

First of all, we transform the key 'im a hacker' into an array of bytes and fill it to 16 bytes in order to be used by the Shamir library method.

With that, we can generate the shares by using 3 as threshold and 8 as the number of samples.

With the share, we can recover the key by using the combined method from Shamir class. We iterate through a number of samples in order to show that if we use 2 samples, the method fails to recover the secret key.

Examples.

Correct deconstruction

```
/Users/Jorge/PycharmProjects/Crypto/venv/bin/python /Users/Jorge/PycharmProjects/Crypto/privacy/week3/shamirSecret.py
ORIGINAL KEY im a hacker
Index #1: b'0c5720c76ab50d2c72a5a656f74b3e76'
Index #2: b'b38ee84b0a4bbb31e06757acefa92ced'
Index #3: b'd6b4e8ed4096d77ef9a783ca28d222ab'
Index #4: b'9ef595af8a4bdef49f6f0c4ccabe0849'
Index #5: b'fbcf9509c096b2bb86afd82a0dc5060f'
Index #6: b'44165d85a06804a6146d29d015271494'
Index #7: b'212c5d23eab568e90dadfdb6d25c1ad2'
Index #8: b'8f20dd978dbf32870b495bdc3dc45d2'
RECONSTRUCTED im a hacker0000

Process finished with exit code 0
```

Using only 2 samples it fails due to the threshold = 3

```
shamirSecret
/Users/Jorge/PycharmProjects/Crypto/venv/bin/python /Users/Jorge/PycharmProjects/Crypto/privacy/week3/shamirSecret.py
ORIGINAL KEY im a hacker
Index #1: b'c6ef1567786391c83597647d4632d707'
Index #2: b'd22b213e62e59bbf9543958667fb6855'
Index #3: b'7da914383aee6b14cbb183cb11f98f62'
Index #4: b'8ee88f906f1bfaf3982391ee709cdbc4'
Index #5: b'216aba9637100a58c6d187a3069e3cf3'
Index #6: b'35ae8ecf2d96002f66057658275783a1'
Index #7: b'9a2cbbc9759df08438f7601551556496'
Index #8: b'e240cab972eeee6b1c407470d8088b5'
RECONSTRUCTED Ê-ûPqâ ãU040YuyÉ

Process finished with exit code 0
```