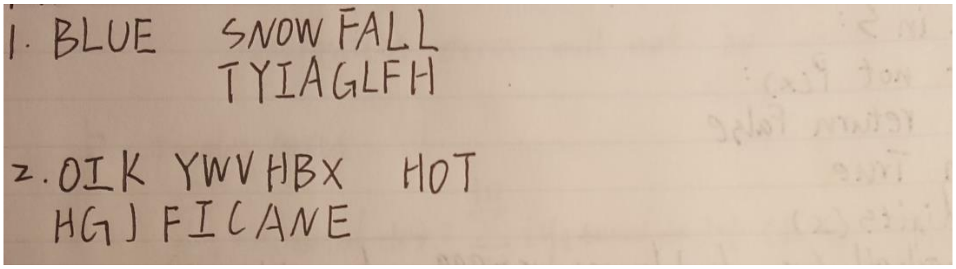
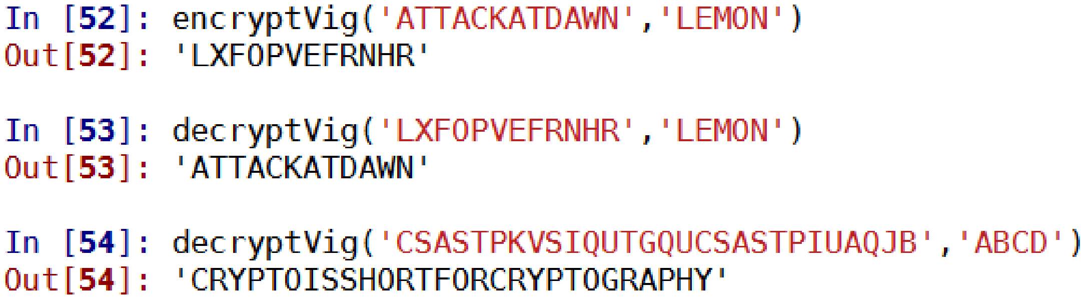
CS236 HW7 – Teng Xu



1. BLUE SNOW FALL
TYIAGLFH

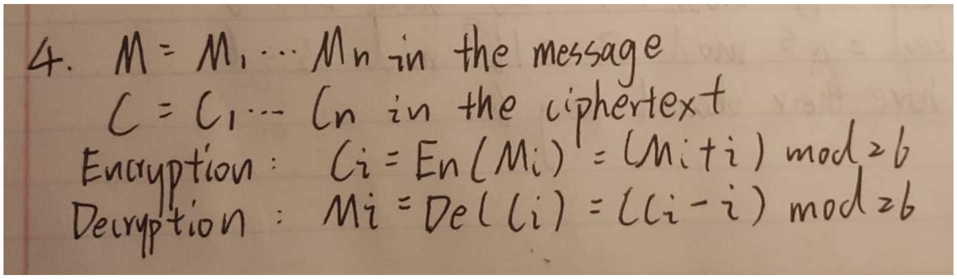
2. OIK YWVHBX HOT
HGJ FICANE

3. Write functions for encryption and decryption using Vigenère cipher: encryptVig(message, keyword) and decryptVig(message, keyword); test them on the examples in #1 (encryption), #2(decryption), and Lecture 7 slide 10: encrypt “ATTACK AT DAWN” and decrypt “LXFOPVEFRNHR” with keyword: “LEMON”. Decrypt “CSASTPKVSIQUTGQUCSASTPIUAQJB” using the keyword ABCD using decryptVig function.

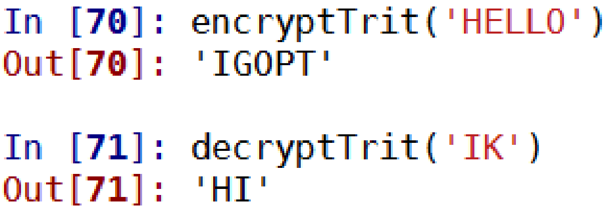


```
In [52]: encryptVig('ATTACKATDAWN','LEMON')
Out[52]: 'LXFOPVEFRNHR'

In [53]: decryptVig('LXFOPVEFRNHR','LEMON')
Out[53]: 'ATTACKATDAWN'

In [54]: decryptVig('CSASTPKVSIQUTGQUCSASTPIUAQJB','ABCD')
Out[54]: 'CRYPTOISSHORTFORCRYPTOGRAPHY'
```

4. Describe algebraically formulas for encryption and decryption using Trithemius cipher. Write functions encryptTrit(message) and decryptTrit(message); test them on the examples in Lecture 7 slide 6 (encode “HELLO” and decode “IK”).

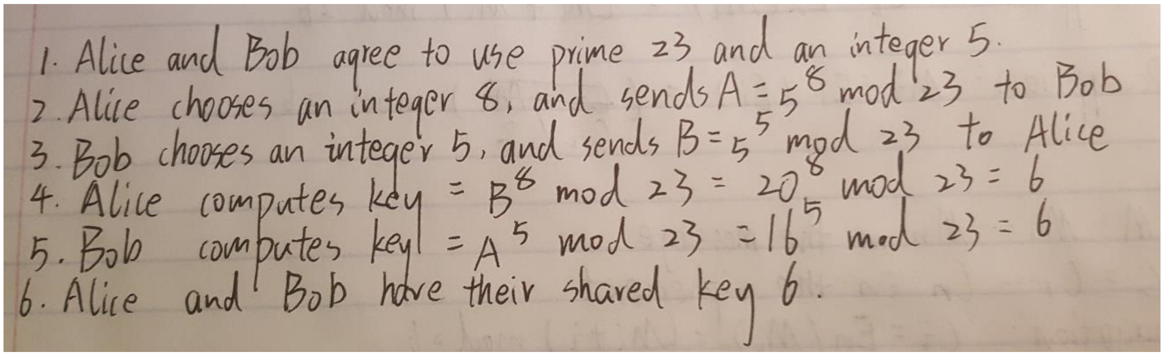


4. $M = M_1 \cdots M_n$ in the message
$C = C_1 \cdots C_n$ in the ciphertext
Encryption : $C_i = En(M_i) = (M_i + i) \bmod 26$
Decryption : $M_i = De(C_i) = (C_i - i) \bmod 26$



```
In [70]: encryptTrit('HELLO')
Out[70]: 'IGOPT'

In [71]: decryptTrit('IK')
Out[71]: 'HI'
```

5. Describe the steps that Alice and Bob follow when they use the Diffie-Hellman key exchange protocol to generate a shared secret key. Assume that they use the prime p=23 and g=5, and that Alice selects a secret number k_1=8 and Bob selects a secret number k_2=5.



1. Alice and Bob agree to use prime 23 and an integer 5.
2. Alice chooses an integer 8, and sends $A = 5^8 \bmod 23$ to Bob
3. Bob chooses an integer 5, and sends $B = 5^5 \bmod 23$ to Alice
4. Alice computes key $= B^8 \bmod 23 = 20^8 \bmod 23 = 6$
5. Bob computes key $= A^5 \bmod 23 = 16^5 \bmod 23 = 6$
6. Alice and Bob have their shared key 6.