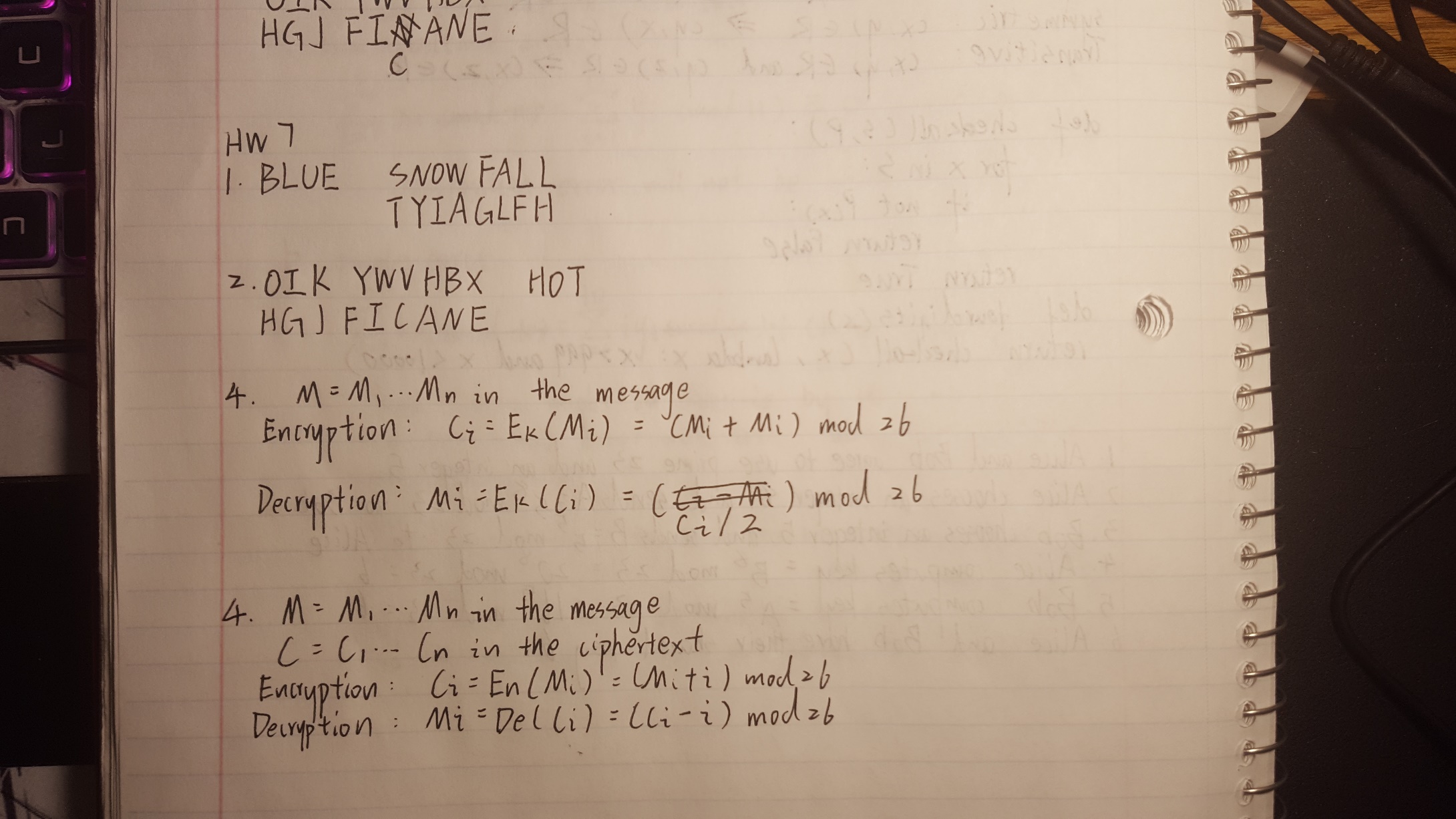
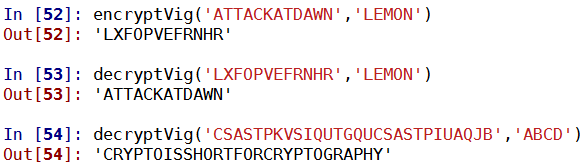
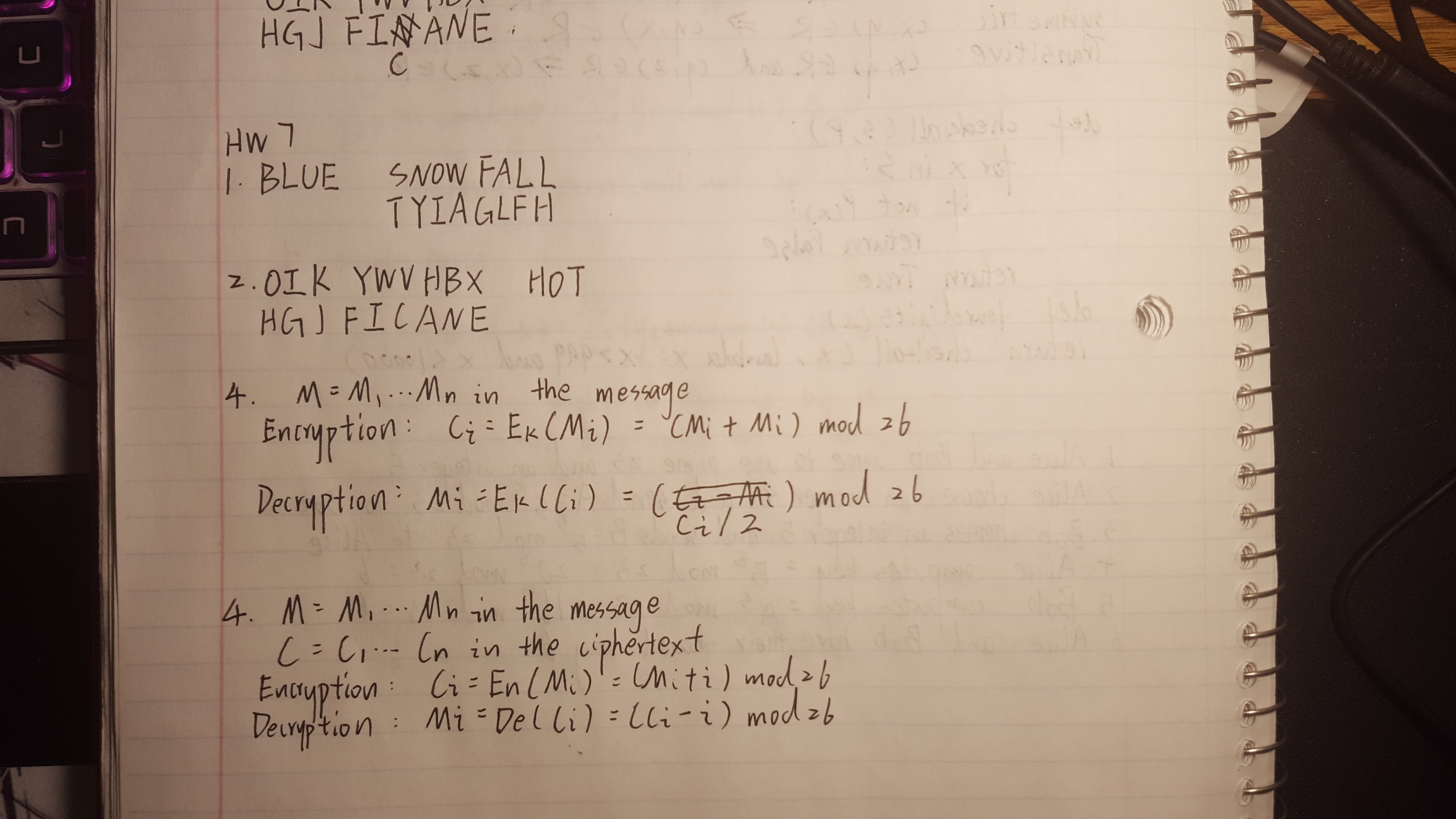
CS236 HW7 – Teng Xu

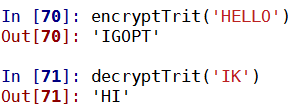


3. Write functions for encryption and decryption using Vigenère cipher: encryptVig(message, keyword) and decryptVig(message, keyword); test them on the examples in #1 (encryption), #2(decryption), and Lecture 7 slide 10: encrypt “ATTACK AT DAWN” and decrypt “LXFOPVEFRNHR” with keyword: “LEMON”. Decrypt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



1. 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”).





1. 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 k1=8 and Bob selects a secret number k2=5.

