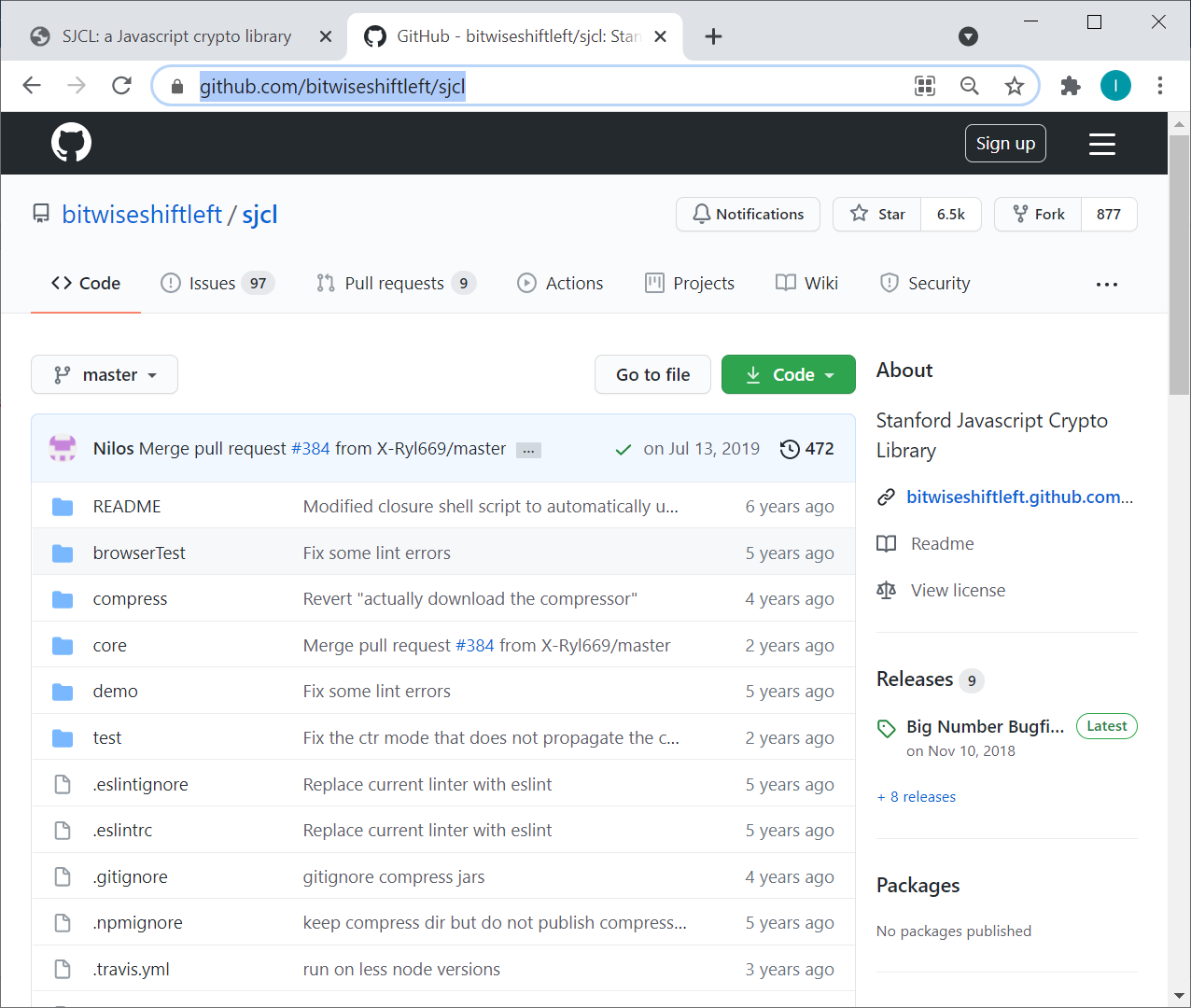
GitHub - sjcl (Javascript Source)

<https://github.com/bitwiseshiftleft/sjcl>

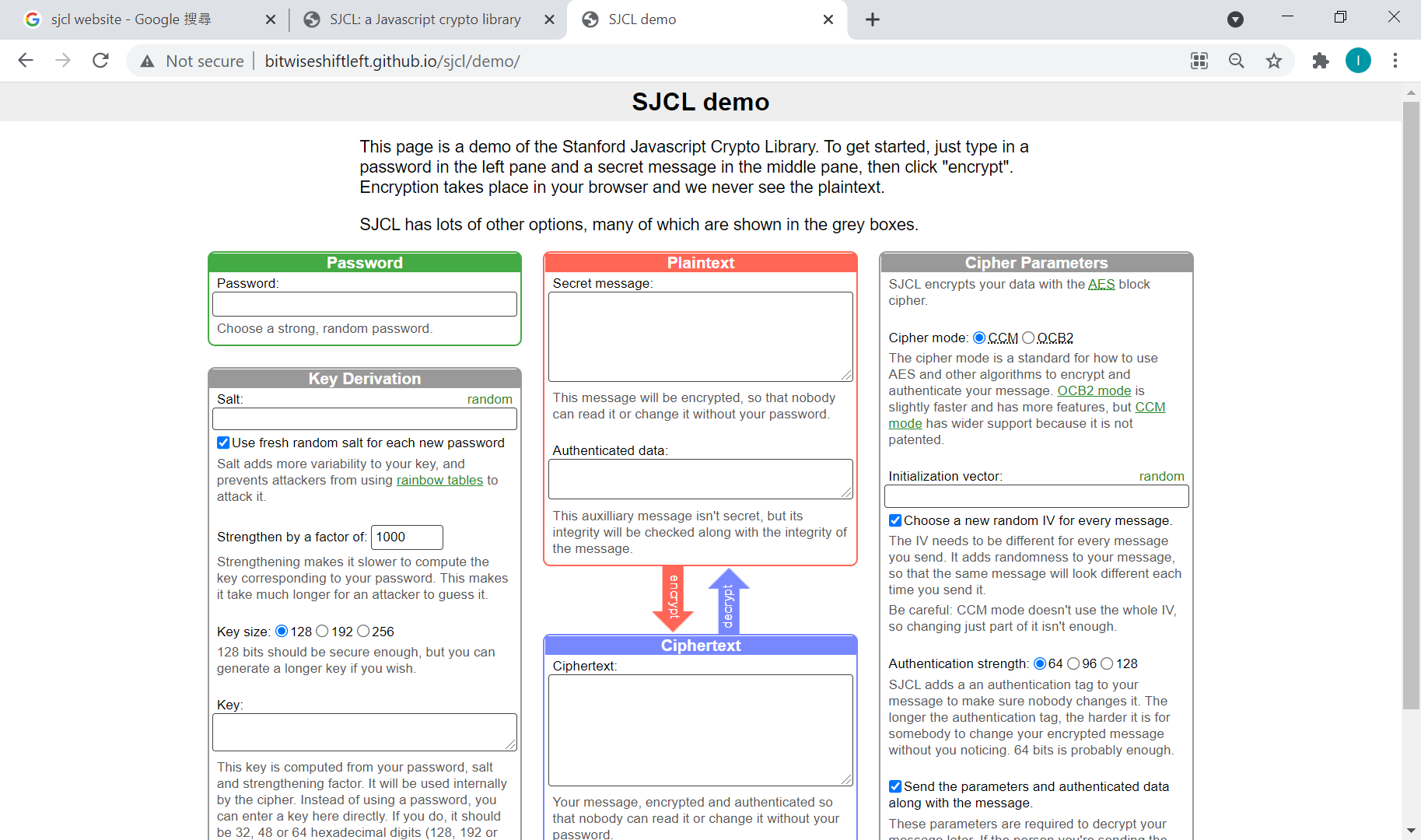


SJCL Source Code:



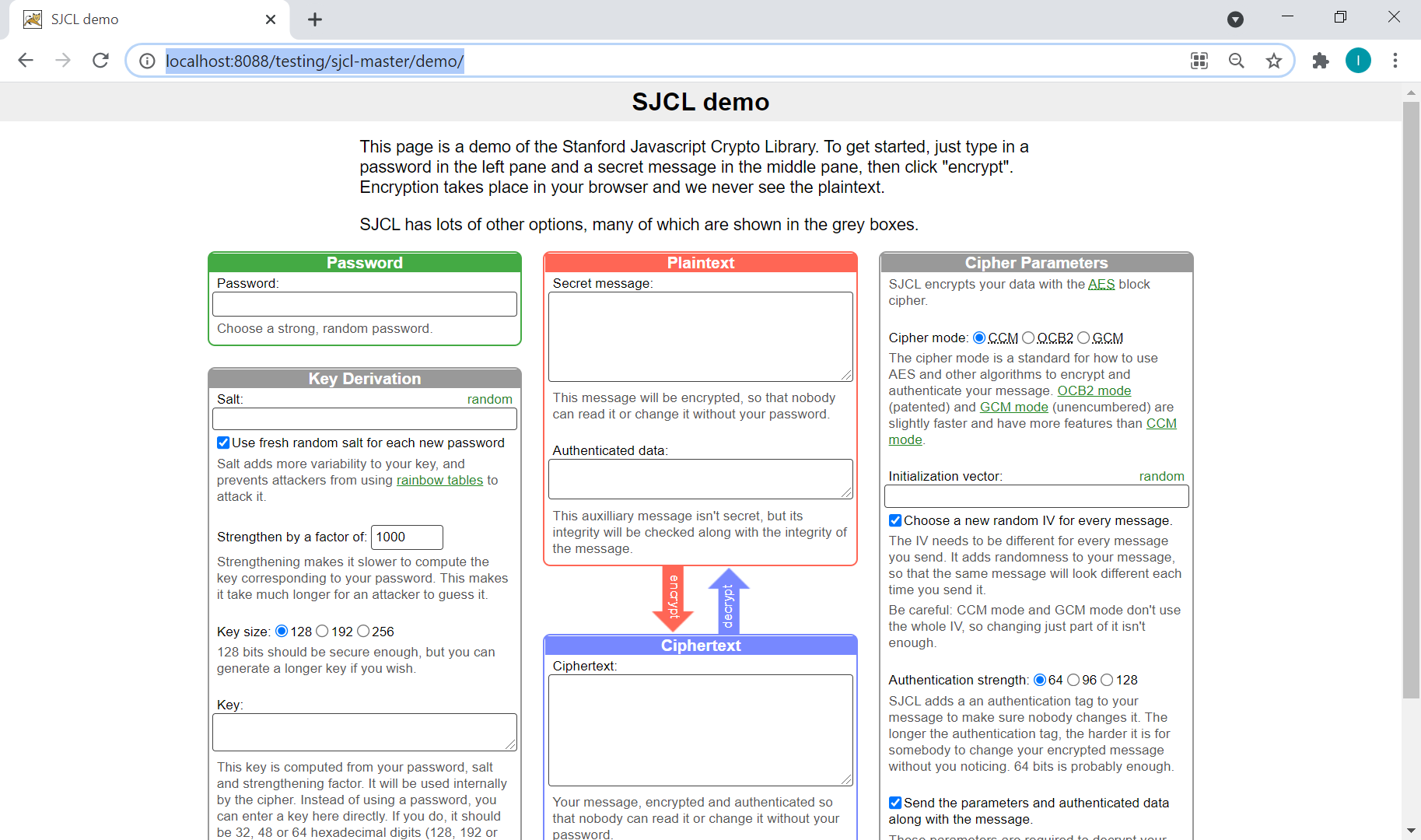
Web Site:

<http://bitwiseshiftleft.github.io/sjcl/demo/>



Local Host:

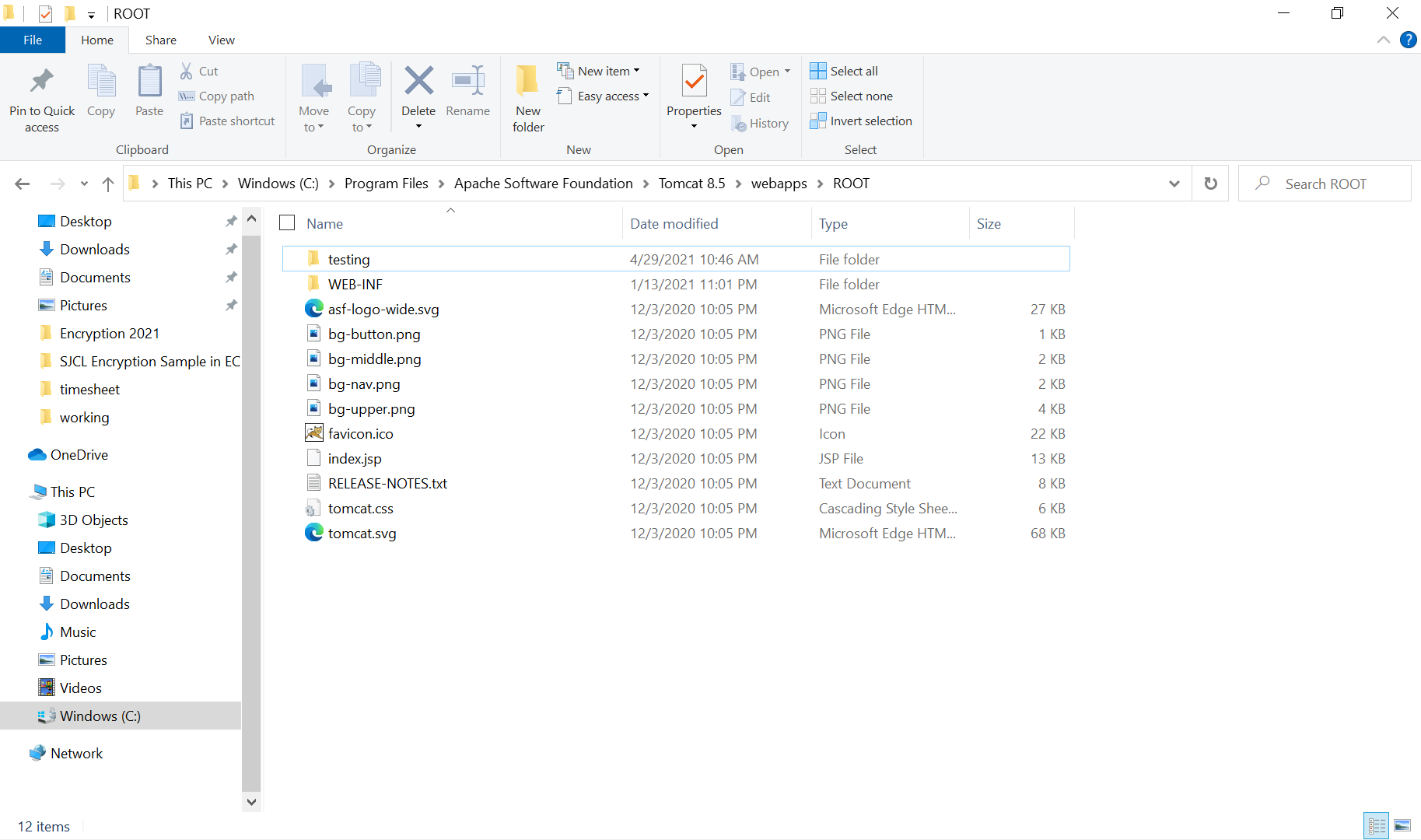
<http://localhost:8088/testing/sjcl-master/demo/>



The Web SJCL demo page doesn’t contain the GCM Mode, that only support in localhost.

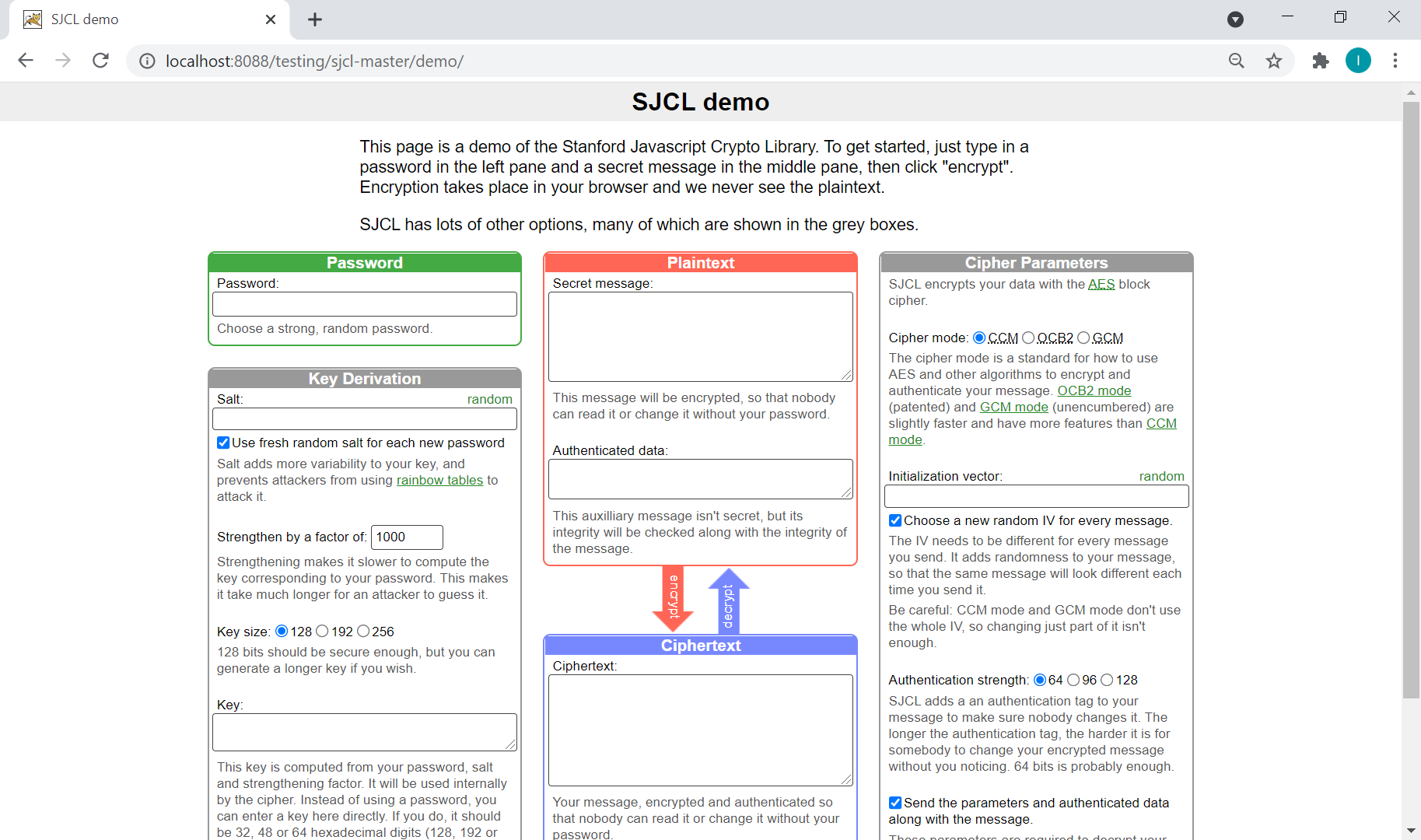
Setup Javascript:

Extract “testing” folder to Tomcat “ROOT” directory (install tomcat not mandatory)



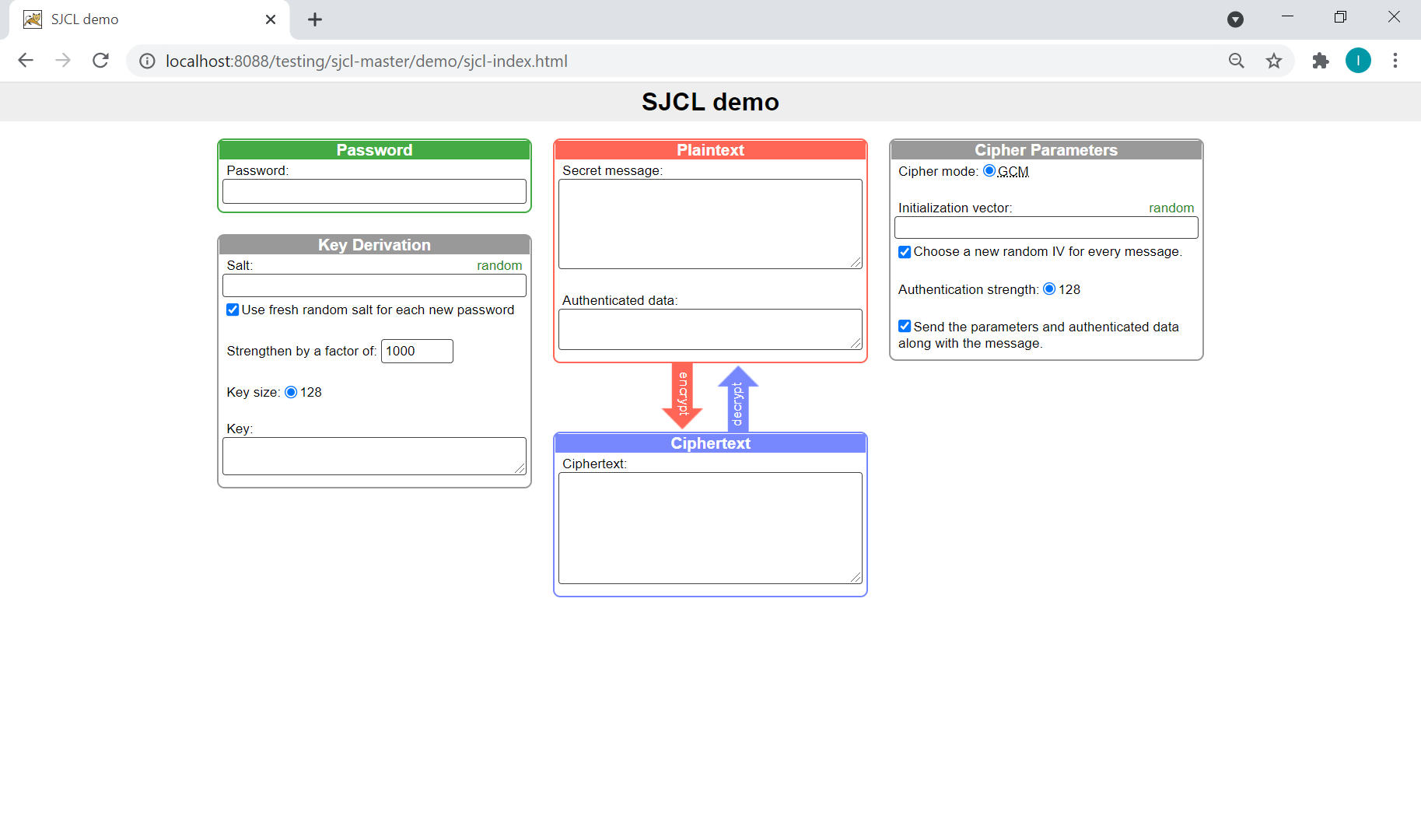
Local Host:

<http://localhost:8088/testing/sjcl-master/demo/>



Local Host: (Automate)

<http://localhost:8088/testing/sjcl-master/demo/sjcl-index.html>

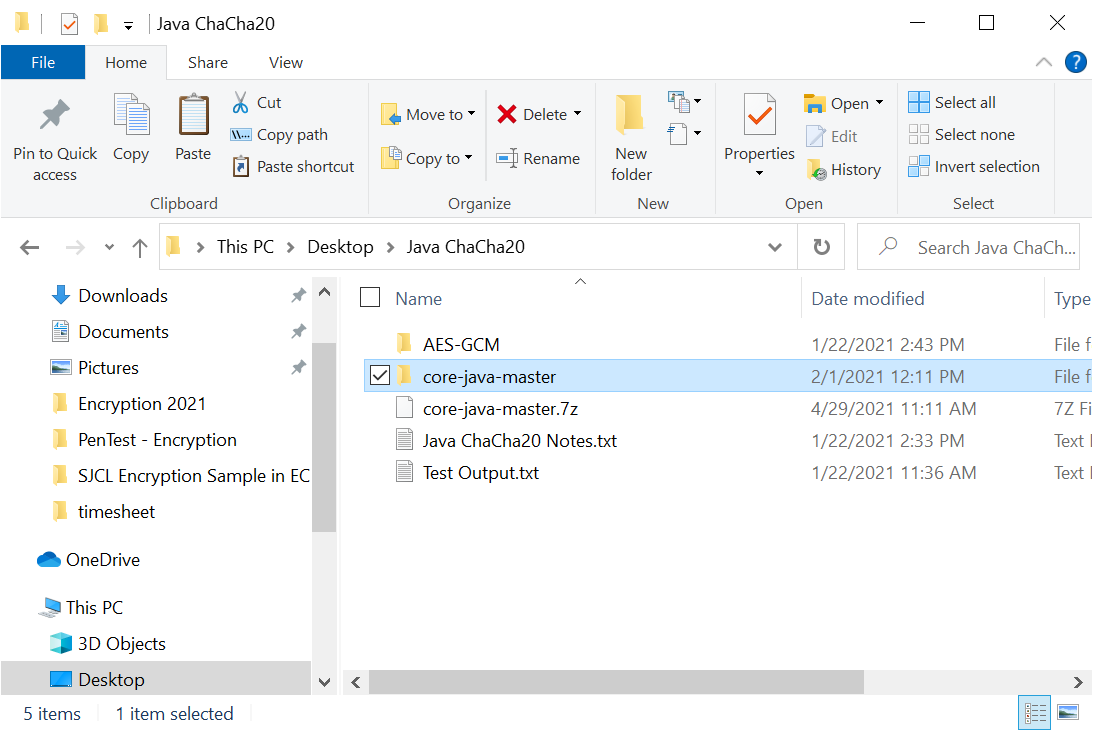


Java Setup – Source Location:

core-java-master\java-crypto\src\main\java\com\mkyong\crypto\encryptor\SJCLDecryptTest.java



Extract “core-java-master” folder to Java Directory

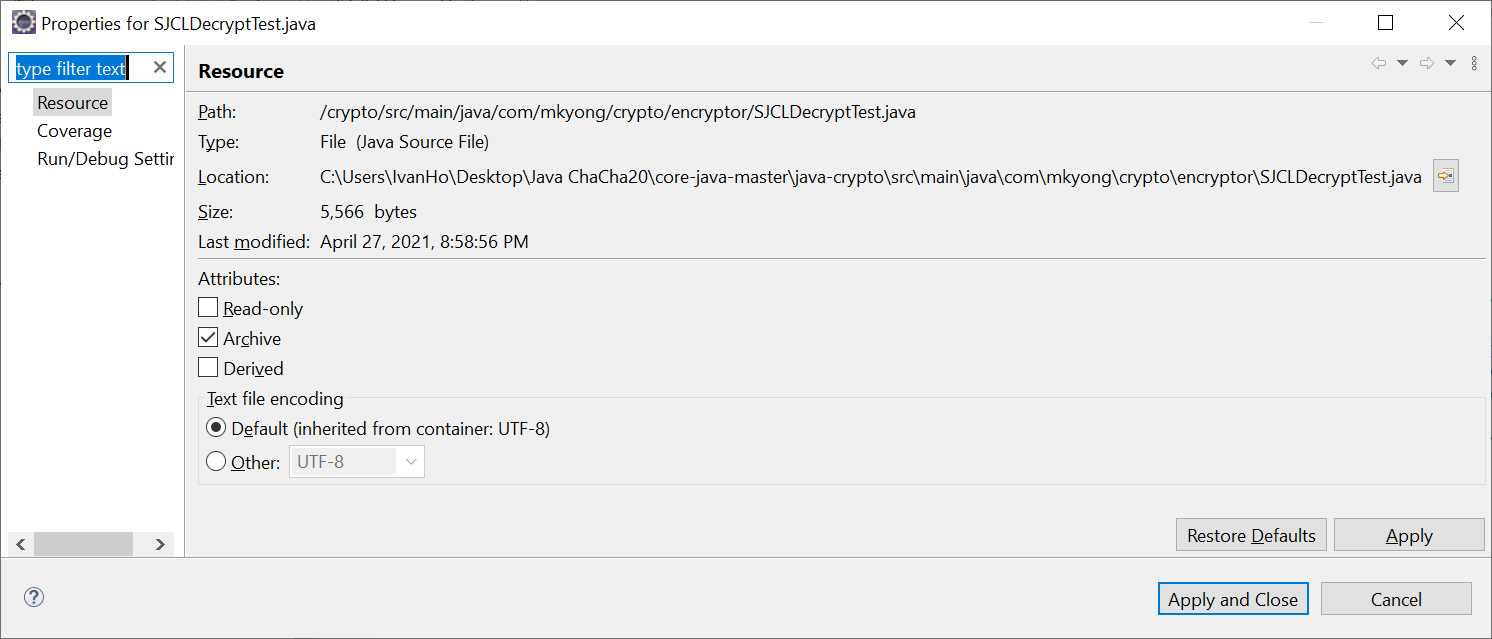


Import Source Code to Eclipse



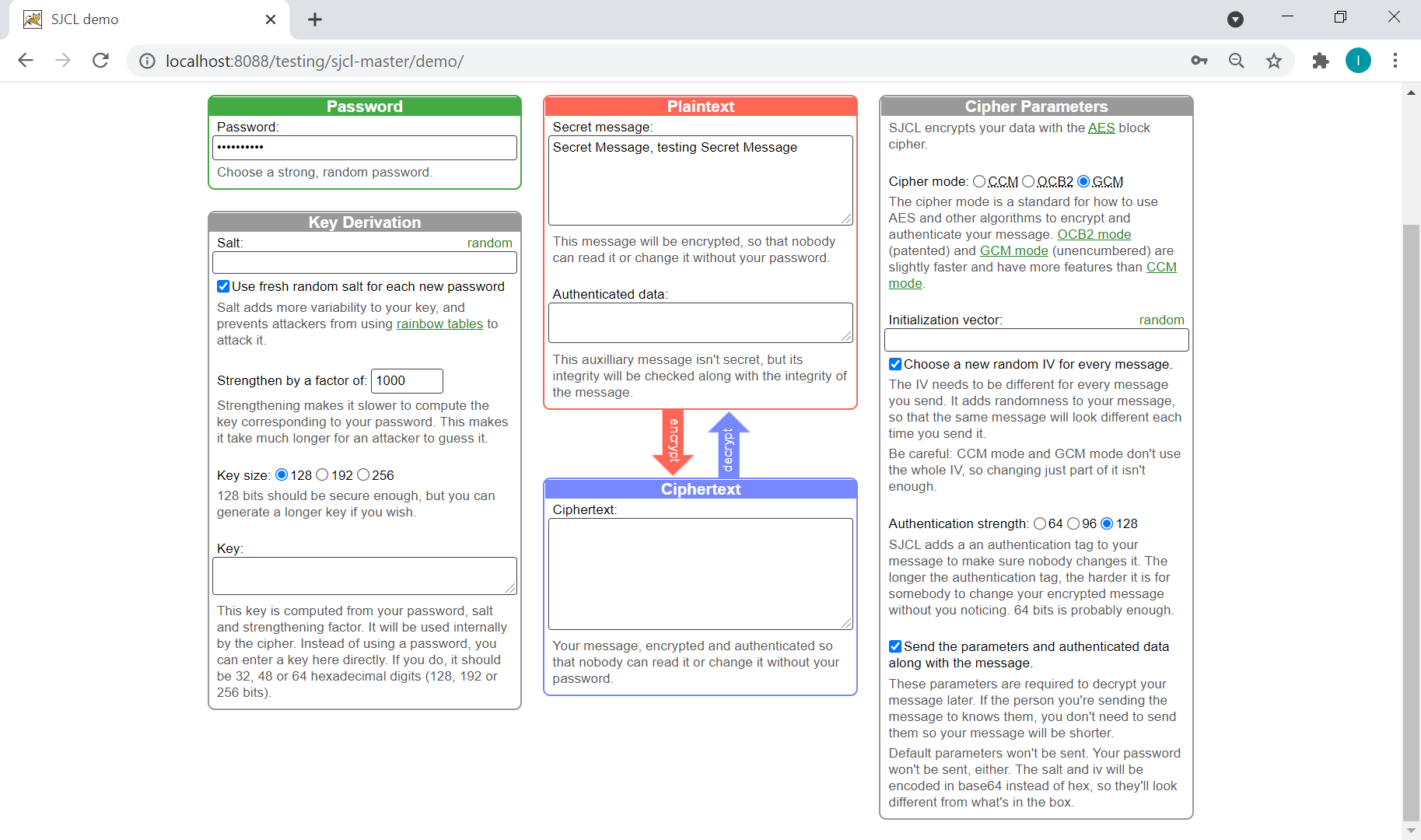
Source Location Path:

core-java-master\java-crypto\src\main\java\com\mkyong\crypto\encryptor\SJCLDecryptTest.java

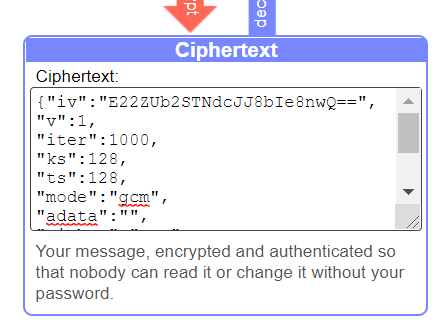


Encryption Procedure:

|  |  |
| --- | --- |
|  | Input Value |
| Password | encryption |
| Cipher Mode | GCM |
| Authentication Strength | 128 |
| Secret Message | Secret Message, testing Secret Message |



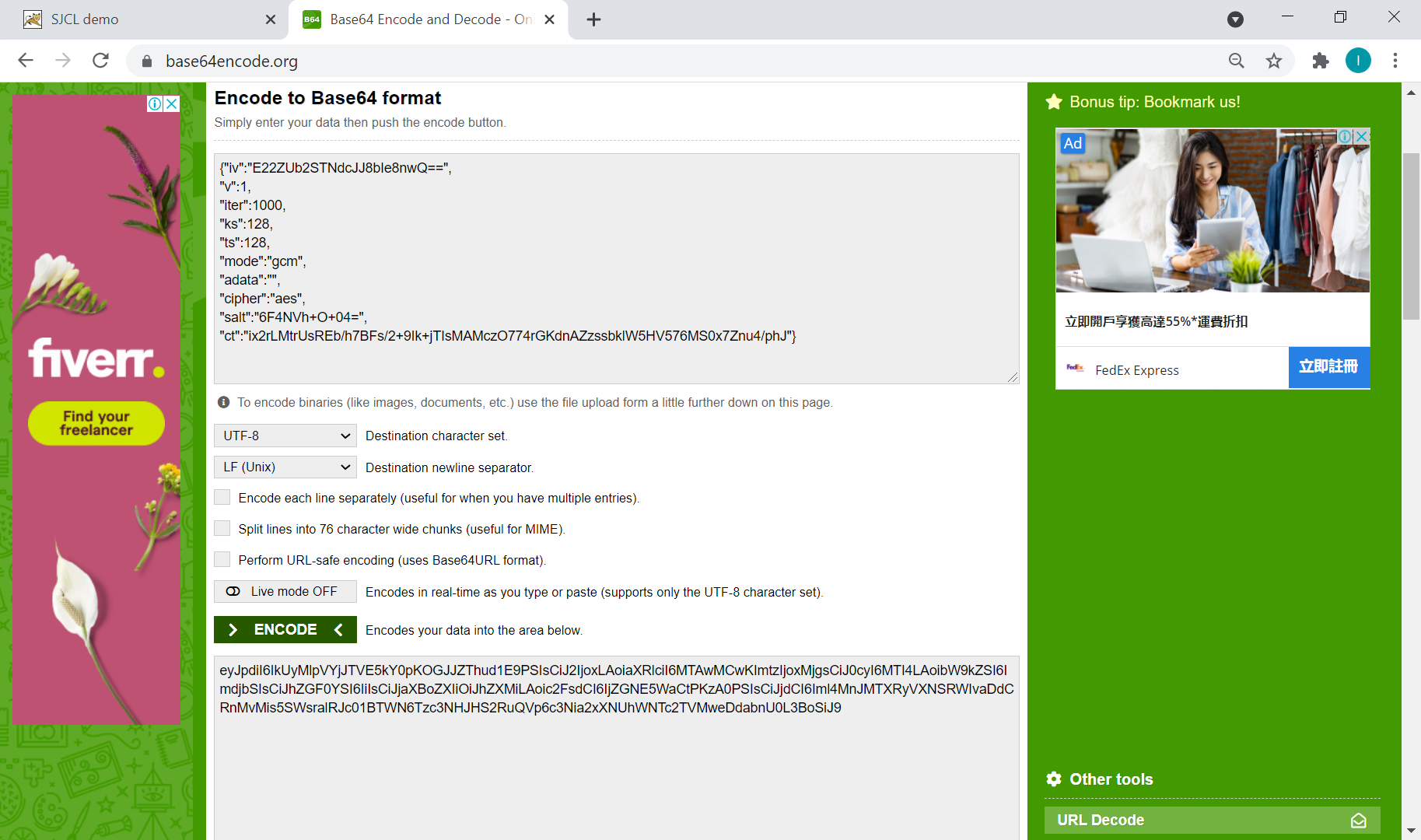
Encryption Output:



|  |  |
| --- | --- |
|  | Encryption Json Output |
| Text Format | {"iv":"E22ZUb2STNdcJJ8bIe8nwQ==",  "v":1,  "iter":1000,  "ks":128,  "ts":128,  "mode":"gcm",  "adata":"",  "cipher":"aes",  "salt":"6F4NVh+O+04=",  "ct":"ix2rLMtrUsREb/h7BFs/2+9Ik+jTIsMAMczO774rGKdnAZzssbklW5HV576MS0x7Znu4/phJ"} |
| Base64 Format | eyJpdiI6IkUyMlpVYjJTVE5kY0pKOGJJZThud1E9PSIsCiJ2IjoxLAoiaXRlciI6MTAwMCwKImtzIjoxMjgsCiJ0cyI6MTI4LAoibW9kZSI6ImdjbSIsCiJhZGF0YSI6IiIsCiJjaXBoZXIiOiJhZXMiLAoic2FsdCI6IjZGNE5WaCtPKzA0PSIsCiJjdCI6Iml4MnJMTXRyVXNSRWIvaDdCRnMvMis5SWsralRJc01BTWN6Tzc3NHJHS2RuQVp6c3Nia2xXNUhWNTc2TVMweDdabnU0L3BoSiJ9 |

Encode SJCL Output to Base64 format

<https://www.base64encode.org/>



Decryption Procedure:

|  |
| --- |
| Replace Base64 format content(First Param) and Password (Second Param) |
| System.***out***.println(**new** SJCLDecryptTest().decrypt("eyJpdiI6IkUyMlpVYjJTVE5kY0pKOGJJZThud1E9PSIsCiJ2IjoxLAoiaXRlciI6MTAwMCwKImtzIjoxMjgsCiJ0cyI6MTI4LAoibW9kZSI6ImdjbSIsCiJhZGF0YSI6IiIsCiJjaXBoZXIiOiJhZXMiLAoic2FsdCI6IjZGNE5WaCtPKzA0PSIsCiJjdCI6Iml4MnJMTXRyVXNSRWIvaDdCRnMvMis5SWsralRJc01BTWN6Tzc3NHJHS2RuQVp6c3Nia2xXNUhWNTc2TVMweDdabnU0L3BoSiJ9", "encryption")); |

Right Click -> SJCLDecrypTest.java -> Run As -> Java Application

