1 Cifrado simétrico

Para realizar el cifrado simétrico en Javascript se puede usar una función como la siguiente:

```
const crypto = require("crypto");

const algorithm = "aes-192-cbc";

function encrypt(text, password, iv, func) {
  //generate encryption key using the secret.
  crypto.scrypt(password, 'salt', 24, (err, key) => {
    if (err) throw err;

    const cipher = crypto.createCipheriv(algorithm, key, iv);

    let encrypted = '';
    cipher.setEncoding('hex');
    cipher.on('data', (chunk) => encrypted += chunk);
    cipher.on('end', () => func(null, encrypted))
    cipher.on('error', (err) => func(err, null))

    cipher.write(text);
    cipher.end();
  });
}

const texto_a_cifrar = 'hello World';
const password = 'contraseña';
const iv = 'ABCDEFGHIJKLMNOP';
//En criptografía, un vector de inicialización (conocido por sus siglas en
// inglés IV) es un bloque de bits que es requerido para permitir un cifrado en
// flujo o un cifrado por bloques, en uno de los modos de cifrado, con un
// resultado independiente de otros cifrados producidos por la misma clave.
encrypt(texto_a_cifrar, password, iv, (err,cifrado) => {
  if(err) console.log(err);
  console.log(cifrado);
});
```

El descifrado se podría realizar con:

```
const crypto = require("crypto");

const algorithm = "aes-192-cbc";

function decrypt(encrypted, password, iv, func) {
  //generate encryption key using secret
  crypto.scrypt(password, 'salt', 24, (err, key) => {
    if (err) throw err;

    //create decipher object
    const decipher = crypto.createDecipheriv(algorithm, key, iv);

    let decrypted = '';
    decipher.on('readable', () => {
      while (null !== (chunk = decipher.read())) {
        decrypted += chunk.toString('utf8');
      }
    });
    decipher.on('end', () => func(null, decrypted));
    decipher.on('error', (err) => func(err, null))
```

```
    decipher.write(encrypted, 'hex');
    decipher.end();
  })
}

const iv = 'ABCDEFGHIJKLMNOP';
const cifrado = 'b7a50483519f701c533498605c38b4df';
const password = "contraseña";
decrypt(cifrado, password, iv, (err, valor) => {
  if(err) console.log(err);
  console.log(valor);
})
```