Report on Observations and Findings:

Task 1: Image Encryption Using Different AES Modes

Encrypting an image using four different AES mode (ECB, CBC, CFB, OFB) with each mode resulting in different encrypted files.

ECB mode encrypts blocks independently, which may result in patterns (outline) if the image has repetitive content like solid colors. Output Image Comparison:

CBC, CFB, and OFB modes use an initialization vector (IV) to provide better security by introducing randomness as observed from the NIST analysis tool.

> Note: The same "Initial Vector" (IV) has been used with these different encryptions modes which can be a security risk. The IV should be unique for each encryption to ensure the security of the encrypted data.

Encryption Script

A script was used to perform the image encryption with each AES mode. It uses the BMP format because it has a static 54 byte header which makes it easier to strip and combine with the encrypted image to help show the effects of encryption (and its strengths).

Create a 128-bit key for encryption:

```
key=$(openssl rand -hex 16)
```

Strip the BMP header from the image body before encryption (does not affect the encryption):

```
tail -c +55 "$image_path" > "$body_file"
head -c $header_size "$image_path" > "$header_file"
```

Encrypt the image using multiple encryption modes:

```
openssl enc -aes-128-cbc -in "$body_file" -out "$cbc_encryption" -K "$key" -iv "$iv"
openssl enc -aes-128-cfb -in "$body_file" -out "$cfb_encryption" -K "$key" -iv "$iv"
openssl enc -aes-128-ofb -in "$body_file" -out "$ofb_encryption" -K "$key" -iv "$iv"
openssl enc -aes-128-ecb -in "$body_file" -out "$ecb_encryption" -K "$key"
```

Combine the striped header with the encrypted body to produce a viewable image:

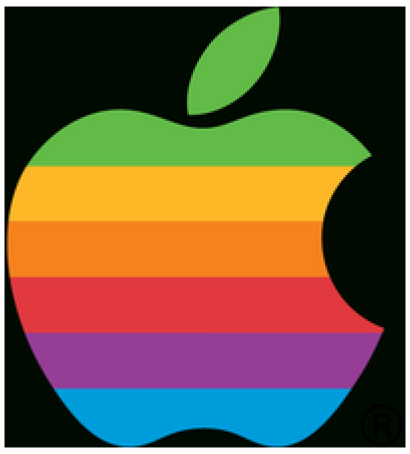
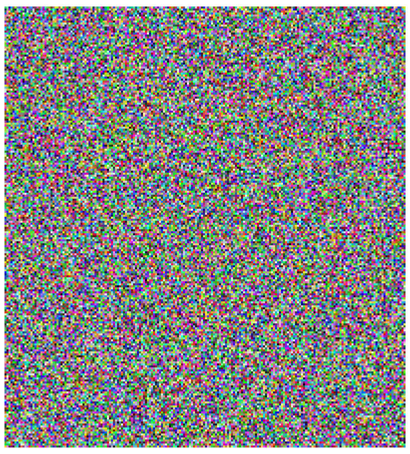
```
cat "$header_file" "$ecb_encryption" > "$ecb_encrypted_image"
cat "$header_file" "$cbc_encryption" > "$cbc_encrypted_image"
cat "$header_file" "$cfb_encryption" > "$cfb_encrypted_image"
cat "$header_file" "$ofb_encryption" > "$ofb_encrypted_image"
```

Loop through the encrypted files to write the binary data into a text file for analysis using NIST's Statistical Analysis Tool: (using xxd)

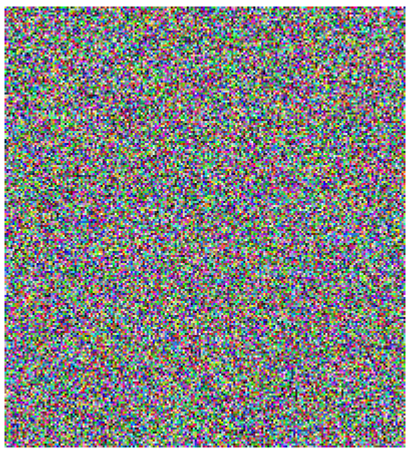
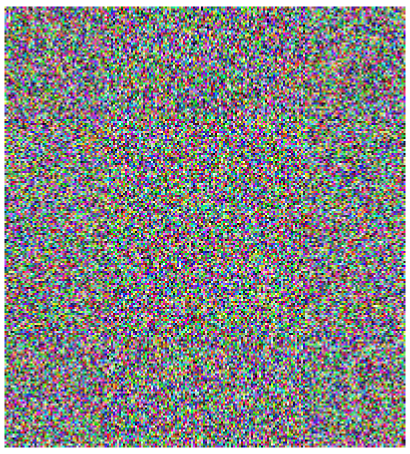
```
for file in "${out_folder}"/*.bin; do
    xxd -b -c 1 "$file" | awk '{print $2}' | tr -d '\n' > "${file}_string.bin"
done
```

Output Image Comparison

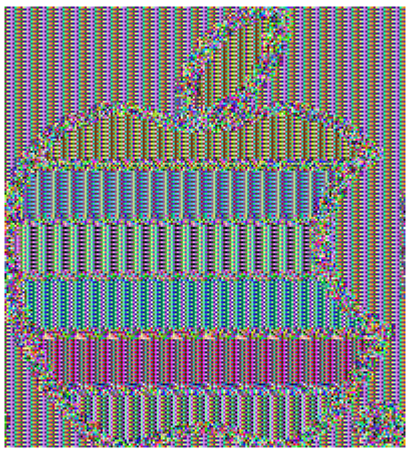
Original Image, Encrypted CBC:

 . 

Encrypted CFB, Encrypted OFB:

 . 

Encrypted ECB:



NIST's Statistical Test Suite Output Reports

Original Image Analysis

```
Test Data File:/Users/samahy/College/Computer System Security/12th_Project/Tasks/Task_1/body.bin_string.bin


Type of Test                                        P-Value                 Conclusion
01. Frequency (Monobit) Test                        0.0                     Non-Random
02. Frequency Test within a Block                   0.0                     Non-Random
03. Runs Test                                       0.0                     Non-Random
04. Test for the Longest Run of Ones in a Block     2.1622349726706396e-272 Non-Random
05. Binary Matrix Rank Test                         0.0                     Non-Random
06. Discrete Fourier Transform (Spectral) Test      0.0                     Non-Random
07. Non-overlapping Template Matching Test          0.0                     Non-Random
08. Overlapping Template Matching Test              0.0                     Non-Random
09. Maurer's "Universal Statistical" Test           0.0                     Non-Random
10. Linear Complexity Test                          0.0                     Non-Random
11. Serial Test:
                          0.0                   Non-Random
                          0.0                   Non-Random
12. Approximate Entropy Test                        0.0                     Non-Random
13. Cumulative Sums Test (Forward)                  0.0                     Non-Random
14. Cumulative Sums Test (Backward)                 0.0                     Non-Random
15. Random Excursions Test:
        State       Chi Squared             P-Value                 Conclusion
        -4          0.14285714285714285     0.9996100613790039      Random
        -3          0.2                     0.9991138612111875      Random
        -2          0.3333333333333333      0.9969687632568645      Random
        -1          1.0                     0.9625657732472964      Random
        +1          3.0                     0.6999858358786276      Random
        +2          15.0                    0.010362337915786429    Random
        +3          35.0                    1.5046506621757205e-06  Non-Random
        +4          63.0                    2.9111549198896303e-12  Non-Random
16. Random Excursions Variant Test:
        State       COUNTS                  P-Value                 Conclusion
        +1.0        1                       1.0                     Random
        +2.0        1                       1.0                     Random
        +3.0        1                       1.0                     Random
        +4.0        1                       1.0                     Random
        +5.0        1                       1.0                     Random
        +6.0        1                       1.0                     Random
        +7.0        1                       1.0                     Random
        +8.0        1                       1.0                     Random
        +9.0        1                       1.0                     Random
```

CBC Encrypted Image Analysis

```
Test Data File:/Users/samahy/College/Computer System
Security/12th_Project/Tasks/Task_1/encrypted_cbc.bin_string.bin


Type of Test                                        P-Value                  Conclusion
01. Frequency (Monobit) Test                        0.4690657350724339      Random
02. Frequency Test within a Block                   0.5598346139293857      Random
03. Runs Test                                       0.7960022885972252      Random
04. Test for the Longest Run of Ones in a Block     0.2723508760326977      Random
05. Binary Matrix Rank Test                         0.6620372427863827      Random
06. Discrete Fourier Transform (Spectral) Test      0.07808402552460242     Random
07. Non-overlapping Template Matching Test          0.4982636600954635      Random
08. Overlapping Template Matching Test              0.01557209779579732     Random
09. Maurer's "Universal Statistical" Test           0.37944591351300916     Random
10. Linear Complexity Test                          0.4509529012654798      Random
11. Serial Test:
                          0.6461155218258582    Random
                          0.6842411613853814    Random
12. Approximate Entropy Test                        0.7610955670663094      Random
13. Cumulative Sums Test (Forward)                  0.5065011877133156      Random
14. Cumulative Sums Test (Backward)                 0.6550124347957142      Random
15. Random Excursions Test:
        State       Chi Squared             P-Value                 Conclusion
        -4          5.204284304112132       0.3914613446354084      Random
        -3          1.6349429921259837      0.8969917357454221      Random
        -2          8.578516574317097       0.12710349496775594     Random
        -1          3.2566929133858267      0.6604782189081345      Random
        +1          4.462992125984252       0.4848501823624932      Random
        +2          6.2845533197239245      0.2795069636346506      Random
        +3          5.151793385826775       0.3976375752674513      Random
        +4          7.076955468030054       0.21497966239407382     Random
16. Random Excursions Variant Test:
        State       COUNTS                  P-Value                 Conclusion
        -9.0        1121                    0.4733478204585916      Random
        -8.0        1063                    0.28892031579493715     Random
        -7.0        1054                    0.23456533238648147     Random
        -6.0        1160                    0.510485955372724       Random
        -5.0        1237                    0.8272258822752373      Random
        -4.0        1245                    0.8512778101237564      Random
        -3.0        1246                    0.8313538238289992      Random
        -2.0        1249                    0.809888257552402       Random
        -1.0        1241                    0.5650106971357869      Random
        +1.0        1327                    0.25806014181100834     Random
        +2.0        1394                    0.15545935064163638     Random
        +3.0        1424                    0.17177297729085883     Random
        +4.0        1371                    0.44877871695161775     Random
        +5.0        1322                    0.7309018059611239      Random
        +6.0        1310                    0.8108712172416049      Random
        +7.0        1251                    0.9167250531058815      Random
        +8.0        1160                    0.5730624164819464      Random
        +9.0        1150                    0.5636125700525985      Random
```

CFB Encrypted Image Analysis

```
Test Data File:/Users/samahy/College/Computer System
Security/12th_Project/Tasks/Task_1/encrypted_cfb.bin_string.bin


Type of Test                                        P-Value                 Conclusion
01. Frequency (Monobit) Test                        0.33705521493367574     Random
02. Frequency Test within a Block                   0.9974124747260082      Random
03. Runs Test                                       0.5073803757767417      Random
04. Test for the Longest Run of Ones in a Block     0.24512632889520208     Random
05. Binary Matrix Rank Test                         0.7515836479160033      Random
06. Discrete Fourier Transform (Spectral) Test      0.20537891034612765     Random
07. Non-overlapping Template Matching Test          0.6144429353439044      Random
08. Overlapping Template Matching Test              0.4139889581685537      Random
09. Maurer's "Universal Statistical" Test           0.8283848113228522      Random
10. Linear Complexity Test                          0.9533639205736885      Random
11. Serial Test:
                          0.3334470051310822    Random
                          0.5457521613990917    Random
12. Approximate Entropy Test                        0.985908562197141       Random
13. Cumulative Sums Test (Forward)                  0.5280552415504154      Random
14. Cumulative Sums Test (Backward)                 0.14852246264978008     Random
15. Random Excursions Test:
        State       Chi Squared             P-Value                 Conclusion
        -4          3.3225018171044884      0.6503984660984446      Random
        -3          0.8056716343143413      0.9766701793358165      Random
        -2          4.264717023431279       0.5119661269996006      Random
        -1          3.413274890419537       0.6365489231358014      Random
        +1          4.311208515967439       0.5055330727280505      Random
        +2          1.7481466020393175      0.8827791473763106      Random
        +3          3.5179752035065692      0.6206695134214877      Random
        +4          5.277873678703588       0.38291759985974294     Random
16. Random Excursions Variant Test:
        State       COUNTS                  P-Value                 Conclusion
        -9.0        1554                    0.853594509226217       Random
        -8.0        1522                    0.7318633006728545      Random
        -7.0        1478                    0.5592248516505007      Random
        -6.0        1502                    0.6122761575245252      Random
        -5.0        1525                    0.6710828144475349      Random
        -4.0        1511                    0.5651890925556817      Random
        -3.0        1557                    0.7516043204112132      Random
        -2.0        1584                    0.8943473961157943      Random
        -1.0        1569                    0.6202899609732611      Random
        +1.0        1597                    1.0                     Random
        +2.0        1579                    0.854104297642865       Random
        +3.0        1657                    0.6349388207740039      Random
        +4.0        1675                    0.6019149510477143      Random
        +5.0        1637                    0.8134919995654255      Random
        +6.0        1588                    0.9617041314827208      Random
        +7.0        1513                    0.680170460943814       Random
        +8.0        1428                    0.440055131974034       Random
        +9.0        1383                    0.3584205780233013      Random
```

OFB Encrypted Image Analysis

```
Test Data File:/Users/samahy/College/Computer System
Security/12th_Project/Tasks/Task_1/encrypted_ofb.bin_string.bin


Type of Test                                        P-Value                 Conclusion
01. Frequency (Monobit) Test                        0.941010385262194       Random
02. Frequency Test within a Block                   0.05123825135018521     Random
03. Runs Test                                       0.5182828994998989      Random
04. Test for the Longest Run of Ones in a Block     0.6335921679439176      Random
05. Binary Matrix Rank Test                         0.5725816814613235      Random
06. Discrete Fourier Transform (Spectral) Test      0.37339444985401704     Random
07. Non-overlapping Template Matching Test          0.4003501498593763      Random
08. Overlapping Template Matching Test              0.9277561172383235      Random
09. Maurer's "Universal Statistical" Test           0.0594866446424713      Random
10. Linear Complexity Test                          0.6149406957654167      Random
11. Serial Test:
                          0.6392245261707353    Random
                          0.3954338500682254    Random
12. Approximate Entropy Test                        0.12681490654470748     Random
13. Cumulative Sums Test (Forward)                  0.9636506200877462      Random
14. Cumulative Sums Test (Backward)                 0.9878443341324801      Random
15. Random Excursions Test:
        State       Chi Squared             P-Value                 Conclusion
        -4          3.598532900381917       0.6085335840324222      Random
        -3          3.69076999175598        0.5947381228015975      Random
        -2          5.0093941151924115      0.41473479222999643     Random
        -1          21.350370981038747      0.0006954222270369647   Non-Random
        +1          2.016488046166529       0.8468589290920094      Random
        +2          3.573529561438327       0.6122920436536197      Random
        +3          2.519870733718059       0.7734995709516156      Random
        +4          6.4861164951536745      0.2617469918539946      Random
16. Random Excursions Variant Test:
        State       COUNTS                  P-Value                 Conclusion
        -9.0        2211                    0.4540944034160217      Random
        -8.0        2156                    0.31691187404990495     Random
        -7.0        2050                    0.13436278942500773     Random
        -6.0        2073                    0.1265172442647895      Random
        -5.0        2182                    0.2429528640190105      Random
        -4.0        2333                    0.6138183537135166      Random
        -3.0        2440                    0.92837935531486        Random
        -2.0        2433                    0.9537327729966885      Random
        -1.0        2452                    0.7089539844984949      Random
        +1.0        2378                    0.4907617464704217      Random
        +2.0        2450                    0.8423211080338107      Random
        +3.0        2348                    0.6165241539304349      Random
        +4.0        2226                    0.2778211404777631      Random
        +5.0        2303                    0.5561267212834601      Random
        +6.0        2263                    0.48046492542746666     Random
        +7.0        2150                    0.27179089507654464     Random
        +8.0        2075                    0.19323405675528882     Random
        +9.0        2081                    0.22965334091310285     Random
```

ECB Encrypted Image Analysis

```
Test Data File:/Users/samahy/College/Computer System
Security/12th_Project/Tasks/Task_1/encrypted_ecb.bin_string.bin


Type of Test                                        P-Value                 Conclusion
01. Frequency (Monobit) Test                        0.0                     Non-Random
02. Frequency Test within a Block                   1.0                     Random
03. Runs Test                                       0.0                     Non-Random
04. Test for the Longest Run of Ones in a Block     4.4003844943604805e-220 Non-Random
05. Binary Matrix Rank Test                         0.0                     Non-Random
06. Discrete Fourier Transform (Spectral) Test      0.0                     Non-Random
07. Non-overlapping Template Matching Test          0.0                     Non-Random
08. Overlapping Template Matching Test              0.0                     Non-Random
09. Maurer's "Universal Statistical" Test           0.0                     Non-Random
10. Linear Complexity Test                          0.0                     Non-Random
11. Serial Test:
                          0.0                   Non-Random
                          0.0                   Non-Random
12. Approximate Entropy Test                        0.0                     Non-Random
13. Cumulative Sums Test (Forward)                  0.0                     Non-Random
14. Cumulative Sums Test (Backward)                 0.0                     Non-Random
15. Random Excursions Test:
        State       Chi Squared             P-Value                 Conclusion
        -4          1.4285714285714286      0.9211625381990318      Random
        -3          2.0                     0.8491450360846096      Random
        -2          3.3333333333333335      0.6487423586675933      Random
        -1          3.6                     0.6083132920814687      Random
        +1          3.6                     0.6083132920814687      Random
        +2          4.434567901234568       0.4886854688472917      Random
        +3          7.07744                 0.21494441643911052     Random
        +4          7.459058725531029       0.18867592181395285     Random
16. Random Excursions Variant Test:
        State       COUNTS                  P-Value                 Conclusion
        -1.0        4                       0.17971249487899987     Random
        +1.0        10                      1.0                     Random
        +2.0        14                      0.6055766163353464      Random
        +3.0        21                      0.27133212189276534     Random
        +4.0        18                      0.49896229860376107     Random
        +5.0        15                      0.7093881150142263      Random
        +6.0        16                      0.6858304344516057      Random
        +7.0        17                      0.6642001619664318      Random
        +8.0        16                      0.729034489538804       Random
        +9.0        11                      0.9567498363337371      Random
```

Task 2: RSA Key Generation, Hashing, Signing, and Verification

RSA key pairs are fundamental to asymmetric cryptography. The strength of the RSA key is related to its length, with 2048 bits being a commonly used length for robust security.

- Private Key: Used for signing data and must be kept secure.
- Public Key: Shared with others for verification of signatures created with the private key.

The hash function (SHA1) produces a unique, fixed-size output (20 bytes for SHA1) from the input data. It's a one-way function, meaning it's computationally infeasible to reverse-engineer the original data from the hash. In Our Case it provides a fixed-size digest of the image data, which is used for creating and verifying the signature. (SHA1 is considered weak by modern standards due to vulnerabilities)

The private key is used to sign the hash. The signature is essentially a cryptographic proof that the data was signed by the owner of the private key. It is saved as a binary file that represents the encrypted hash. This step is crucial for authenticity verification. The size of the signature is consistent with RSA key size (2048-bit).

The public key is used to check if the signature matches the hash of the data. If it does, the signature is valid, indicating that the data hasn't been tampered with and was signed by the owner of the private key. The verification result should show "Verified OK" if the signature matches the hash and public key. If it shows an error or "Verification Failed," there might be issues with the key, signature, or hash.

RSA Generation and Verification Script

Private and Public key generation

```
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -pkeyopt rsa_keygen_pubexp:3 -out
"$private_key" > /dev/null 2>&1
openssl pkey -in "$private_key" -out "$public_key" -pubout
```

```
samahy@Samahys-Mac Tasks % cat Task_2/private_key.pem
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC9AmSpQGe0wPRS
2Jg6FsCPnLLWrF9YJGiNeOMBmBN3GrzvzKW5rN5oczaGhqNrvwmzDXa+7VGvor1e
......
......
......
wce9U6AewfuKUaWr6l1KS+NQSgQSnotVcCmBwejpJmvZuxDaX0pSIoiW6ZhZiVl3
RcqTXuPgeHBq+MMMr5WN6mo=
-----END PRIVATE KEY-----
```

```
samahy@Samahys-Mac Tasks % cat Task_2/public_key.pem
-----BEGIN PUBLIC KEY-----
MIIBIDANBgkqhkiG9w0BAQEFAAOCAQ0AMIIBCAKCAQEAvQJkqUBntMD0UtiYOhbA
......
88FM9NZJ/0CurKL1VPu55490UYhFuJLIy6ESoPIn8Awcl43AvXSEf6/7KfSwrT0+
cwIBAw==
-----END PUBLIC KEY-----
```

Generating and saving the hash value of an image

```
openssl dgst -sha1 "$cbc_encrypted_image" | awk '{print $2}' > "$file_hash"
```

```
samahy@Samahys-Mac Tasks % cat Task_2/hash.txt
f2137af6da0b192236d77365d4f5127adb54068d
```

Create a signature based the image hash and signed by the Private Key

```
openssl dgst -sha1 -sign "$private_key" -out "$signature_file" "$file_hash"
```

```
samahy@Samahys-Mac Tasks % xxd Task_2/signature.bin
00000000: 93bb 6454 d29f b4cb 847f 04fe 6756 00e8  ..dT........gV..
00000010: ab14 8c31 64db 9cdd c119 e916 82c6 bcb8  ...1d...........
00000020: 8f7b c001 14c4 e21b 6b76 01aa 7ae0 280e  .{......kv..z.(.
00000030: 5e27 7ed3 8bb4 2173 7976 5a1c e64d 5c53  ^'~...!syvZ..M\S
00000040: d2c6 23c6 2f24 f197 28a5 226d b681 6c35  ..#./$..(."m..l5
00000050: a29e cdd1 4e10 d50d 17e9 b85c 4133 4006  ....N......\A3@.
00000060: 3ebe d78b be62 1fea 4055 e261 c26b eef6  >....b..@U.a.k..
00000070: 0eb4 8375 e1b0 c581 45b8 5b63 7432 1477  ...u....E.[ct2.w
00000080: c2fe 1fb4 aa6d 1a1f efd9 f3b4 c013 43e3  .....m........C.
00000090: f794 d77f f34e d506 b699 589b a441 65b6  .....N....X..Ae.
000000a0: 1418 a2ab 1fe3 deb9 f5e8 f8d5 d1d7 e5ec  ................
000000b0: 2dc6 52ed 7c89 146d 0b17 9143 2bb4 149c  -.R.|..m...C+...
000000c0: e5b3 2a98 1ffa 75e4 bf27 3688 548f 0f9b  ..*...u..'6.T...
000000d0: 00f7 49b7 936d 8303 17fa 0461 f81d 8dff  ..I..m.....a....
000000e0: 2b4e 736a 41b7 0b0c 77bd e28a e178 f7ae  +NsjA...w....x..
000000f0: e96d 2ccc f642 48ba 07ae e24c 367a 307e  .m,..BH....L6z0~
```

Verify the signature using the Public Key (this step is usually done by the file recipient)

```
openssl dgst -sha1 -verify "$public_key" -signature "$signature_file" "$file_hash"
```

```
samahy@Samahys-Mac Task_2 % openssl dgst -sha1 -verify public_key.pem -signature signature.bin hash.txt
Verified OK
```