GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura i Esport

ceedcv CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

Unidad 4.2
Criptografía
Ejercicio evaluable 3

Licencia

1 Cifrado simétrico - AES

En este ejercicio, se solicita realizar un cambio en el algoritmo de cifrado simétrico que utiliza el algoritmo DES, para migrar el código a AES, ajustando también los comentarios correspondientes en el código ejemplo.

Teniendo en cuenta que:

- DES y AES están en la misma librería
- Usa el mismo modo OFB. Este modo también usa el vector de industrialización IV, pero en este caso debe tener la longitud del bloque AES.
- La longitud de la clave debe ser de 16, 24, o 32 bytes. Yo he usado la de 32 (clave de 256 bits).
- AES es una cipher (algoritmo de cifrado) de 16 bytes y por ello los datos deben tener una longitud múltiplo de 16: Longitud%16=0. Si tenemos un texto que no cumple esto, debemos modificarlo añadiendo, por ejemplo, espacios al final.
- Realiza las modificaciones necesarias en las funciones encrypt y decrypt para utilizar el algoritmo AES en lugar de DES. Asegúrate de que el modo de operación utilizado sea adecuado para AES.
- Actualiza los comentarios del código para reflejar los cambios realizados y proporcionar información sobre las diferencias entre DES y AES

Comentarios Adicionales:

- **DES (Data Encryption Standard)**: Fue un estándar de cifrado simétrico ampliamente utilizado. Sin embargo, su clave corta de 56 bits ha llevado a preocupaciones sobre su seguridad, y AES se ha convertido en su sucesor preferido.
- **AES (Advanced Encryption Standard)**: Es un algoritmo de cifrado simétrico más moderno y seguro que DES. Ofrece longitudes de clave de 128, 192 o 256 bits, proporcionando un mayor nivel de seguridad en comparación con DES.