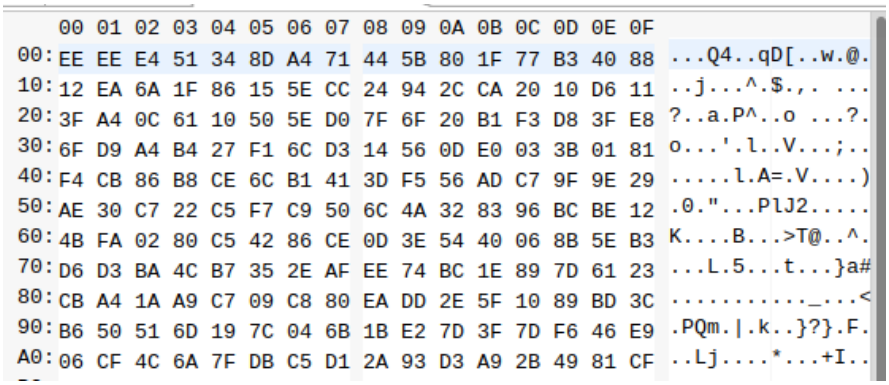

Figure 9: Output AES con ECB y padding PKCS #5

2.7 Probar los distintos métodos de relleno. El sistema nos permite no usar relleno, usar el estándar PKCS #5, relleno de unos y ceros, o ningún relleno. En particular conviene probar a cifrar usando un relleno y descifrar sin relleno. De este modo, veremos el relleno que el sistema ha añadido a nuestro texto claro original. ¿Qué ocurre cuando la longitud del texto claro coincide exactamente con el tamaño del bloque?

Sin padding el mensaje es más corto, una línea menoss

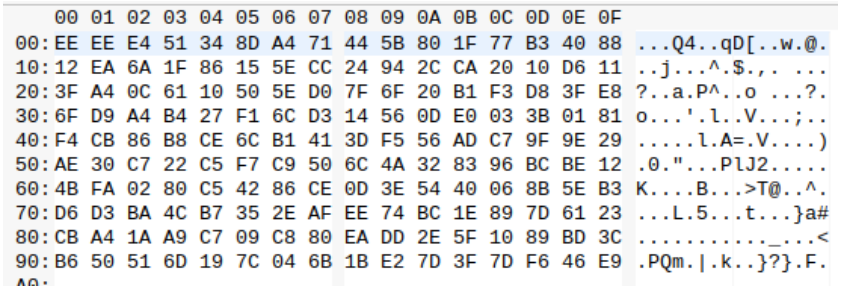

Figure 10: Output AES sin padding

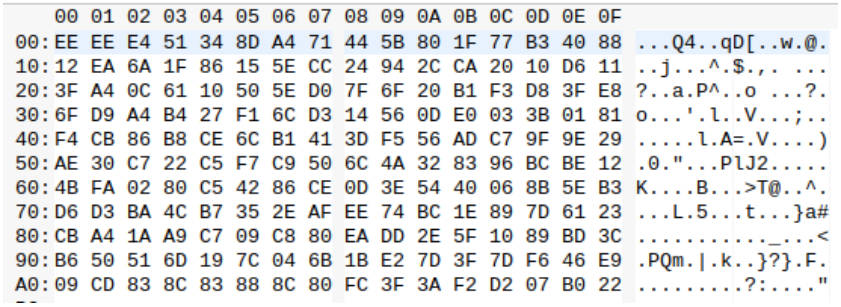

Figure 11: Output AES con padding 0 y 1

Cmo prueba se ha cifrado el mensaje de la figura 9 y se ha descifrado sin relleno, como se muestra en la figura 12 los ultimos bytes son $0B$, que en ASCII corresponde al número 11, como se explicó en clase corresponse al número de bytes que se rellena hasta llegar al final.

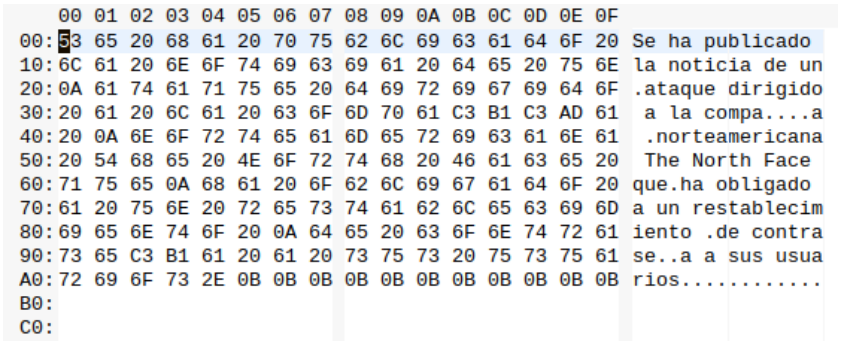

Figure 12: Descifrando sin relleno de un texto cifrado con relleno PKCS#5

Sin embargo si el texto de la imagen 9 se descifra con el mismo relleno no aparecen bytes de más como en el ejemplo anterior (y como se muestra en la figura 13)

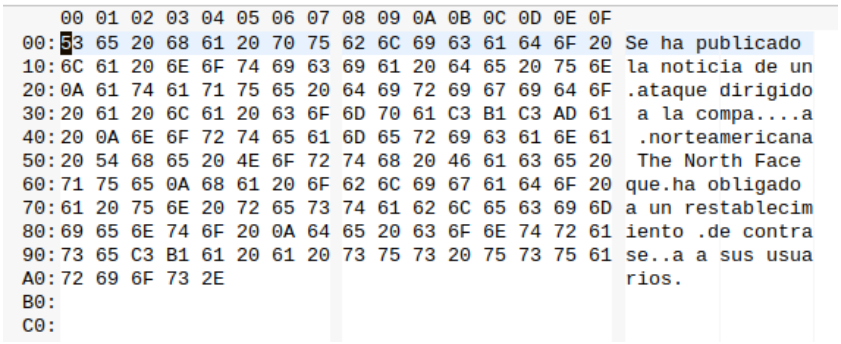

Figure 13: Descifrando con relleno PKCS#5 de un texto cifrado con relleno PKCS#5

2.8 Probar también los distintos modos de cifrado para asegurarse de que se producen distintas salidas.

Como se puede observar, distintos modos de operación, en este caso hemos probado con CBC (cifrado por bloques) y CTR (modo contador) nos genera distinta salida, obviamente del mismo tamaño.

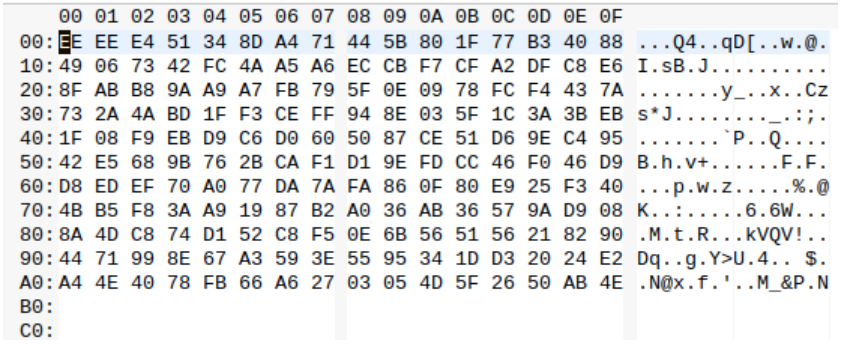

Figure 14: Output AES modo CBC con padding PKCS#5

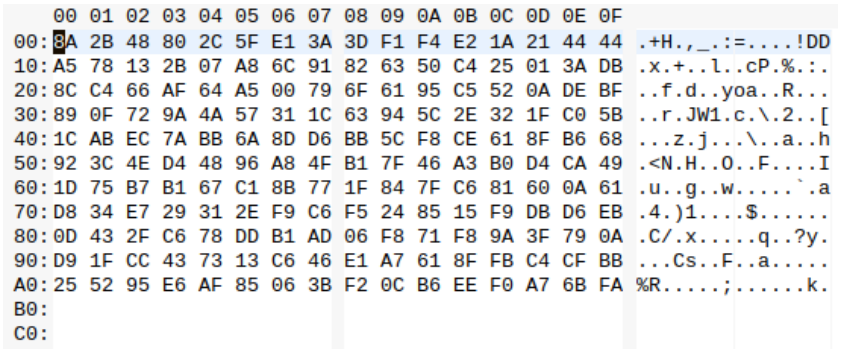

Figure 15: Output AES modo CTR con padding PKCS#5