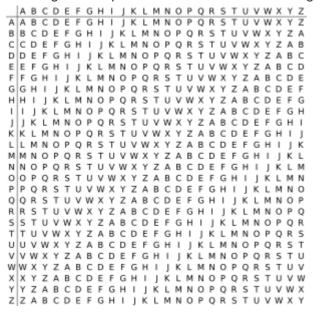# CS381 Exercise 2

**Name**: Zhang Yupeng
**Student ID**: 5130309468

**1. Which security services are required to do secure online shopping?**

To secure online shopping, we need confidentiality because we don't want the pravite shopping information known by the adversary, we also need authenticity to make sure that the sellers and buyers are really themselves, integrity and non-repudiation are also needed to make the deal fair and legal, access-control is required to make the database safe.

**2. Decrypt the ciphertext of TZUYH of Vigenère Cipher with keyword OR.**

The Vigenère Cipher Table is shwon as following picture.



To decrypt the ciphertext, we align the ciphertext with the keyword, as:

**T Z U Y H**

**O R O R O**

Then, find the corresponding letter in the table, and put them into the plaintext,the plaintext is **FIGHT**.

**3. Is one-time-pad cipher practical, and why?**

One-time-pad cipher is not practical because although it can provide a perfect secercy system but the length of key is longer than the length of plaintext, which means it is not practical.