**OBJETIVOS**

Esta prueba evalúa los conocimientos relativos a criptografía, comunicaciones seguras en servidores web, transferencia de archivos, servidores de aplicaciones y documentación de programas (JavaDoc).

**descripción DE LA PRUEBA**

El test consta de unas preguntas y de una parte práctica. Las respuestas siempre deben ser breves. En cualquier caso, tanto si las preguntas son binarias (tipo si/no o cierto/falso) o de respuesta simple/múltiple, hay que añadir un texto corto justificando la elección.

La respuestas incorrecta en preguntas tipo test, binarias o de respuesta simple o múltiple no puntúan negativamente.

Esta prueba es eliminatoria de materia a efectos de la evaluación.

**recursos**

A fin de realizar esta prueba correctamente pueden usarse los apuntes propios realizados en clase, la consulta a libros y artículos así como la consulta a recursos web.

**Cuestiones (4 puntos)**

1. Responde brevemente, ¿Qué es HTTPS, para qué se usa y en que puerto?

* HTTPS significa protocolo de transferencia de hiper texto seguro, y es la versión encriptada de HTTP. Se utiliza para una comunicación segura a través de Internet o de una red.
* Usa el puerto 443.

1. ¿Qué tipo de criptografía usa HTTPS?

* Utiliza un cifrado basado en SSL/TLS con el fin de crear un canal cifrado entre el cliente y el servidor.

1. Define brevemente que es un servidor de aplicaciones. ¿Es tomcat un servidor de aplicaciones?

* Es un [servidor](https://es.wikipedia.org/wiki/Servidor" \o "Servidor) en una [red de computadores](https://es.wikipedia.org/wiki/Red_de_computadoras" \o "Red de computadoras) que ejecuta ciertas [aplicaciones](https://es.wikipedia.org/wiki/Aplicaci%C3%B3n_(inform%C3%A1tica)" \o "Aplicación (informática)).
* Tomcat no es un servidor de aplicaciones, es un contenedor web con soporte de servlets y JSPs.

1. En la arquitectura a 3 niveles, ¿donde se ubica un servidor de aplicaciones?

* En el 2 nivel.
* En el nivel 1 se encuentra el nivel Cliente, solicitud de archivos, https, se envía la solicitud al servidor de aplicaciones, nivel 2 y luego al servidor de base de datos, nivel 3. El nivel 3 hace la consulta SQL y devuelve hasta el nivel 1.

1. ¿Cierto o falso? Si quiero enviar un correo con mi firma digital necesito tener la llave privada del destinario.

* Falso, se necesita llave pública.

1. Define brevemente que es el hash. ¿Es posible general el hash de cualquier archivo?

* Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.
* Sí, es posible general el hash de cualquier archivo.

1. ¿Puede usarse la función hash para encriptar un mensaje?

* Sí, se puede usar para encriptar cualquier tipo de archivo, mensaje, etc.

1. Relaciona los siguientes conceptos:

Criptografia, https, FTP, JBoss

Criptografia, Firma digital, hash: Necesitas el HASH para poder codificar algún tipo de mensaje, por ejemplo la firma digital.

Una persona quiere enviar un mensaje, primero lo cifra y lo envía con la llave pública. El receptor compara los datos usando el hash y lo compara con el hash descriptando usando la llave pública del emisor. Si los hashes coinciden, la firma es válida.

**Práctica (6 puntos)**

1. A través de la web <https://md5file.com/calculator>, el md5 del fichero anexado en esta prueba es.
2. 196a9ed3d7d2a0e1851483d175b2631a
3. a51b3b56a60919be1299e563b12acb30e64b59c0
4. 1baea1aceea8fd3a1159bd96b82db9a9da86e1e170b6388e014529442885812c5082d2bf2a071583e925ad4f1156c4b
5. Contenido de un mensaje. Has recibido el siguiente mensaje de Patricia:

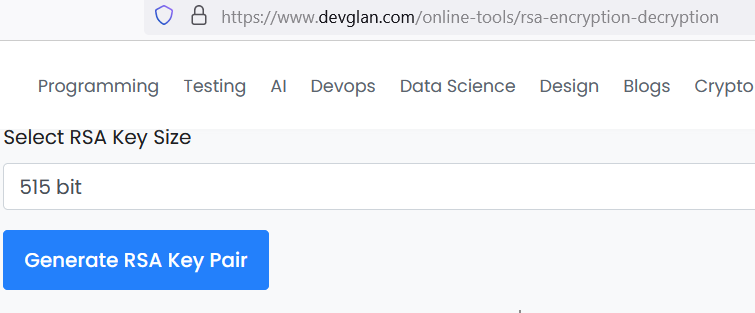
Estamos a mediados de Diciembre de 2022. Felices fiestas.

TuTe9OyNWKzuOAPdO9oNNVAd3yw+iSCRLZvPkLVu4k831kGh9d8S/83SCdzu1Z1GOtqNu8lzDUCWCqkA1NXVdw==

¿Lo está enviando realmente Patria o no? Describe los pasos que sigues y el resultado que vas obteniendo para decir que la firma digital del mensaje corresponde o no a Patricia.

<https://herramientas-online.com/generador-hash-online.html>

<https://www.devglan.com/online-tools/rsa-encryption-decryption>

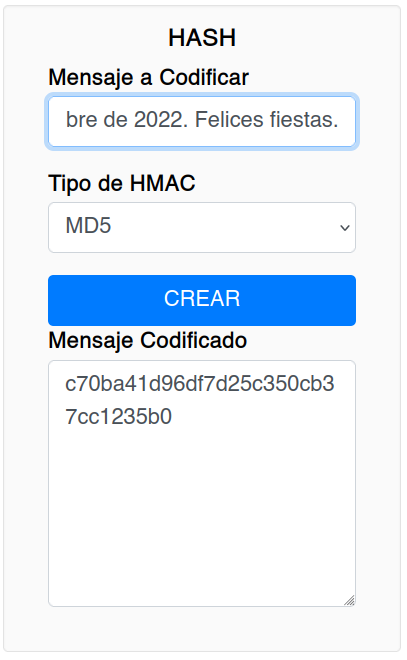


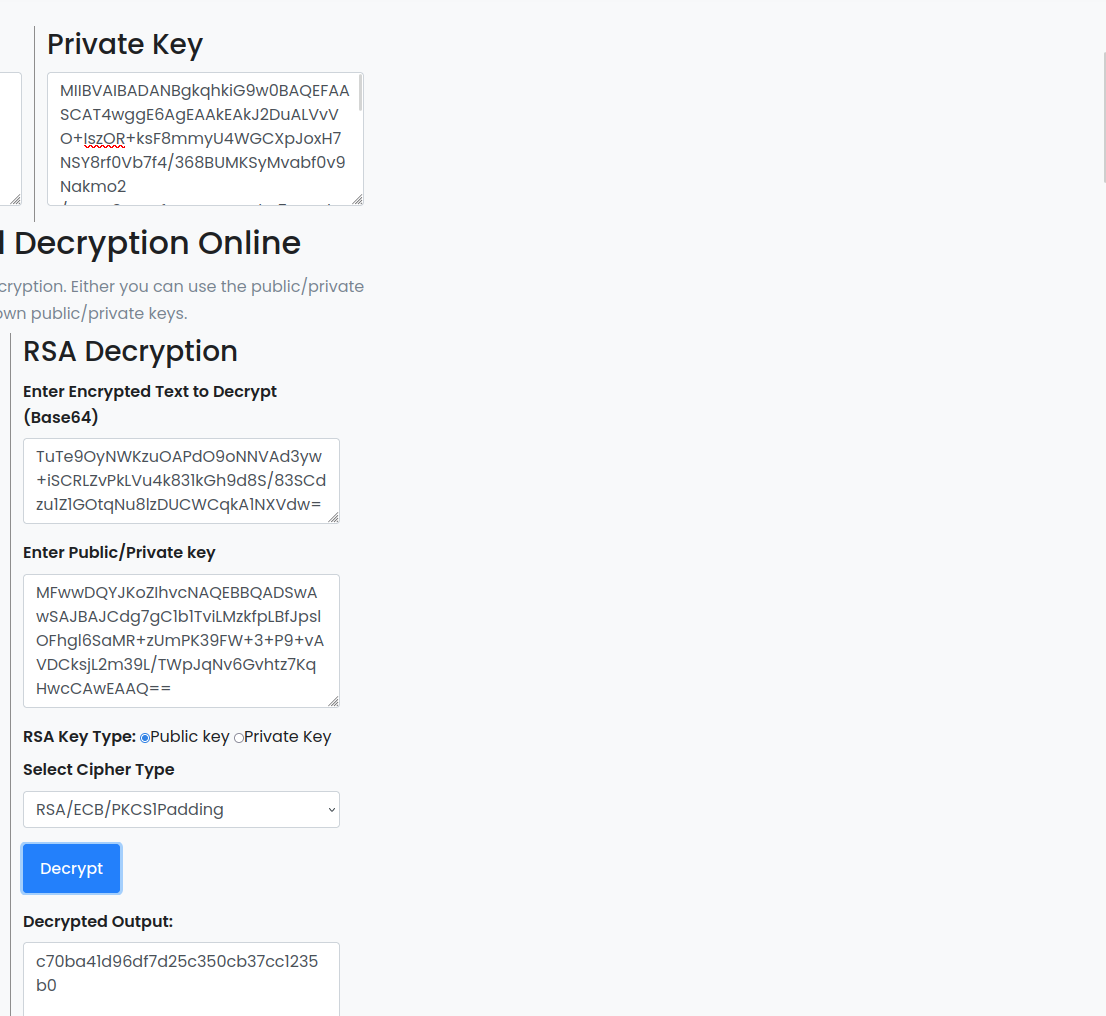
|  |
| --- |
| **Llave pública de Patricia** |
| MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJCdg7gC1b1TviLMzkfpLBfJpslOFhgl6SaMR+zUmPK39FW+3+P9+vAVDCksjL2m39L/TWpJqNv6Gvhtz7KqHwcCAwEAAQ== |
| **Llave privada de Patricia** |
| MIIBVAIBADANBgkqhkiG9w0BAQEFAASCAT4wggE6AgEAAkEAkJ2DuALVvVO+IszOR+ksF8mmyU4WGCXpJoxH7NSY8rf0Vb7f4/368BUMKSyMvabf0v9Nakmo2/oa+G3PsqofBwIDAQABAkA5rKgwhejqZfCJfnayVTsBjamX1S2Ymd3/QqkYubz552vQSKcOVBWCF1CIFdRbqy88zZYYs+nM3zogYRGG+G4pAiEAyFpGwi0aJrOl28C6vULZNY4mevJPN10qR93i1aM2PwUCIQC4yCGlgZOukIWw3AlHXCuni9HofmdGf9mKc5zQRsXLmwIhAKumTIEHyyPlPfAsCtEjeJydkPI8rwmr1BGGVFTcZBlRAiADxFCrRxDzpg6TpGisA70AFWGaE7mXPlP49pJjzI2LsQIgXRr7lyOJ+YH7xUwF6+PGVQ9lkWWfe230rFBLeM1kjAM= |

|  |
| --- |
| **Tu llave pública** |
| MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAOwTEo9nIbfwmjG/O/vV+HBgI0WIyQrcFAEpfaKfvm1T5K9RsL/rK9mti+Nb46rvUakI8rUSSdj+aalXH/ZG5wsCAwEAAQ== |
| **Tu llave privada** |
| MIIBVQIBADANBgkqhkiG9w0BAQEFAASCAT8wggE7AgEAAkEA7BMSj2cht/CaMb87+9X4cGAjRYjJCtwUASl9op++bVPkr1Gwv+sr2a2L41vjqu9RqQjytRJJ2P5pqVcf9kbnCwIDAQABAkEAkdGiGEQK1tReWjYWdhMP11H613uLOxL/pEwdl3L2rA4C99N6kOXBVGysvX/dksyTb6sLJHN1XD/zOVdAMriC6QIhAP+j13WiYVUOwnXazdwXZLm1TLP9WBNExMn9usm6ABA9AiEA7Ggtb8kESc/EzMAVtAhegf5oOeOucG6wwfg6jW5dQOcCIQDOhr1AqejcYMo1kImTb8rORWwsVVZcashZL4VCB+SZOQIgMlmFw9cmSKotmgYXGT7nEfyjKiEp19xbXRSHM/QbfGUCIE2IBor5SDx6XsW3pCVMnZSUqMDC1lBqCydWMWidfzyt |

**PASOS**

* Primero codifico el mensaje que me envía Patricia para luego ver si concide.



* En Private Key, pongo la de Patricia.
* Pongo el mensaje cifrado *TuTe9OyNWKzuOAPdO9oNNVAd3yw+iSCRLZvPkLVu4k831kGh9d8S/83SCdzu1Z1GOtqNu8lzDUCWCqkA1NXVdw==*
* Pongo la Public Key de Patricia, le doy a decrypt y puedo comprobar que ambos mensajes coinciden, por lo tanto, sí es Patricia quien envía el mensaje.
* 

**evaluación**

En todas las respuestas se valorará el grado de concreción, la argumentación en las mismas. No se trata de dar opiniones, propias ni ajenas (como si hiciera cortar/pegar), sino de demostrar que se entienden los conceptos estudiados y se es capaz de aplicarlos.

La prueba se evalúa teniendo en cuenta los resultados y su análisis posterior, y se evalúa cada parte independientemente.

* >= 9 Excelente
* < 9 Notable
* < 7 Suficiente
* < 5 Insuficiente
* < 3 Muy deficiente

**Nota: Propiedad intelectual**

Al contestar una pregunta a menudo es inevitable hacer uso de recursos creados por terceras personas. Para que ello no suponga un plagio, siempre que una respuesta haga uso de recursos ajenos, se citará la fuente ajena de manera correcta.

Referencias:

[Empresaactual.com](https://www.empresaactual.com/funciones-hash-su-explicacion-mas-sencilla/)

[Uanataca.com](https://web.uanataca.com/es/blog/tecnologia/hash-y-firma-electronica)

[wikipedia.com](https://es.wikipedia.org/wiki/Funci%C3%B3n_hash)

[ibm.com](https://www.ibm.com/mx-es/cloud/learn/three-tier-architecture)