UNIVERSIDAD COMPLUTENSE MADRID

ntic master

TAREA EVALUABLE

Máster en Ciberseguridad

MÓDULO

Criptografía aplicada y Esteganografía

PROFESOR

Dr. Alfonso Muñoz Muñoz

Contenido

1 Enunciado de la práctica y evaluación

La empresa Crypto S.A le ha contratado, gracias a su conocimiento criptográfico adquirido durante esta formación, para ayudar en el diseño de soluciones tecnológicas que faciliten a la empresa mayor confidencialidad, integridad y autenticidad de su información, almacenada o en tránsito.

Dada las restricciones de presupuesto para resolver las siguientes cuestiones utilizará el software opensource OpenSSL y si fuera necesario pequeños scripts usando los lenguajes accesibles en las terminales de Windows/Linux/Mac.

Se le solicita sus servicios para resolver las siguientes cuestiones:

Pregunta 1 (5 puntos) - Encuentre la mejor solución para dada una clave de usuario de 128 bits generar 10 claves que permitan cifrar 10 ficheros, cada uno con una clave diferente. Implemente la solución para cifrar y descifrar dichos ficheros (su contenido no es relevante). Pista: Openssl y scripts le ayudarán en esta tarea.

Pregunta 2 (2,5 puntos) - Utilizando Openssl cifre un fichero usando el algoritmo autenticado AES-GCM

Pregunta 3 (2,5 puntos) - Utilizando Openssl cree un par de clave pública/privada con curva elíptica, elija cualquier curva, y firme un documento verificando posteriormente su firma

Justifique y documente su respuesta para cada una de las preguntas en un mismo documento. Incorpore capturas de pantalla para facilitar la corrección y evaluación de las soluciones alcanzadas.

2 Referencias

https://www.openssl.org/
https://www.geeksforgeeks.org/practical-uses-of-openssl-command-in-linux/