


Lecture 18: Introduction to Cryptography

Sunday, October 23, 2022 9:51 PM

CSC110 Lecture 18: Introduction to Cryptography

 Print this handout

Exercise 1: The One-Time Pad Cryptosystem

1. Suppose we want to encrypt the plaintext 'david' using the one-time pad cryptosystem and the secret key 'mario'. Fill in the table below to come up with the encrypted ciphertext. You may find the following useful:

```
>>> [ord(char) for char in 'david']  
[100, 97, 118, 105, 100]  
>>> [ord(char) for char in 'mario']  
[109, 97, 114, 105, 111]
```

If you are trying to do this first without using the Python console, you can use the ASCII code chart found [at the bottom of this worksheet](#).

message char	ord of message char	key char	ord of key char	ord of ciphertext char	ciphertext char
'd'	100	'm'	109	81	'Q'
'a'	97	'a'	97	$(97+97) \% 128 = 66$	'B'
'v'	118	'r'	114	104	'h'
'i'	105	'i'	105	82	'R'
'd'	100	'o'	111	83	'S'

2. Next, implement the one-time pad cryptosystem by completing the following two functions `encrypt_otp` and `decrypt_otp`. Some tips/hints:

