**Report Cryptosytem Assignment**

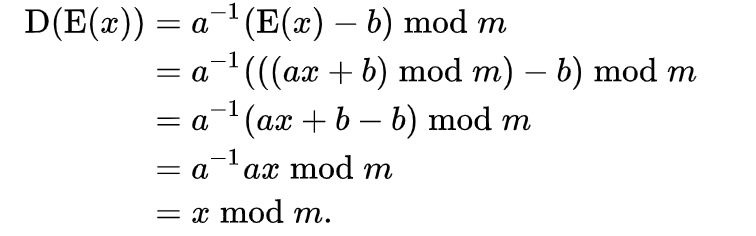
1. **Reviews**

The encryption function for a single letter is

E(x) = (ax + b) mod 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](https://en.wikipedia.org/wiki/Coprime).

The decryption function is

D(x) = (x-b) mod m, where is the [modular multiplicative inverse](https://en.wikipedia.org/wiki/Modular_multiplicative_inverse) of a [modulo](https://en.wikipedia.org/wiki/Modular_arithmetic) m. I.e., it satisfies the equation

****

1. **Implementation**
   * Install Pycharm for programing: Python
   * Build table

* 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]

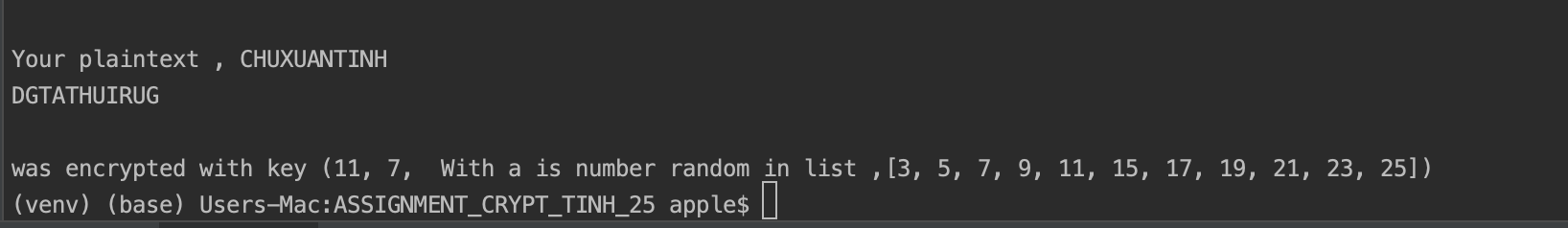
b: random

**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)*

**

\*Use command: *python enc\_aff.py tinh.txt 11 7 (ex:11 7 -> a b)*

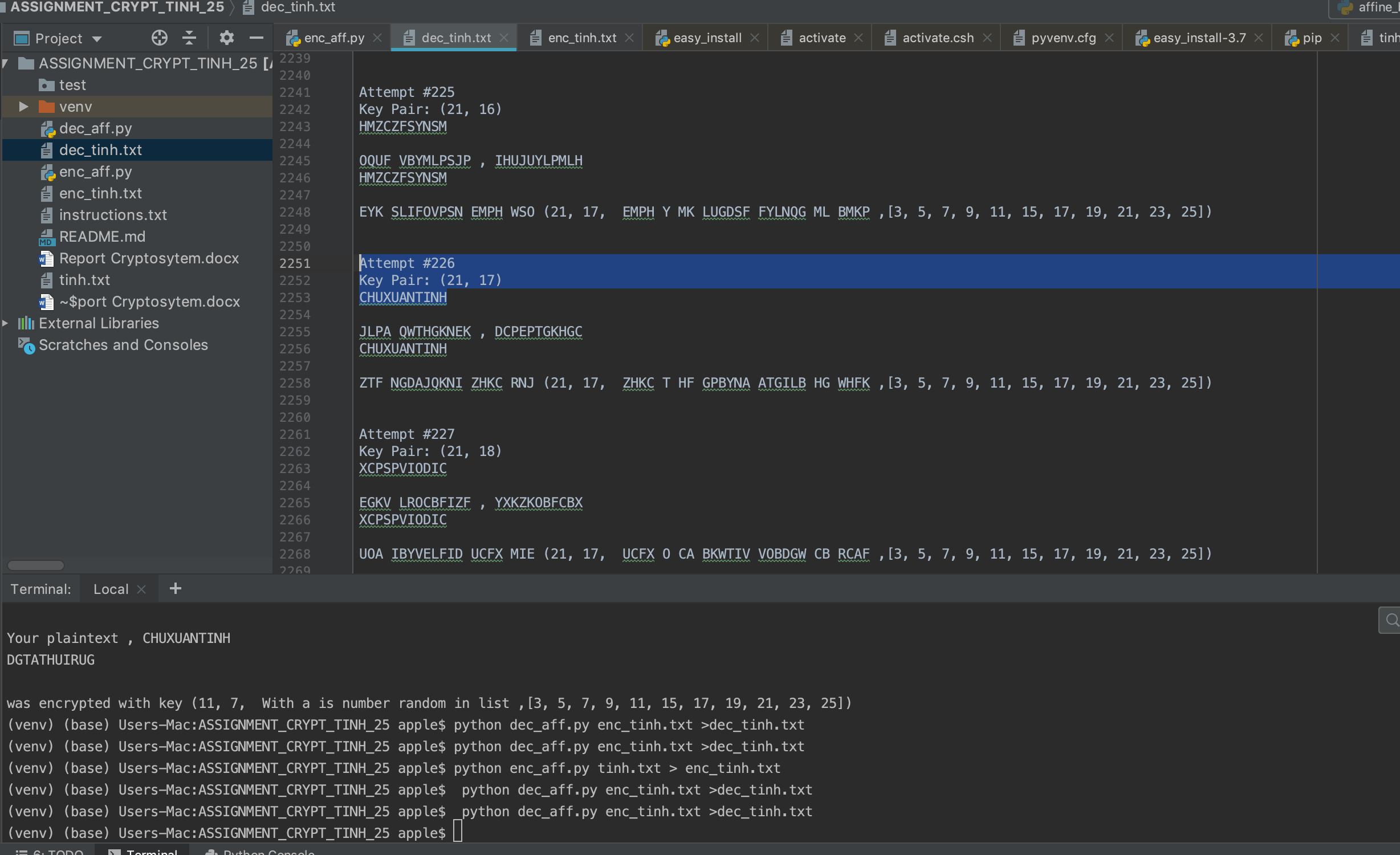
\*Use command: *python enc\_aff.py tinh.txt >enc\_tinh.txt , in order to gen ciphertext file*

*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*

****

**File *dec\_tinh.txt* after decrypt**

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