Secret-Key Encryption Lab

Xinyi Li

April 21, 2020

Instruction: https://seedsecuritylabs.org/Labs_16.04/PDF/Crypto_Encryption.pdf

Task 1

- Step 1: Use the text of the Gettysburg Address as the original article file `gettysburg.txt`. The usage of `tr` is available in GNU documentations. `-d` means 'delete' and `-cd` means 'delete the complement of', so first we just keep the letters, spaces, and newlines as the plaintext.

```
$tr [:upper:] [:lower:] < gettysburg.txt > lowercase.txt
$tr -cd '[a-z][\n][:space:]' < lowercase.txt > plaintext.txt
```

- Step 2: Use Python console to generate a permutation of `a-z`:

```
>>> import random
>>> s = "abcdefghijklmnopqrstuvwxyz"
>>> ''.join(random.sample(s,len(s)))
'azfgmunhrqwetlxicdksjbpvyo'
```

- Step 3: encryption

```
$tr "abcdefghijklmnopqrstuvwxyz" "azfgmunhrqwetlxicdksjbpvyo" <
    plaintext.txt > ciphertext.txt
```