Cifrado y websockets

Buscar en Internet la forma de enviar correos electrónicos con NodeJS. Hacer un ejemplo que envíe correos electrónicos usando los servidores de EducaMadrid.

Leer en los apuntes el apartado “9 Variables de entorno”. Entender que actualmente no se codifica información como pueden ser contraseñas o credenciales de acceso a bases de datos en el código. Se pasan a través de variables de entorno. Hacer un pequeño ejemplo en el que se cree una variable de entorno y se trate de mostrar su valor en pantalla a través de NodeJS.

Leer el apartado “10 Código HASH de textos”. Entender que las contraseñas no se pueden descifrar una vez cifradas, pero se pueden volver a cifrar para comparar valores almacenados. Dependerá del algoritmo, pero actualmente se suele generar un salt y una hash.
Hacer un pequeño ejemplo en el que se cifre un texto y se compruebe que está correctamente cifrado.

Leer el apartado “11 Tokens”. Entender el concepto y hacer el siguiente ejercicio (cayó en examen):
Hacer una página web en la que se le pase un texto y éste sea cifrado en un token que se muestre como resultado. Hacer una segunda página web en el que se le introduzca el token generado y devuelva el texto original.

Leer los apartados 11.1 y 11.2 y tratar de hacer el siguiente ejercicio:
Hacer una página web en la que se le pase un texto. El servidor debe cifrar el texto en un token y enviarlo al cliente en una cookie. Si el servidor recibe la cookie y tiene un token, debe descifrar el token y mostrar el contenido del texto descifrado al cliente.

Leer el apartado “12 Cifrando conexiones con HTTPS” y sus subapartados.

Leer el apartado “13 Websockets” y sus subapartados. Haga los ejercicios de WebSockets.