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 thought 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

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