PREGUNTAS CODEFEST

1. Un compañero piensa que para esto se puede tener un set de llaves públicas y uno de llaves privadas, entonces lo que se envía es la llave pública para descifrar, y tanto el satélite como el centro de control tienen sus set de llaves privadas, que esas si no se envían, y están cifran las otras llaves.

   Otro compañero dice que esto tiene que ser totalmente desacoplado, osea que de alguna manera ambos sepan cual es la llave, por ejemplo lo del timestamp(aunque lógicamente eso no se puede usar al ser tan trivial). Pero algo parecido que sea inaccesible por otra persona.

   >> Totalmente desacoplado, solo hay comunicación cuando el satélite envíala información. El problema de tener llaves privadas es que estás se deben gestionar de forma dinámica también

2. ¿El sistema puede tener salida a internet?

   >> No

3. ¿Alguna restricción al uso de algoritmos de cifrado ya existentes?

   >> Se deben usar los de calidad satelital, o con mejores capacidades.

4. ¿Alguna restricción al uso de protocolos orientados a comunicación ya existentes?

   >> No

5. ¿Cuáles son los recursos del computador en el que se va a compilar y ejecutar (Hilos, CPU)?

   >> Recursos similares a una jetson nano

6. ¿Cuáles son los recursos del sistema embebido en el que se va a trabajar?

   >> Jetson nano

7. ¿En esta primera entrega, es necesario tener la comunicación con el satélite, o se va a ejecutar todo local?

   >> No es necesaria la comunicación, todo se va a ejecutar local en esta fase.

8. ¿En los test con plataformas automáticas (NFER (Facebook) y SonarQube) se va a subir la imagen, o en que formato se va a evaluar el mismo?

   >> SonarQube a INFER son analizadores estáticos. Las pruebas funcionales las vamos a hacer con ayuda de una herramienta propia automatizadora, que invoca el código entregado por los equipos.

9. Una pregunta, como debemos simular la creación de llaves dinámicas?Por ejemplo, nuestro grupo ha considerado utilizar Diffie-Hellman. ¿Como se espera representar este proceso u otros similares?

>> Parte del reto es que ustedes propogan una solución para generar llaves dinámicas

10. Buenas noches, queríamos preguntar si tenemos libertad de escoger la versión de C++ para hacer el reto, concretamente queríamos preguntar si podemos usar C++20
    >> No hay problema
11. ¿Las funciones de encriptar y desencriptar pueden estar en diferentes archivos?
    >> No. Deben usar la plantilla que les dimos

12. ¿Para la solución del reto se puede tomar que el proceso de encriptación se hace en simultáneo al envío de datos? Es decir que no, el sistema no tiene que esperar a tener el total de encriptada para enviar la imagen
    >> Se hace en tándem, es decir el cifrado termina y ahí si se puede descifrar

13. ¿Para el reto podemos tener en cuenta que durante el proceso de encriptación hay comunicación bidireccional del satélite y la estación terrena?
    >> No hay comunicación bidireccional

14. Respecto al **algoritmo de descifrado**, si bien dijeron que para esta entrega no se va a simular un ataque o alteración de datos, debemos de igual manera verificar que la información no haya sido modificada. Siguiendo las pautas del CCSDS 352.0-B-2, es decir, ¿debemos usar GCM (Galois/Counter Mode) o podemos simplemente usar CTR (Couter) y no verificar?

    >> Tanto en las charlas como en las guías se les indica que el modo debe ser CTR

15. ¿Respecto al uso de llaves dinámicas, esta debe ser actualizada según el tiempo, actualizarse por cada imagen (ser diferente para cada imagen), o es algo que queda libre a nuestro criterio?

    >> Libre a su criterio. Sin embargo tengan en cuenta que entre más rápido se cambie, más seguro el sistema

16. ¿El proyecto debería tener una estructura en específico?
    >> No, pero el archivo principal debe seguir la plantilla que les dimos

17. Respecto a las librerías utilizadas, ¿cómo debería hacerse la importación y en qué sistema operativo van a probarla?
    >> Les recomendamos que tengan un make file

18. ¿Se espera que las funciones encriptar - desencriptar se ejecuten siempre de manera secuencial (Es decir, que la imagen se encripta e inmediatamente después se desencripta) o es posible que se encripten varias imágenes y luego se llame la función desencriptar?

    >> Por ahora vamos a probar de a una imagen

19. ¿Se pueden modificar los parámetros de las funciones añadiendo el número de imágenes a encriptar o se deben respetar las interacciones con el usuario propuestas en la plantilla?

    >> Se debe seguir la plantilla

20. ¿Todas las imágenes se encontrarán en el almacenamiento local del dispositivo de ejecución, o es posible que nos entreguen enlaces?
    >> Imágenes locales

21. ¿Cuál va a ser el tamaño máximo y los formatos de las imágenes?

    >> EL formato es TIFF. El dataset de pruebas incluye imágenes muy grandes (e.g., 16g)

22. Si porfa nos pueden compartir las imágenes y el formulario para enviar el repositorio de git hub. Quedamos pendientes, gracias

    >> Las imágenes y el formulario se los enviaremos pronto

23. En el documento del enunciado se lee: "Dediquen tiempo al diseño de la solución; recuerden que el algoritmo AES necesita llaves y estas llaves deben ser dinámicas. Piensen muy bien en la estrategia de generación o de transmisión segura de la llave, el satélite y la estación terrena solo se conectan cuando están alineados. "No entendemos muy bien a qué hace referencia la idea de que se conectan cuando están alineados. Además de eso nos queda la duda de si el satélite y la estación se pueden transmitir algún tipo de información además de la imagen cifrada, y de ser así, en qué parte de la plantilla del código se podría añadir esta comunicación.

    >> Hagan de cuenta que lo único que se transmiten es el archivo de una imagen cifrada

24. ¿Debemos considerar que el medio por el cual se transmiten las llaves es inseguro? Es decir, ¿Se deben implementar mecanismos para garantizar atributos como la confidencialidad, la autenticación y la integridad a la hora de transmitir las llaves? ¿O una posible solución puede ser comunicar la llave de formar explícita?

    >> El medio no es seguro

25. ¿Podemos asumir que el intercambio de llaves ocurre dentro de un mismo entorno de ejecución (por ejemplo, un mismo dispositivo)? Es decir, ¿Las llaves se pueden guardar en un directorio específico al cual las funciones de cifrado y descifrado acceden cada vez que necesiten? ¿O es necesario utilizar medios como internet para la transmisión de las llaves?

>> No se pueden trasmitir las llaves a través de un directorio porque cifrado y descifrado se hacen en lugares diferentes; No se puede hacer transmisión de llaves a través de internet

26. ¿Cuál es el tamaño estimado para una sola de las imágenes a cifrar y descifrar? Pues esto nos permitiría evaluar nuestro desempeño y determinar si los algoritmos cumplen con las restricciones de memoria del reto.

>> La restricción de memoria es que los métodos al ser ejecutados no pueden consumir más de 4G de RAM

27. Me dirijo a ustedes para aclarar una inquietud que ha surgido en nuestro equipo. Queremos saber si es permitido entregar el código del reto, indicando el sistema operativo en el que se realizaron las pruebas de ejecución y describiendo los pasos necesarios para utilizar las librerías externas implementadas en el proyecto. En caso contrario, agradeceríamos que nos informaran si existe un protocolo específico para el uso de este tipo de librerías.

>> Si, aclaren por fa todo eso en el README sin embargo les recomendamos que tenga en el repo un MAKE file