# Report Cryptosytem Assignment

## 1. Reviews

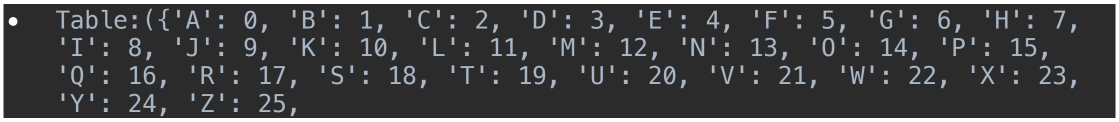
The encryption function for a single letter is
$E(x) = (ax + b) \bmod m$ (m=26), where modulus *m* is the size of the alphabet and *a* and b are the keys of the cipher. The value a must be chosen such that a and m are coprime.

The decryption function is
$D(x) = a^{-1}(x-b) \bmod m$, where $a^{-1}$ is the modular multiplicative inverse of a modulo m. I.e., it satisfies the equation

$$\begin{aligned}\mathrm{D}(\mathrm{E}(x)) &= a^{-1}(\mathrm{E}(x)-b) \bmod m \\ &= a^{-1}(((ax+b) \bmod m)-b) \bmod m \\ &= a^{-1}(ax+b-b) \bmod m \\ &= a^{-1}ax \bmod m \\ &= x \bmod m.\end{aligned}$$

## 2. Implementation

- ○ Install Pycharm for programing: Python
- ○ Build table $\pi$

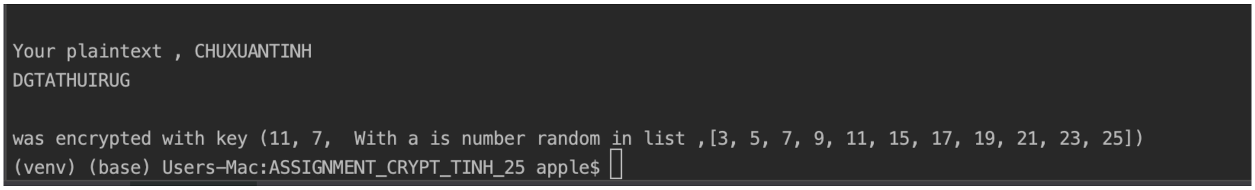


```
• Table:({'A': 0, 'B': 1, 'C': 2, 'D': 3, 'E': 4, 'F': 5, 'G': 6, 'H': 7,
  'I': 8, 'J': 9, 'K': 10, 'L': 11, 'M': 12, 'N': 13, 'O': 14, 'P': 15,
  'Q': 16, 'R': 17, 'S': 18, 'T': 19, 'U': 20, 'V': 21, 'W': 22, 'X': 23,
  'Y': 24, 'Z': 25,
```

- gcd(a, 26) =1
  a: random in [3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25]
  b: random

### Encrypt:

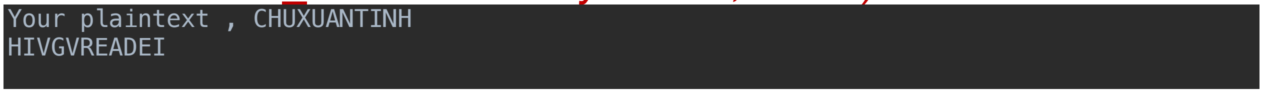
* Use command: *python enc_aff.py tinh.txt, in order to gen Ciphertext from file plaintext, key a, b random*
*=> call function enc_aff(plaintext, a, b, m)*



```
Your plaintext , CHUXUANTINH
DGTATHUIRUG

was encrypted with key (11, 7,  With a is number random in list ,[3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25])
(venv) (base) Users-Mac:ASSIGNMENT_CRYPT_TINH_25 apple$ 
```

*Use command: *python enc_aff.py tinh.txt 11 7 (ex:11 7 -> a b)*
*Use command: *python enc_aff.py tinh.txt >enc_tinh.txt , in order to gen ciphertext file*
*Details file enc_tinh.txt with key a = 21, b =17)*

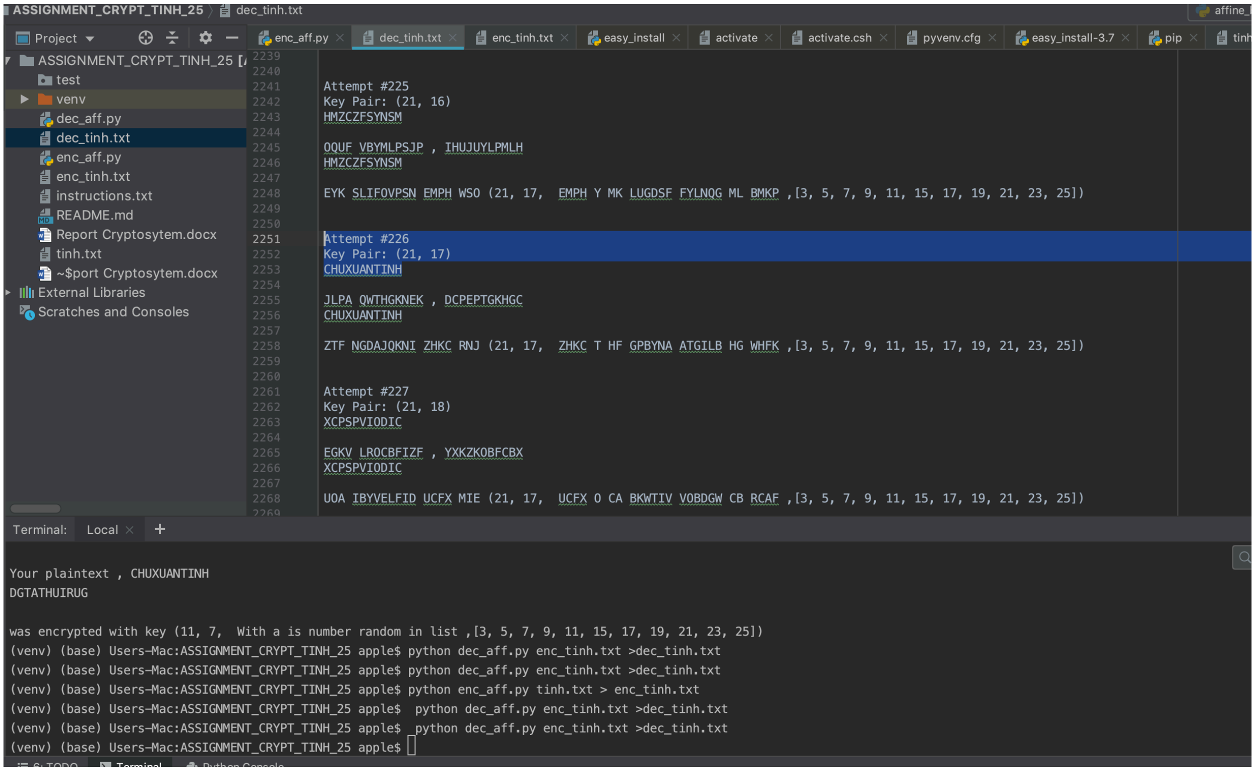


```
Your plaintext , CHUXUANTINH
HIVGVREADEI
```

```
was encrypted with key (21, 17,  With a is number random in list ,[3, 5, 7, 9, 11, 15,
17, 19, 21, 23, 25])
```

## Decrypt:

*Use command: *python dec_aff.py enc_tinh.txt >dec_tinh.txt , in order to decrypt -> plaintext*



```
Attempt #225
Key Pair: (21, 16)
HMZCZFSYNSM

OQUF VBYMLPSJP , IHUJUYLPMLH
HMZCZFSYNSM

EYK SLIFOVPSN EMPH WSO (21, 17,  EMPH Y MK LUGDSF FYLNQG ML BMKP ,[3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25])


Attempt #226
Key Pair: (21, 17)
CHUXUANTINH

JLPA QWTHGKNEK , DCPEPTGKHGC
CHUXUANTINH

ZTF NGDAJQKNI ZHKC RNJ (21, 17,  ZHKC T HF GPBYNA ATGILB HG WHFK ,[3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25])


Attempt #227
Key Pair: (21, 18)
XCPSPVIODIC

EGKV LROCBFIZF , YXKZKOBFCBX
XCPSPVIODIC

UOA IBYVELFID UCFX MIE (21, 17,  UCFX O CA BKWTIV VOBDGW CB RCAF ,[3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25])
```

```
Your plaintext , CHUXUANTINH
DGTATHUIRUG

was encrypted with key (11, 7,  With a is number random in list ,[3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25])
(venv) (base) Users-Mac:ASSIGNMENT_CRYPT_TINH_25 apple$ python dec_aff.py enc_tinh.txt >dec_tinh.txt
(venv) (base) Users-Mac:ASSIGNMENT_CRYPT_TINH_25 apple$ python dec_aff.py enc_tinh.txt >dec_tinh.txt
(venv) (base) Users-Mac:ASSIGNMENT_CRYPT_TINH_25 apple$ python enc_aff.py tinh.txt > enc_tinh.txt
(venv) (base) Users-Mac:ASSIGNMENT_CRYPT_TINH_25 apple$  python dec_aff.py enc_tinh.txt >dec_tinh.txt
(venv) (base) Users-Mac:ASSIGNMENT_CRYPT_TINH_25 apple$  python dec_aff.py enc_tinh.txt >dec_tinh.txt
(venv) (base) Users-Mac:ASSIGNMENT_CRYPT_TINH_25 apple$
```

## File *dec_tinh.txt* after decrypt

```
Attempt #226
Key Pair: (21, 17)
CHUXUANTINH
```