## Math 316, 4.1 The Vigenère Cipher

Name:	
Read and take notes on Section 4.1 The Vigenère Cipher.	
Reading Questions	
1. Encrypt 'snowy day' with the Vigenère cipher with key 'cold.'	

2. Known-plaintext attack: Suppose you know that the plaintext 'drink your ovaltine' has been encrypted via a Vigenère cipher with unknown key as 'URTCR GSLR ZKHTXZNP'. Find the key and use it to decrypt the following ciphertext, 'Z PCTMMV R MTARALRKP'.

3. Compare and contrast the Vigenère cipher and the one-time pad. What features do they have in common? What makes them different? What is the weakness of the Vigenère cipher?
4. What struck you in this reading? What is still unclear? What remaining questions do you have?