EJERCICIO 1

Analice los siguientes fragmentos de un mismo texto cifrado con dos algoritmos clásicos. ¿Que nota? ¿Qué puede decir de cada uno? Luego de un pequeño análisis, pruebe descifrarlos con la herramienta jcryptool.

```
"Jxyj jx zs yjcyt ij qf rfyjwnf xjlzwnifi ij qf nsktwrfhnts.
Qt afrtx f hnkwfw hts itx fqltwnyrtx inxynsytx, d afrtx f ajw
htrt xj inkjwjshnfs frgtx wjxzqyfitx."
```

```
"Wwzm rx mr zmkyg hk tn rsxkzvf kimcenvej lr qs mtnbweeiqbs.
Ds biztk e iqswsv iwa igw gtttjmzubx vmybvslsy, g ifesy i ijj
guub xw honrwwriqns sqhwf wwwatgfvsy."
```

EJERCICIO 2

Genere un archivo de imagen de tipo raw, de 800x600 pixels, en blanco y negro. Escriba en él su nombre, lo más grande que pueda.

Encripte dicho archivo con openssl, utilizando aes-128 y los distintos modos de operación. Compare los resultados.

EJERCICIO 3

Se tienen sospechas de que en la imagen wargames.jpg está escondida, de alguna manera, una contraseña. ¿Cuál es dicha clave?

EJERCICIO 4

Situación:
Dado el mensaje firmado mail.eml, y los certificados y crl asociados, verifique si la firma es válida sin utilizar el cliente de correo. Documente el procedimiento que siguió para llegar al resultado.

Consigna:
Para resolver el ejercicio utilice como herramienta OpenSSL, y realice todos los pasos necesarios en forma individual.

EJERCICIO 5

El Timestamp es un mecanismo que sirve para demostrar que un dato existe y no fue alterado a partir de un momento dado en el tiempo. Un Timestamp es emitido por una Autoridad de Timestamping que actúa como tercero confiable testificando la existencia de dichos datos electrónicos en una fecha y hora concretos. Proponer un protocolo para Autoridad de Timestamping (TSA) utilizando certificados X.509 y firma digital. ¿Qué posibilidades de Fraude existen por parte de la TSA, y como se los podría disminuir?

EJERCICIO 6

La función crypt(3) de UNIX es utilizada para calcular el hash de las claves de usuario. Internamente funciona de la siguiente manera:

1. Se construye una clave DES (56 bit) truncando la contraseña del usuario a 8 caracteres y tomando 7-bits de cada carácter.

2. Se cifra un bloque de ceros utilizando la clave anterior utilizando una "SALT" (de 12 bits) para que dos contraseñas iguales cifren en dos valores distintos:
   crypt(s;x) = s +E(0)

3. Se itera 24 veces cifrando cada vez los resultados de la iteración anterior.

Supongamos que una aplicación Web construye una cookie de la siguiente forma:
crypt(SALT, nombre_de_usuario+secreto) = SALT + data_cifrada

¿Cómo se podría evadir la autenticación? ¿Qué otros problemas presenta el mecanismo de autenticación? ¿Se puede obtener el secreto del servidor?

EJERCICIO 7

El siguiente código es utilizado para verificar una firma:

```
checkSignature(text, sig, pubkey)
{
     sigHashPad = decrypt(sig, pubkey);
     textHash = hash(text);
     sigHash = removePadding(sigHashPad);

     padCheck = checkPadding(sigHashPad);
     hashCheck = (strncmp(sigHash, textHash,
HASH_SIZE) == 0);

     return (padCheck && hashCheck);
}
```

¿Cuál es el problema con el código? ¿Cómo lo solucionaría? ¿Si no se verificase el padding qué problemas podría traer?

Considerar el padding PKCS#1, donde:

- sigHashPad = 00 01 FF … FF 00 <SHA1-OID> <SHA1-HASH>
- len(sigHashPad) = RSAKeySize

EJERCICIO 8

Encontrar el error en el uso de la criptografía en el siguiente código en Ruby.

```
require 'active_support/secure_random'
require 'openssl'

def encrypt(key, text)
     # Initialize Cipher
     c = OpenSSL::Cipher::Cipher.new("aes-256-cbc")
     c.encrypt

     # Set Key
     c.key = key

     # Generate and set 32 byte Initialization Vector
     iv = ActiveSupport::SecureRandom.hex(32)
```

```
      c.iv = iv

      # Encrypt
      c.update(text)

      return c.final
end
```

Ayuda: Mirar la página del manual
http://api.rubyonrails.org/classes/ActiveSupport/SecureRandom.html

EJERCICIO 9

Una empresa tiene una aplicación Web que utiliza una cookie para autentificar al usuario. Contratan a un consultor en seguridad informática y éste les dice que su esquema no tiene protección de integridad de los datos y les sugiere que le agreguen un HMAC a la cookie.
La empresa decide implementar la sugerencia e implementa la validación de la cookie de la siguiente forma:
- Descifrar la cookie y verifica su contenido.
- Si es la versión nueva de la cookie, además verifica la integridad. Si no hay errores ejecuta el pedido del usuario.
- Si es la versión vieja de la cookie, y no hay errores, ejecuta el pedido del usuario y adicionalmente le emite una cookie de la versión nueva equivalente.

¿Cuál es el problema con este esquema?

EJERCICIO 10 (Opcional)

Descargue el siguiente archivo ISO (169MB)
https://download.vulnhub.com/pentesterlab/ecb_i386.iso
Arme una VM que bootee del mismo. Como podrá ver, tendrá disponible una aplicación web a la que puede registrarse y luego ingresar. Analice las cookies que devuelve el servidor una vez que el usuario se autenticó correctamente. Asumiendo que en contenido de la cookie esta cifrado con un algoritmo de cifrado simétrico por bloque, en modo ECB, genere una nueva cookie cifrada que le permite ingresar como si fuera el usuario admin.