**EXPERIMENT NUMBER 5**

| Name of Student: Sangeet Agrawal | PRN: 21070122140 | Section: CS-B3 |
| --- | --- | --- |

**Title:** Symmetric and Asymmetric Key Encryption - DES, Triple DES and RSA.

**Aim:** Study, understand and demonstrate symmetric key algorithms

**Objective:** To make students understand and demonstrate various symmetric encryption algorithms.

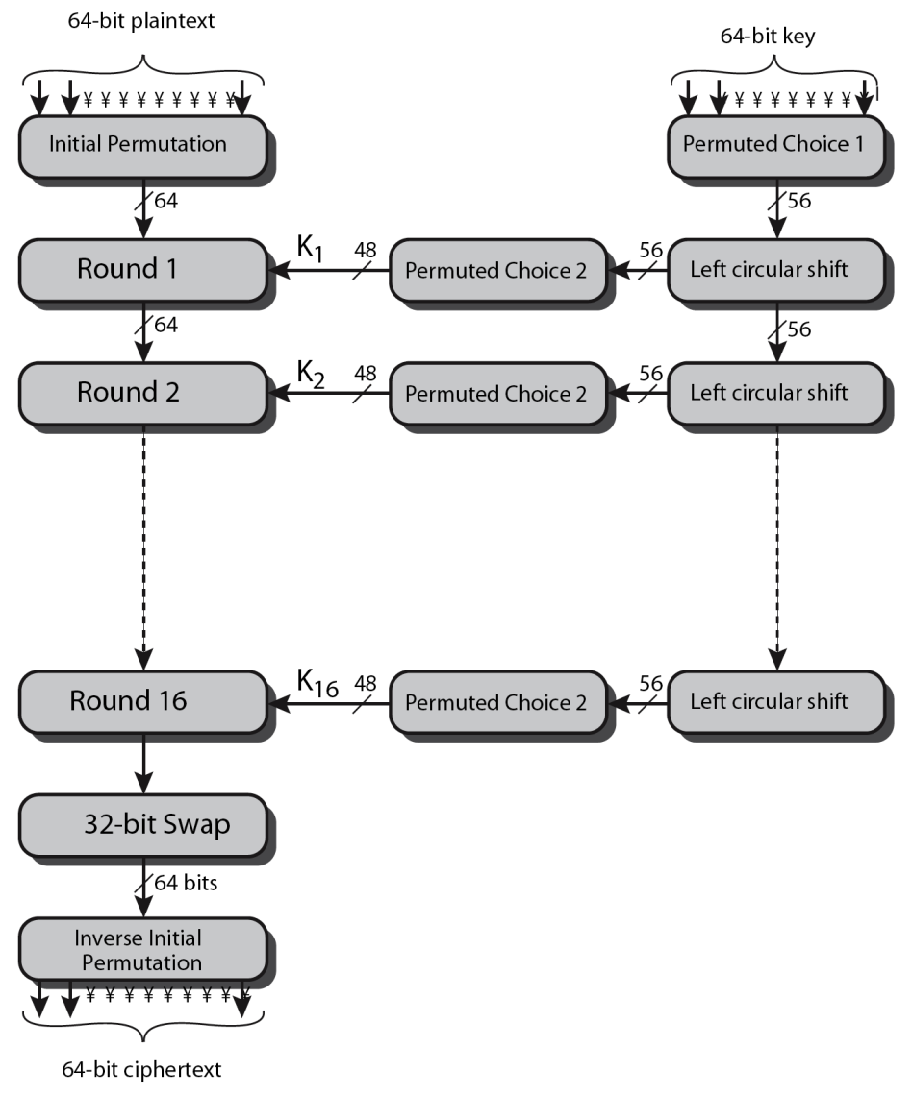
**Theory:**

**The Data Encryption Standard (DES) [Source: Cryptography and Network Security by Stallings]**

* most widely used block cipher in world
* adopted in 1977 by NBS (now NIST)
* as FIPS PUB 46
* encrypts 64-bit data using 56-bit key
* has been considerable controversy over its security
* has widespread use

**DES History:**

* IBM developed Lucifer cipher
* by team led by Feistel in late 60’s
* used 64-bit data blocks with 128-bit key
* then redeveloped as a commercial cipher with input from NSA and others
* in 1973 NBS issued request for proposals for a national cipher standard
* IBM submitted their revised Lucifer which was eventually accepted as the DES



**Figure: DES Encryption Overview**

**TDES / 3DES / 3-DES:**

* 3DES cipher was developed because DES encryption, invented in the early 1970s and protected by a 56-bit key, turned out to be too week and easy to break using modern computers of that time. The effective security which 3DES provides is 112 bits, when an attacker uses meet-in-the-middle attacks.
* For several years, TripleDES was of used for electronic payments (for example, in EMV standard). New protocols based on the cipher are still being created and maintained.

**Algorithm –3DES**

* The encryption-decryption process is as follows –
* Encrypt the plaintext blocks using single DES with key K1.
* Now decrypt the output of step 1 using single DES with key K2.
* Finally, encrypt the output of step 2 using single DES with key K3.
* The output of step 3 is the ciphertext.
* Decryption of a ciphertextis a reverse process. User first decrypt using K3,then encrypt with K2,and finally decrypt with K1.

**RSA by Rivest, Shamir & Adleman of MIT in 1977**

* best known & widely used public-key scheme
* based on exponentiation in a finite (Galois) field over integers modulo a prime
* uses large integers (eg. 1024 bits)
* security due to cost of factoring large numbers

**RSA Key Setup**

* each user generates a public/private key pair by:
* selecting two large primes at random - p, q
* computing their system modulus N=p.q
  + note ø(N)=(p-1)(q-1)
* selecting at random the encryption key e
  + - where 1<e<ø(N), gcd(e,ø(N))=1
* solve following equation to find decryption key d
  + e.d=1 mod ø(N) and 0≤d≤N
* publish their public encryption key: KU={e,N}
* keep secret private decryption key: KR={d,p,q}

**Tools to be practiced:**

1. BitLocker
2. VeraCrypt
3. DiskCryptor
4. FileVault 2
5. SensiGuard
6. Challenger
7. CyberGhost
8. Assignment from Cryptography Virtual Lab (website link 5)

**Reference web links:**

1. <https://www.encryption-software.de>
2. <https://www.comparitech.com/blog/vpn-privacy/encrypt-windows-files/>
3. <https://www.youtube.com/watch?v=9fGrzXAuZZs>
4. <https://www.youtube.com/watch?v=bTHARNVWRzU>
5. <https://cse29-iiith.vlabs.ac.in/>

**Conclusion:**

**Implementation question:**

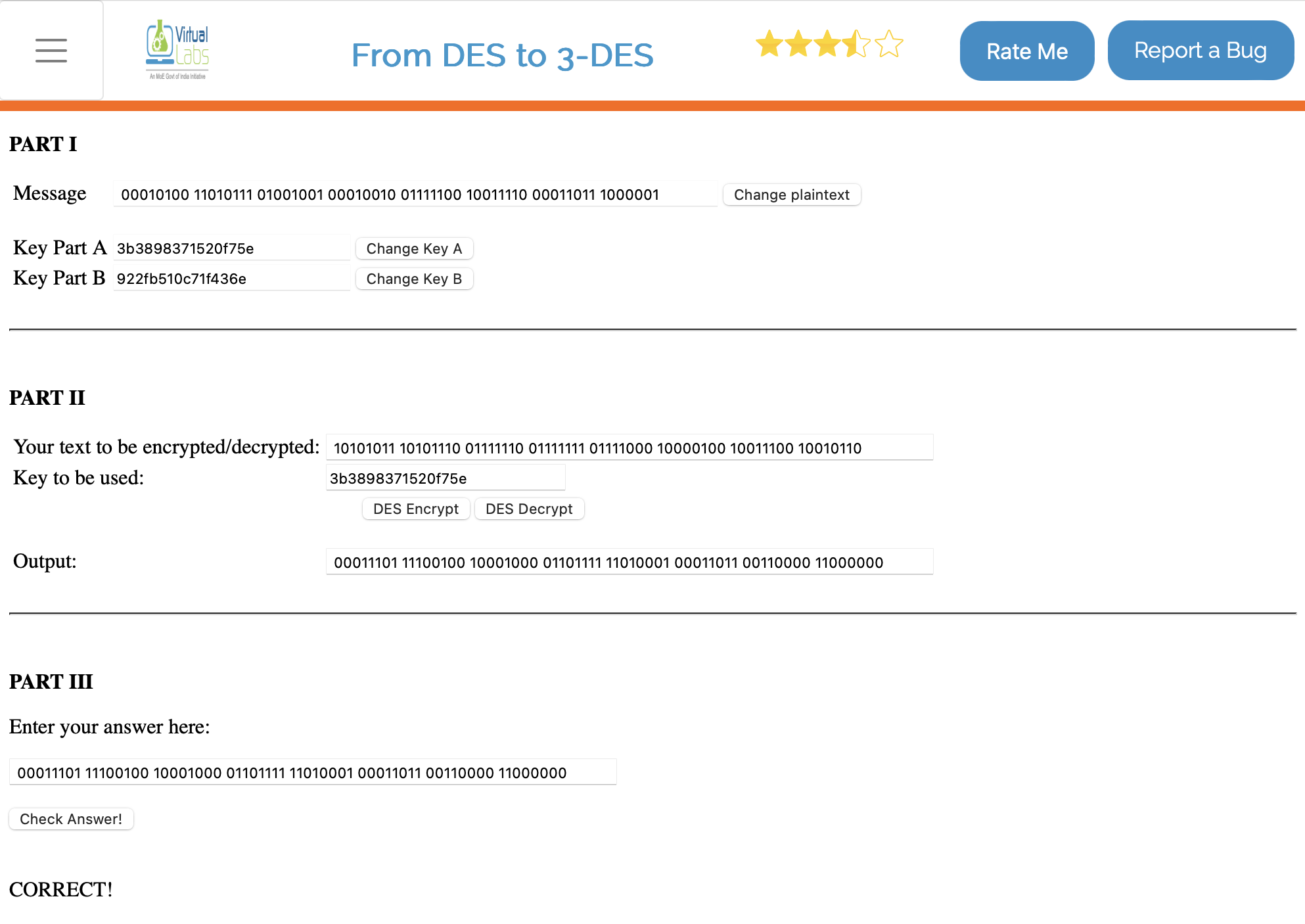
1. Study assignment 6 and assignment 7 from virtual lab-based.
2. Perform Lab 2 - page 45 from the given pdf link and share a screenshot of the completed task.
3. Perform Lab 3 - page 54 from the given pdf link and share a screenshot of the completed task.
4. Perform any 2 tools from lab 4 and lab 5 from the given pdf link and share a screenshot of the completed task.
5. Differentiate between DES and 3-DES.

PDF link: <https://drive.google.com/file/d/1wuPDiV500JD8CgFPVAgnXx5Qc3JVtSsm/view?usp=sharing>

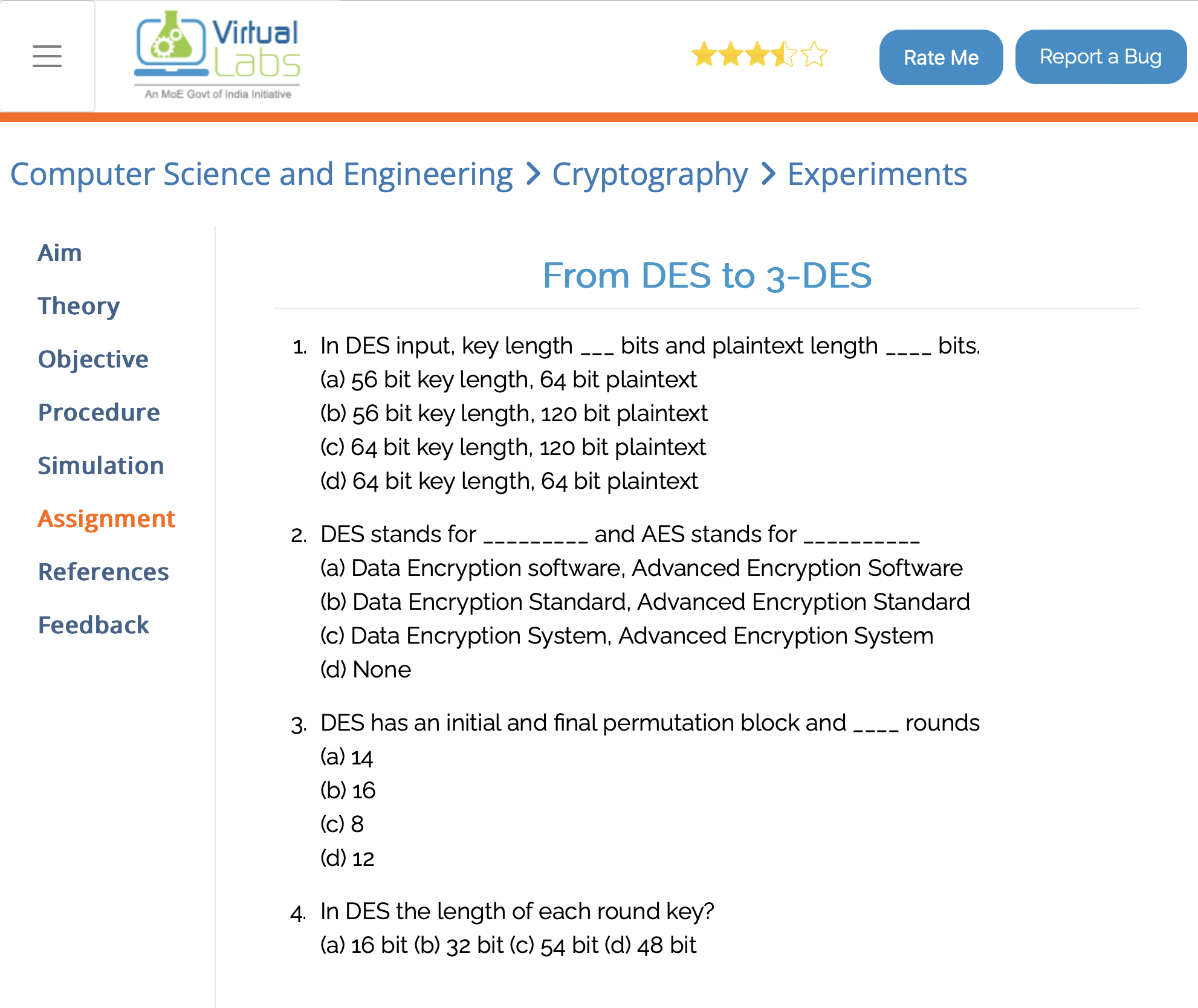
**Note:** Students are suggested to use Linux OS-based tools or free Windows OS-based tools.

**Screenshots:**

VLab - Exp 6 - Simulation



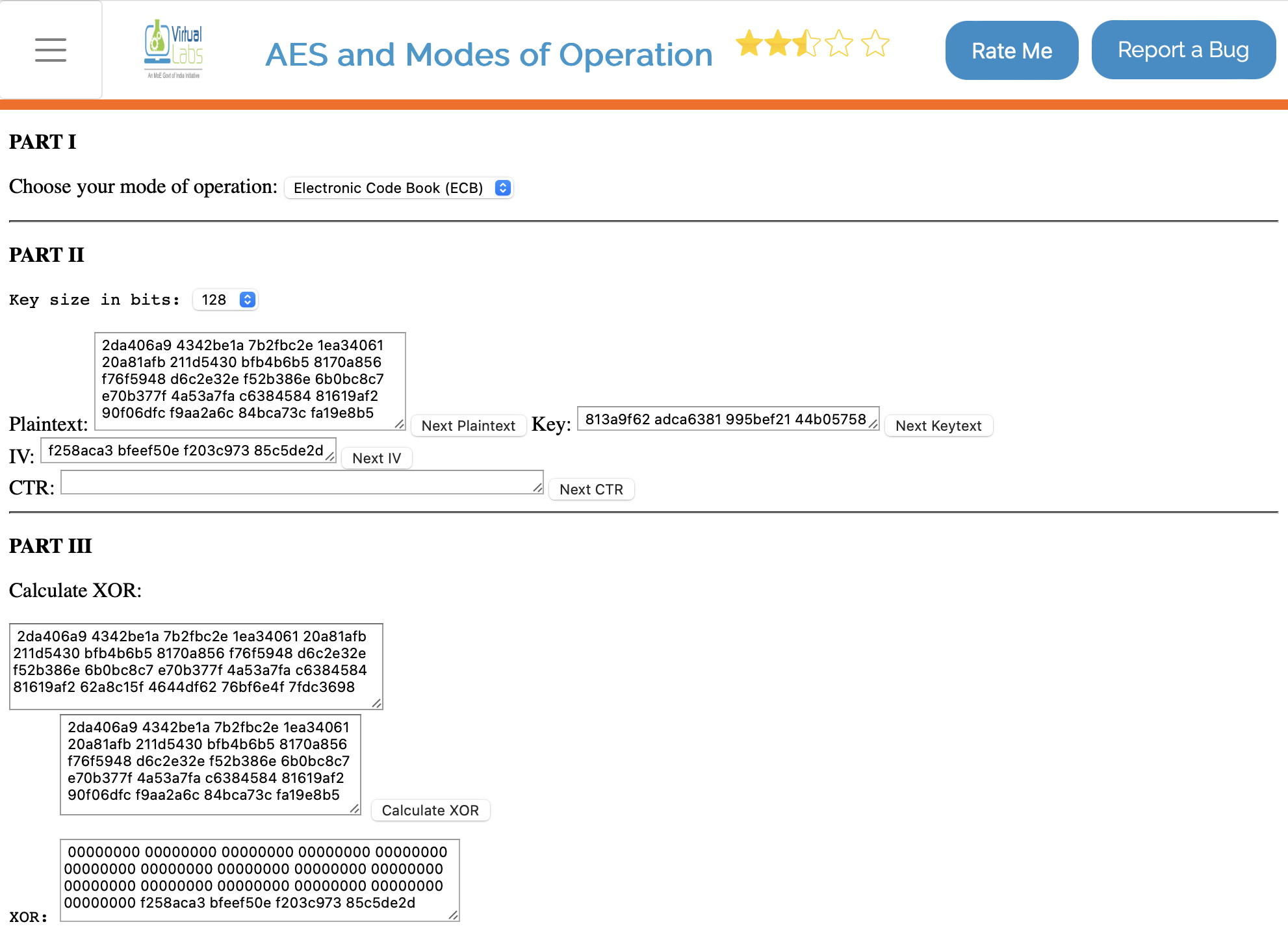
VLab - Exp 6 - Assignment Questions

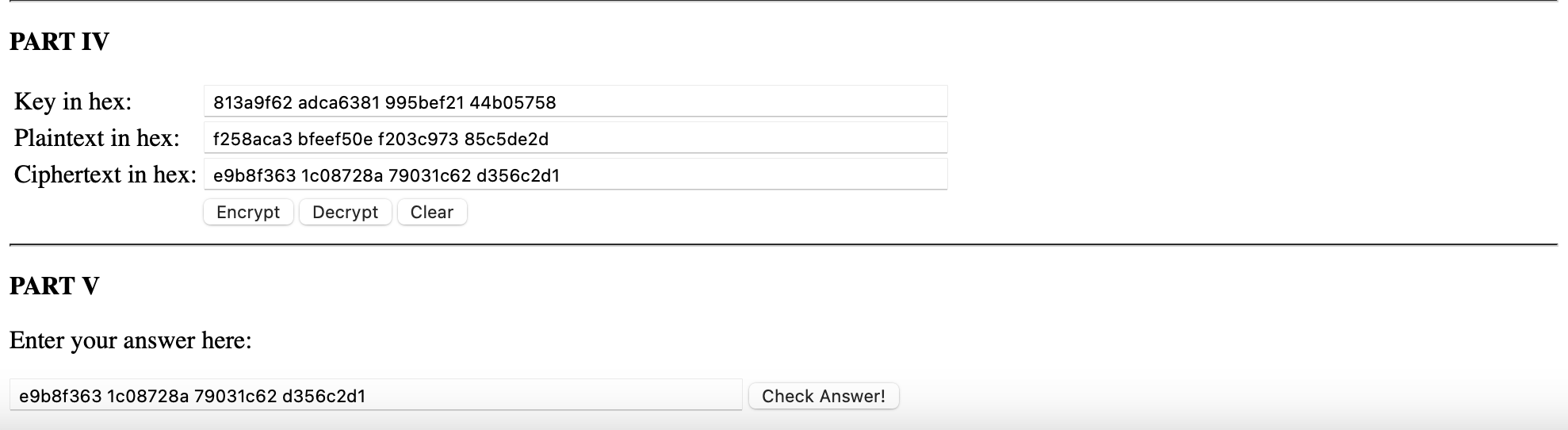


VLab - Exp 6 - Assignment Answers

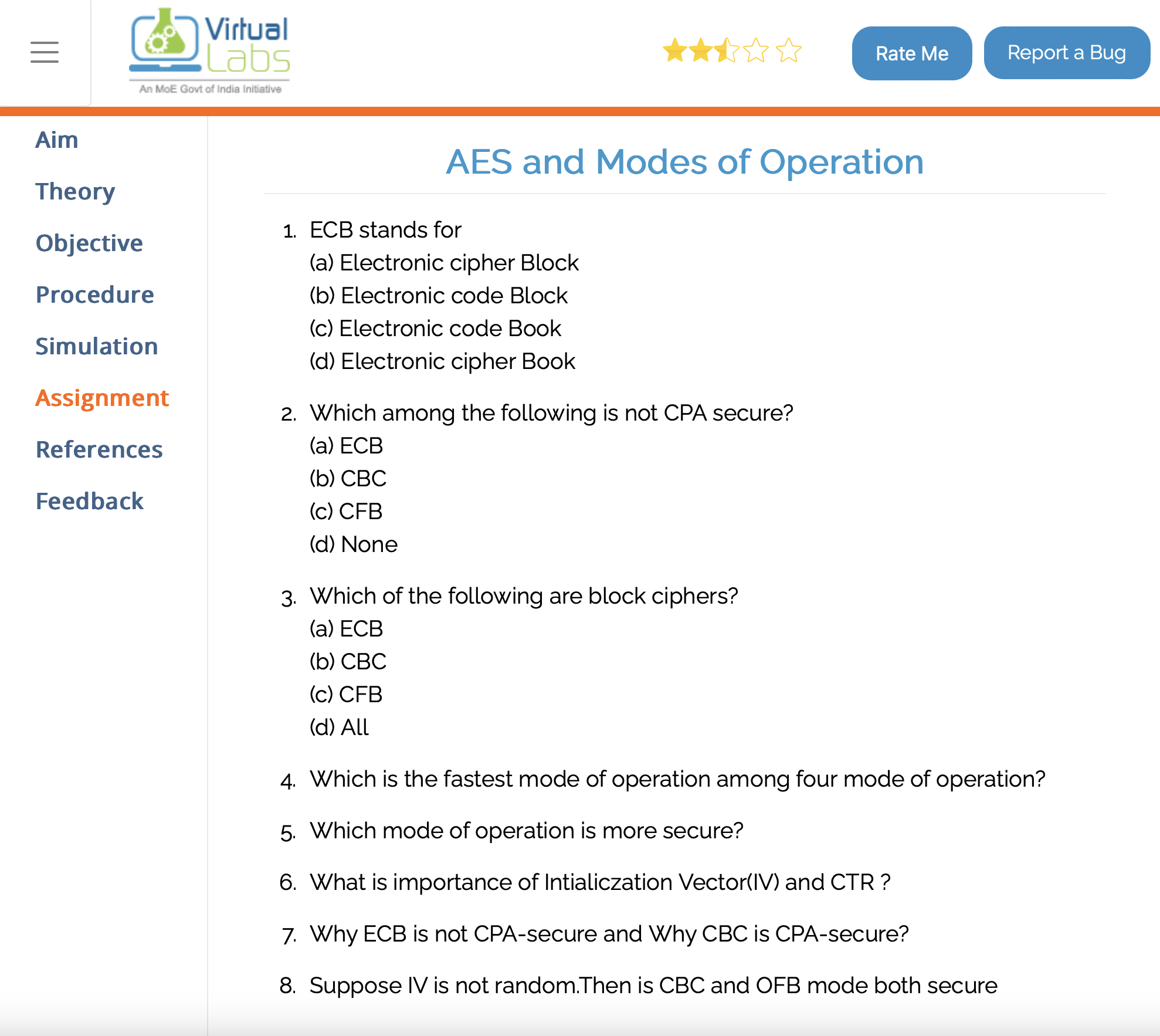
1. (a) 56 bit key length, 64 bit plaintext
2. (b) Data Encryption Standard, Advanced Encryption Standard
3. (b) 16
4. (d) 48 bit

VLab - Exp 7 - Simulation





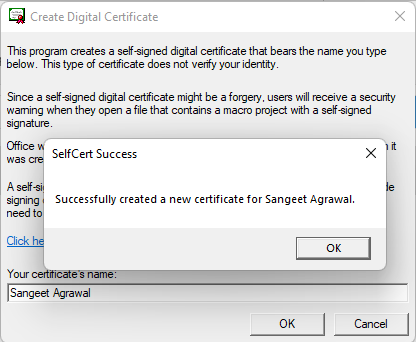
VLab - Exp 7 - Assignment Questions

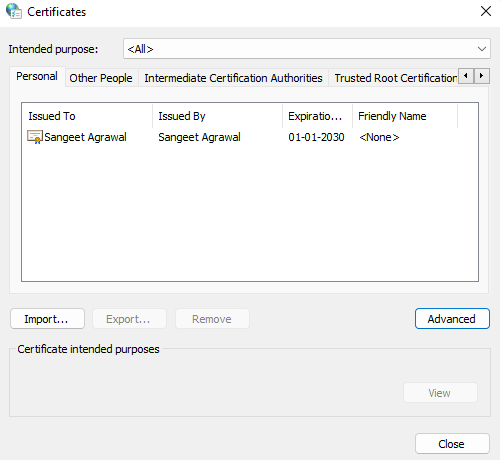


VLab - Exp 7 - Assignment Answers

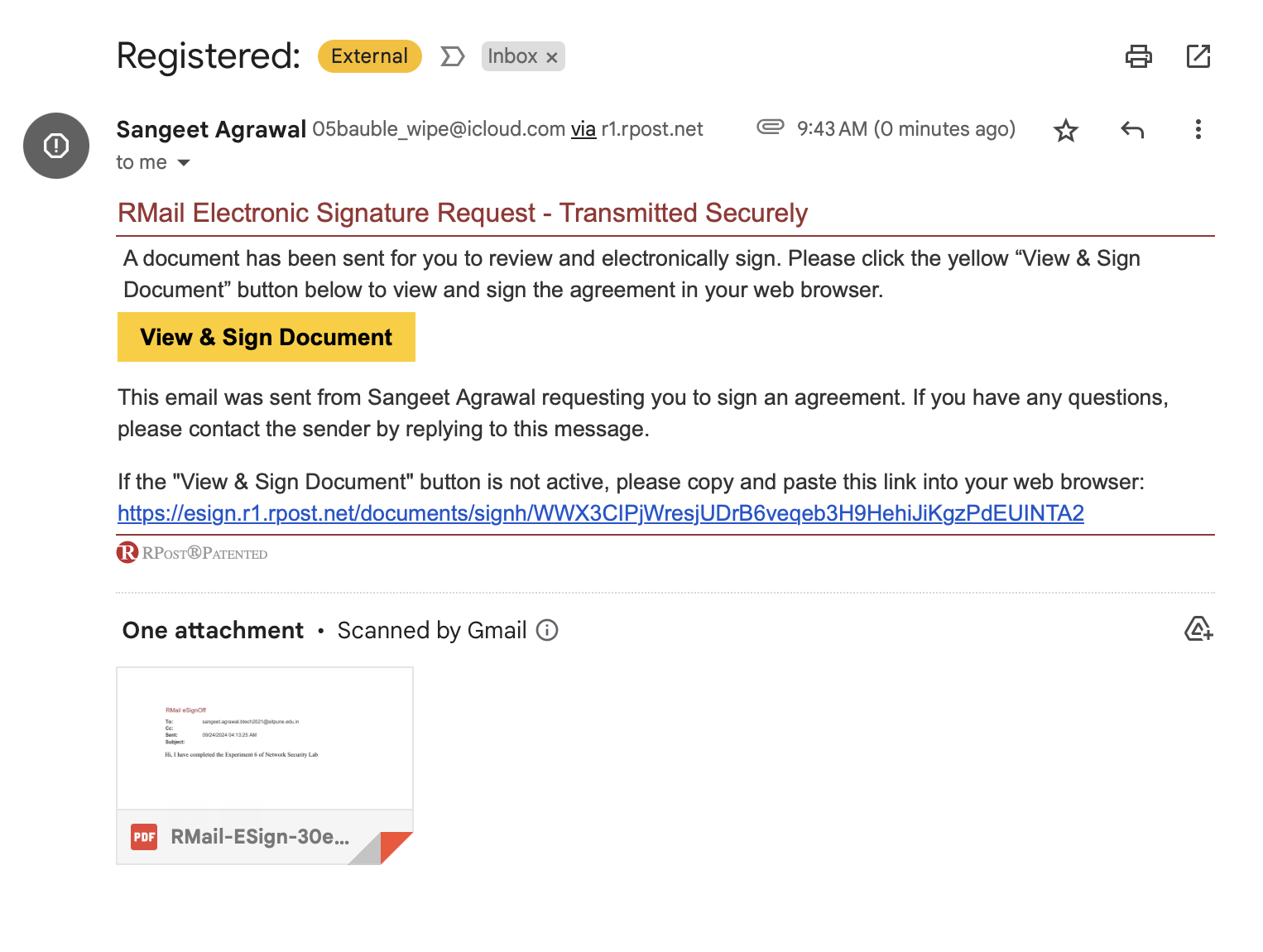
1. (c) Electronic Code Book
2. (a) ECB
3. (d) All (ECB, CBC, CFB are block cipher modes.)
4. ECB is the fastest because it encrypts each block independently without additional computations.
5. CBC and CTR are more secure due to chaining and randomization, which prevent pattern recognition.
6. IV ensures different ciphertexts for identical plaintexts by adding randomness, preventing patterns and replay attacks.
7. ECB is not CPA-secure because it encrypts identical blocks the same way. CBC is CPA-secure because it XORs each block with the previous ciphertext, hiding patterns.
8. No. A non-random IV makes CBC and OFB insecure as it can lead to predictable patterns, compromising encryption.

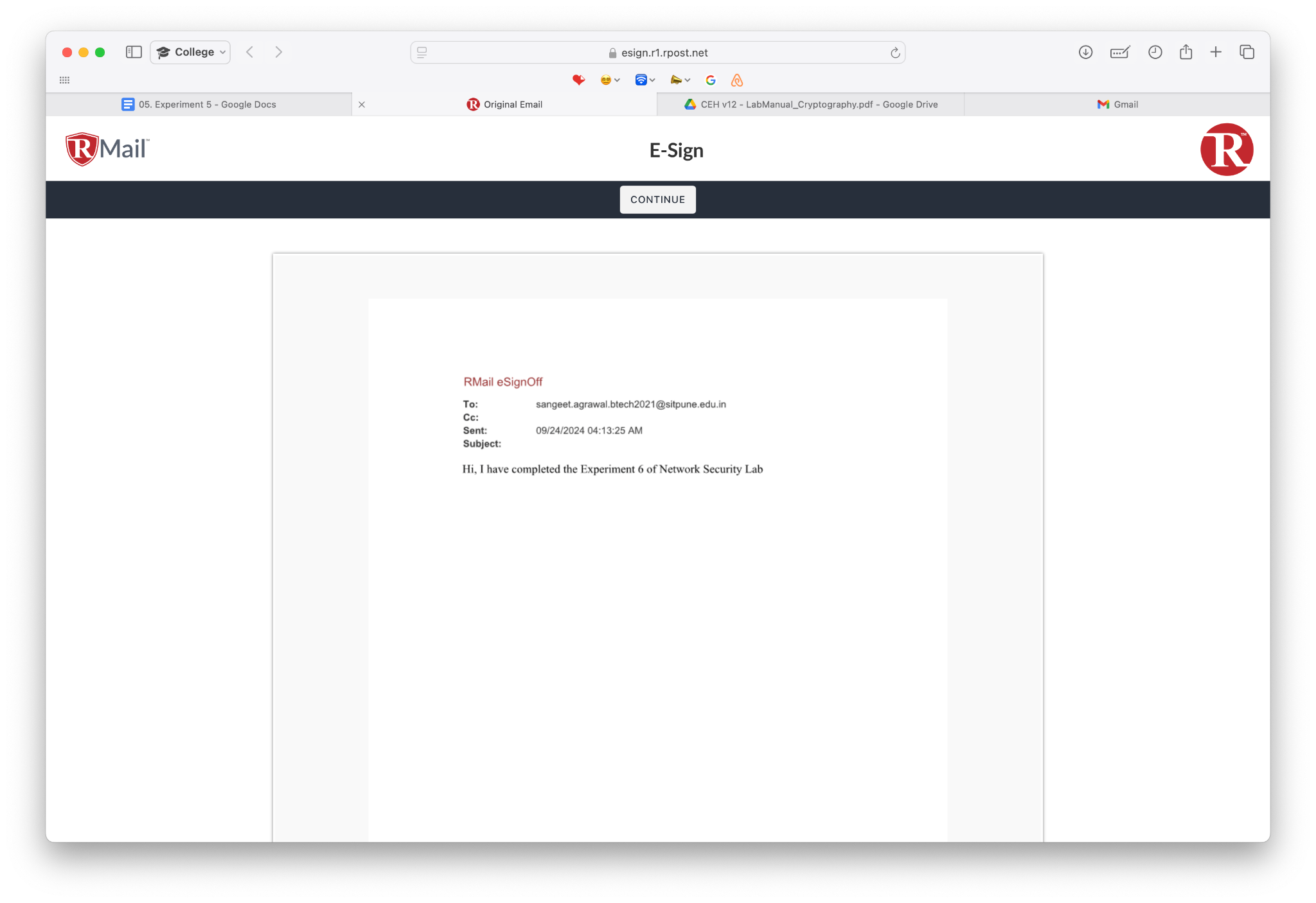
Performing Lab 2 - page 45 from the given pdf link

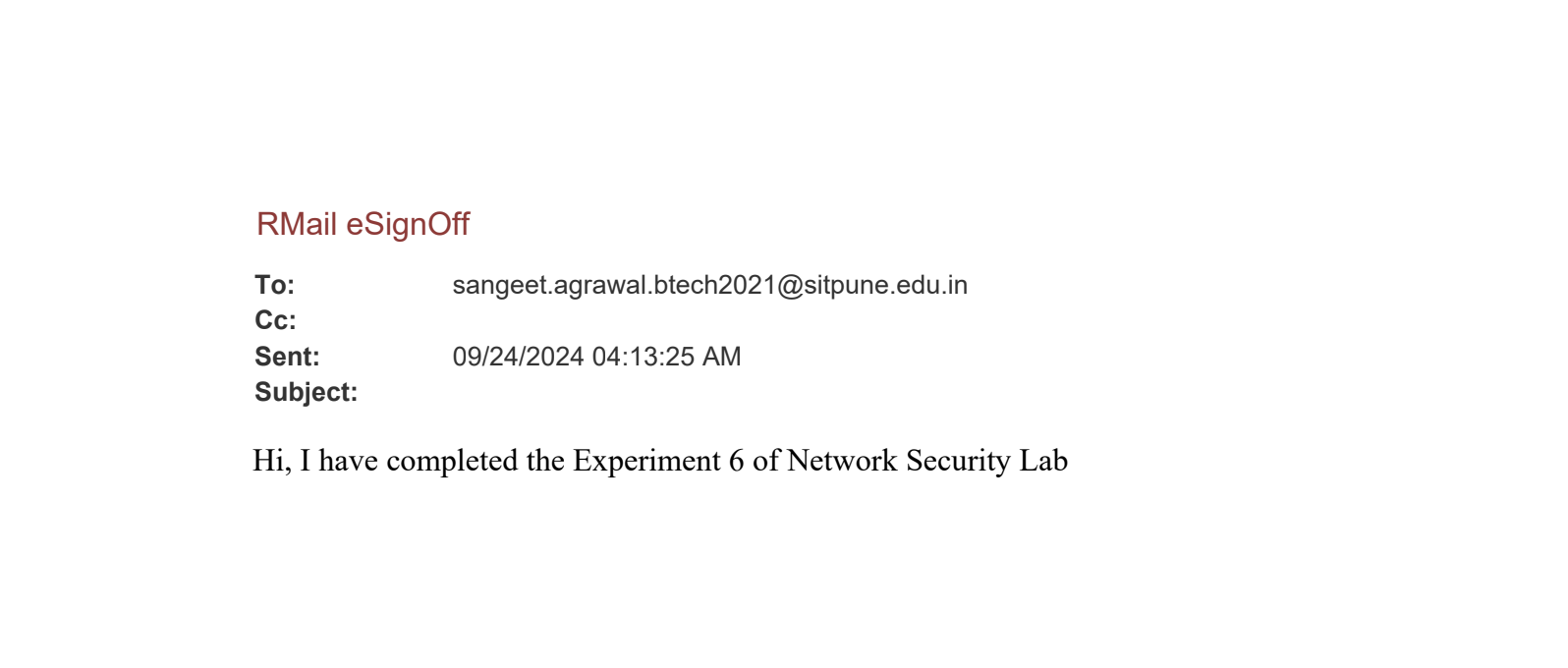




Performing Lab 3 - page 54 from the given pdf link

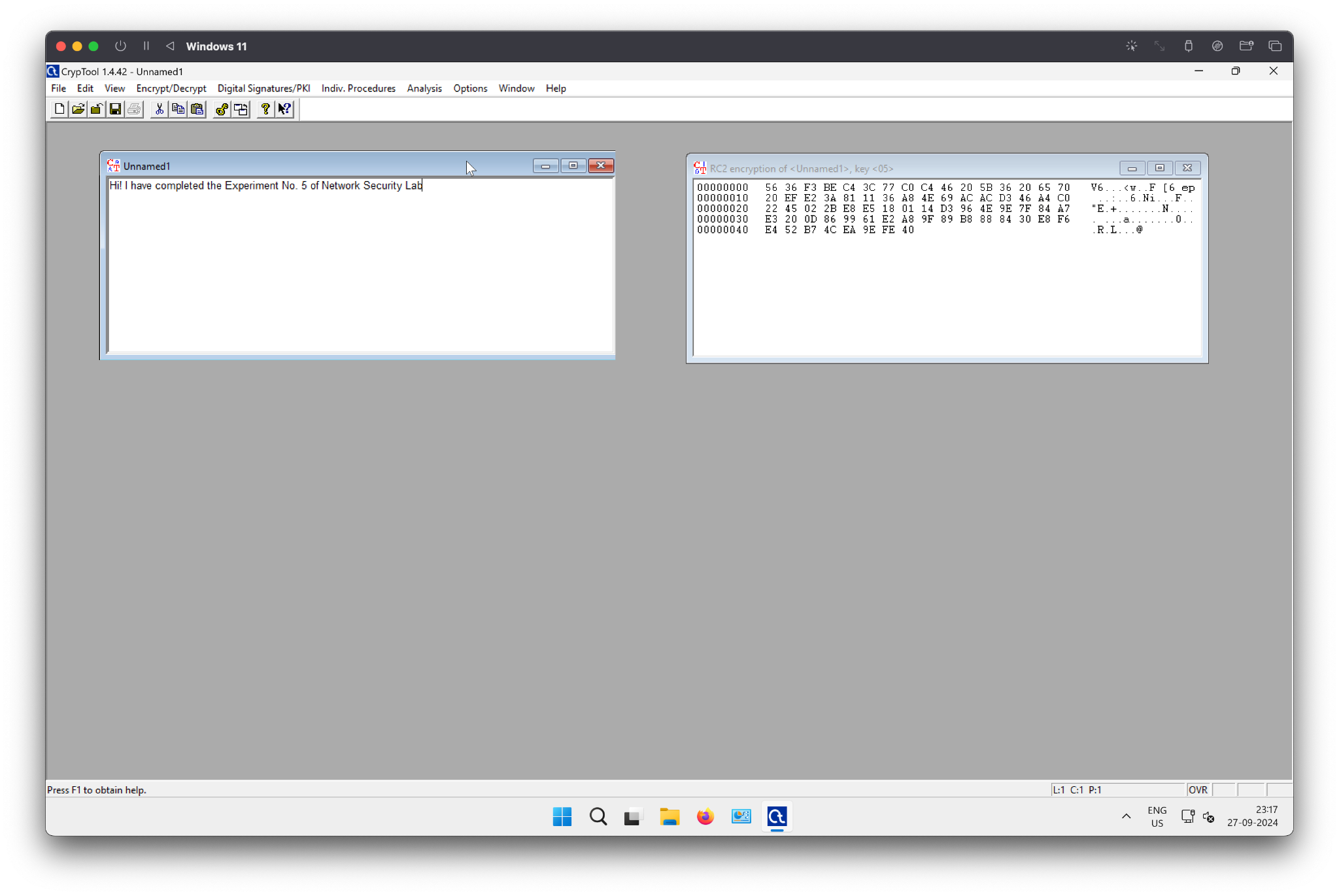


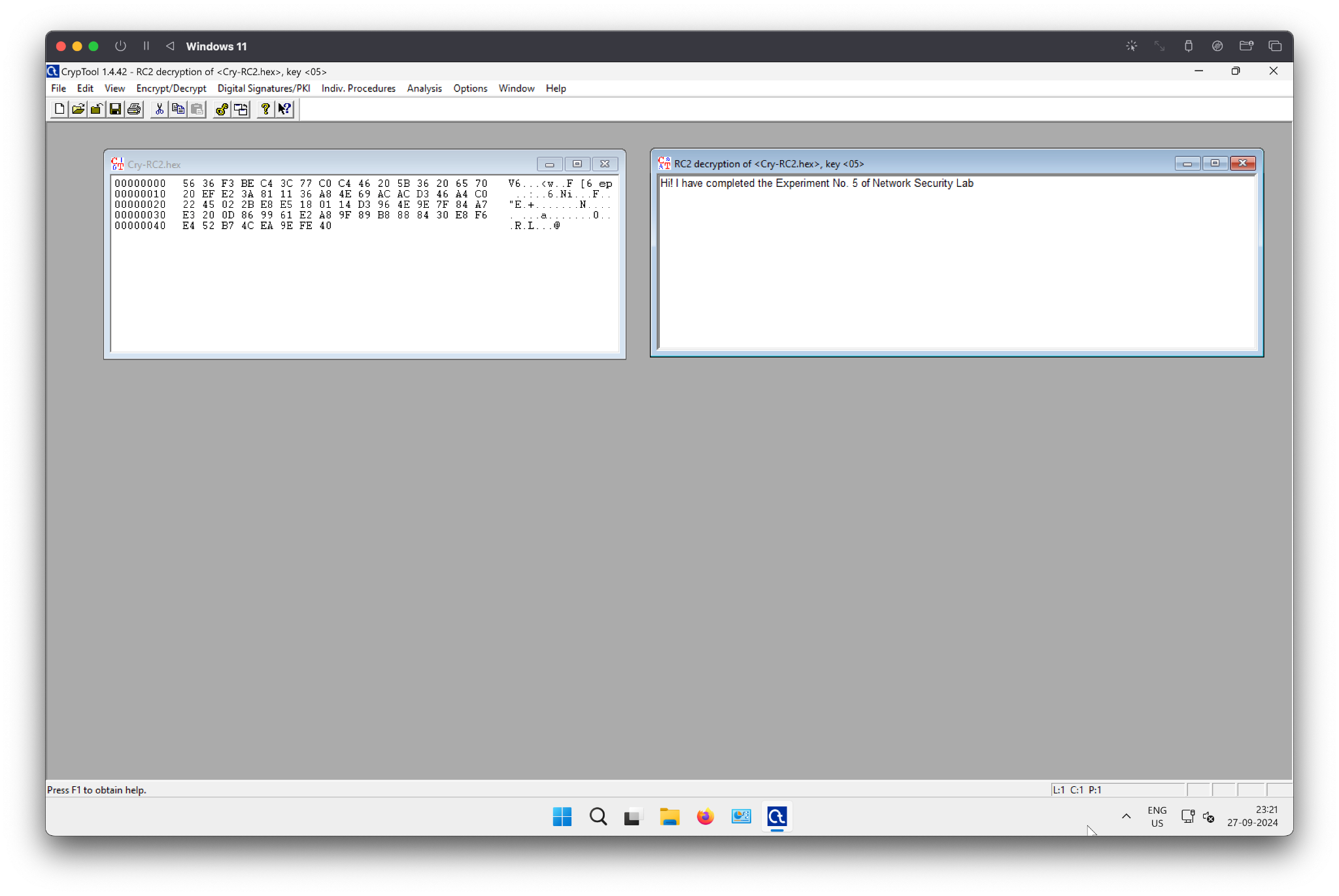


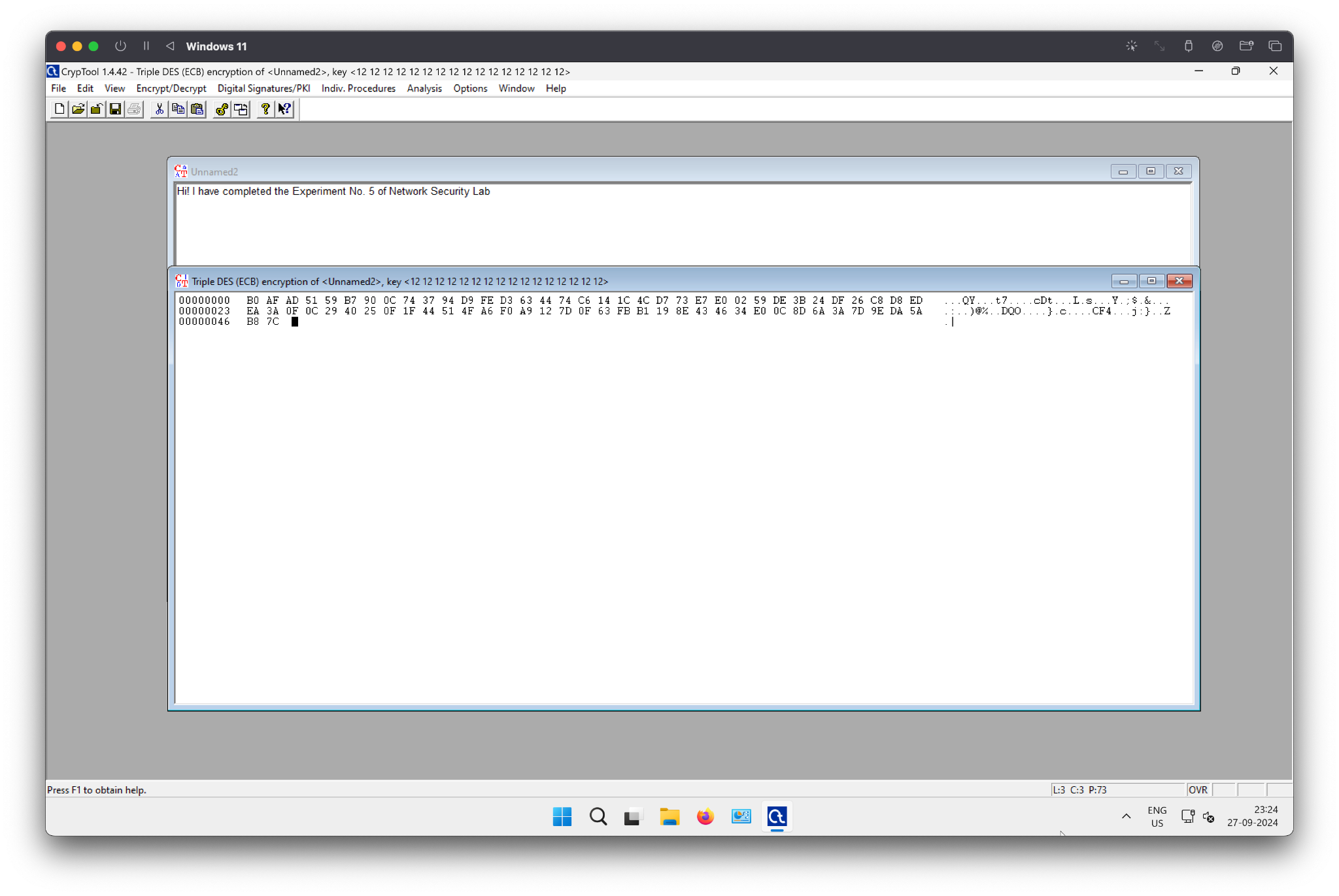


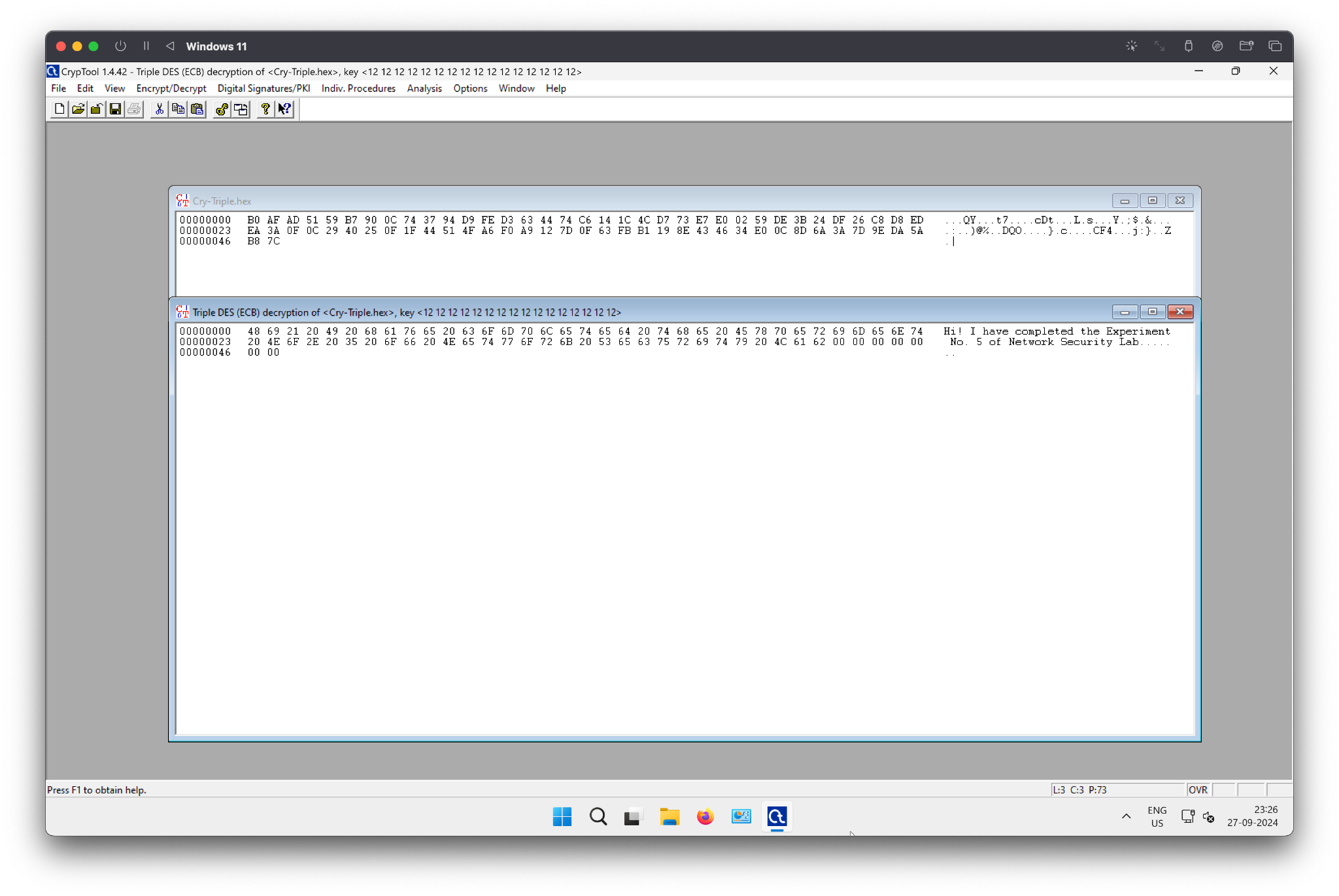
Performing any 2 tools from lab 4 and lab 5:

1. Cryptool

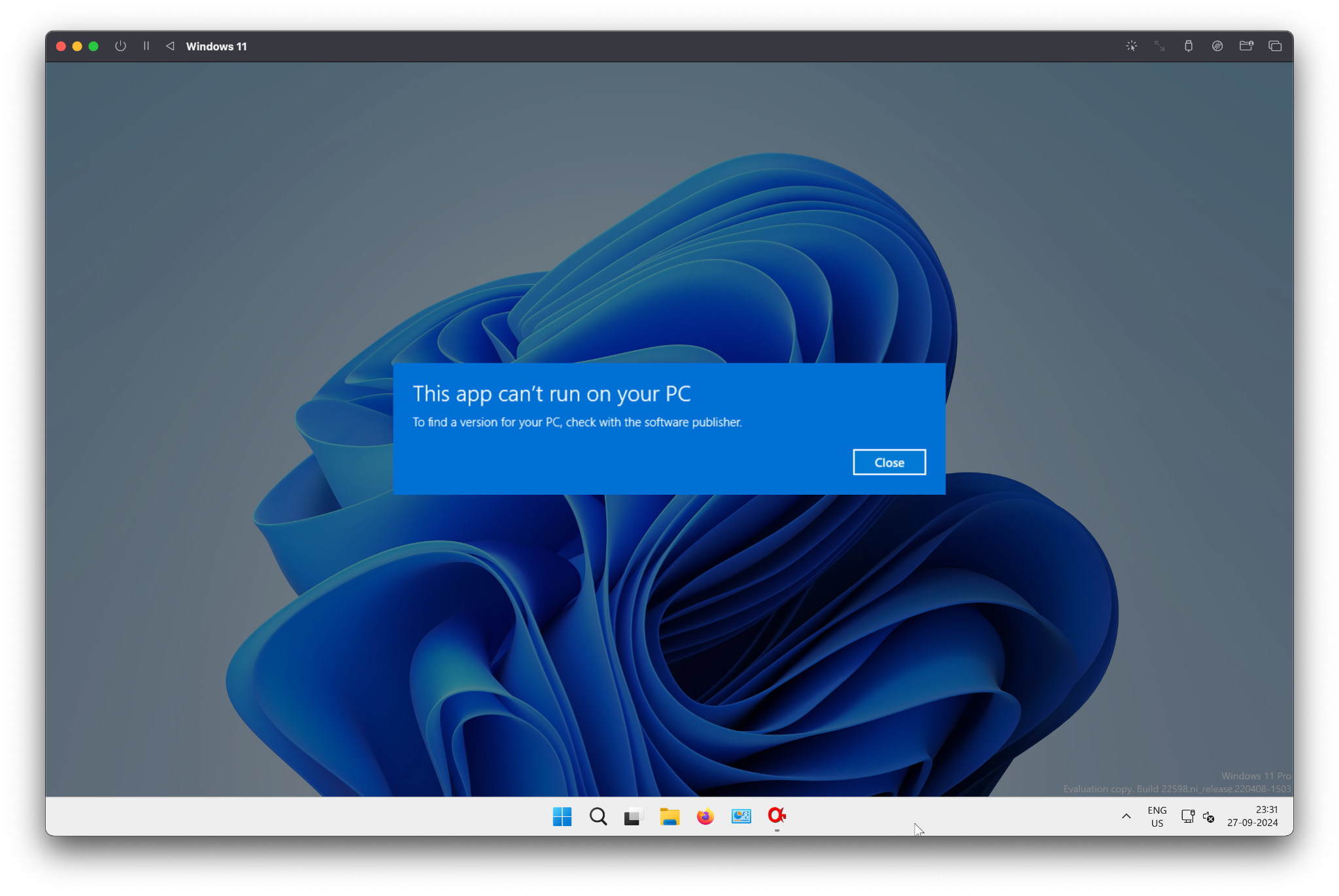








1. AlphaPeeler: The software isn't compatible to use on a Windows 11 VM.



Differentiate between DES and 3-DES:

| **Features** | **DES (Data Encryption Standard)** | **3-DES (Triple DES)** |
| --- | --- | --- |
| **Key Length** | Uses a 56-bit key for encryption. | Uses three 56-bit keys, making the total key length 168 bits. |
| **Rounds** | Performs 16 rounds of encryption. | Performs 48 rounds of encryption (16 rounds repeated three times). |
| **Security Level** | Considered insecure today due to the short key length. | More secure than DES, but still outdated compared to modern algorithms. |
| **Process** | Operates with a single encryption process. | Uses the Encrypt-Decrypt-Encrypt process by applying DES three times with different keys. |
| **Speed** | Faster compared to 3-DES since it requires fewer operations. | Slower due to the triple encryption process. |
| **Vulnerability** | Vulnerable to brute-force attacks. | Less vulnerable to brute-force attacks, but newer standards like AES are preferred. |
| **Usage** | Rarely used today due to better alternatives. | Still used in some legacy systems. |