

- ```
pip install hashlib
```

```
python algorithm.py
```

- [illegible]

- [illegible]

Same as above

- **Step 1:** If the length of  $K = B$ : set  $K_0 = K$ . Go to step 4.
- **Step 2:** If the length of  $K > B$ : hash  $K$  to obtain an  $L$  byte string, then append  $(B-L)$  zeros to create a  $B$ -byte string  $K_0$  (i.e.,  $K_0 = H(K) \parallel 00 \dots 00$ ). Go to step 4.
- **Step 3:** If the length of  $K < B$ : append zeros to the end of  $K$  to create a  $B$ -byte string  $K_0$  (e.g., if  $K$  is 20 bytes in length and  $B = 64$ , then  $K$  will be appended with 44 zero bytes  $x'00'$ ).
- **Step 4:** Exclusive-Or  $K_0$  with  $\text{ipad}$  to produce a  $B$ -byte string:  $K_0 (+) \text{ipad}$ .
- **Step 5:** Append the stream of data 'text' to the string resulting from step 4:  $(K_0 (+) \text{ipad}) \parallel \text{text}$ .
- **Step 6:** Apply  $H$  to the stream generated in step 5:  $H((K_0 (+) \text{ipad}) \parallel \text{text})$ .
- **Step 7:** Exclusive-Or  $K_0$  with  $\text{opad}$ :  $K_0 (+) \text{opad}$ .
- **Step 8:** Append the result from step 6 to step 7:  $(K_0 (+) \text{opad}) \parallel H((K_0 (+) \text{ipad}) \parallel \text{text})$ .
- **Step 9:** Apply  $H$  to the result from step 8:  $H(K_0 (+) \text{opad} \parallel H((K_0 (+) \text{ipad}) \parallel \text{text}))$ .

All functions are already noted from the file `algorithm.py`