*1. The _____ cipher is the simplest monoalphabetic cipher. It uses modular arithmetic with a modulus of 26. （分值：1分）

- (●) shift (正确答案)
- ( ) additive
- ( ) transposition
- ( ) none of the above

*2. Consider the ransposition cipher over the lowercase English alphabet, there are how many different keys? （分值：1分）

- ( ) 26^26
- (●) 26! (正确答案)
- ( ) 2^26
- ( ) 26

*3. Vigenere cipher

key: deceptive
plaintext: wearediscoveredsaveyourself
ciphertext:（答案：ZICVTWQNGRZGVTWAVZHCQYGLMGJ，分值：2分）

都是大写字母

*4. The rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.The cipher text is MEMATRHTGPRYETEFETEOAAT with a rail fence of depth 2.The plain text is （答案：meet me after the toga party，分值：2分）

小写字母，有意义的一句话

*5. Consider the Vigenere cipher over the lowercase English alphabet, where the key can have length 1 or length 2 or length 3, length1 with 30% probability and length2 with 30% and length3 with 40%. Say the distribution over plaintexts is Pr[M='aa'] = 0.4 and Pr[M='ab'] = 0.6. What is Pr[C='bb']? Express your answer to 4 decimal places with a leading 0, i.e., if your answer was 1/2 then you would enter 0.5000 (without a trailing period).（答案：0.005651，分值：2分）

答案精确到小数点后6位

*6. Consider the one-time pad over the message space of 5-bit strings, where Pr[M=00100] = 0.05 and Pr[M=11011] = 0.05. What is Pr[C=00000]? Express your answer to 5 decimal places with a leading 0. I.e., if your answer was 1/2, then you would enter 0.50000 (without a trailing period).（答案：0.03125，分值：2分）

答案精确到小数点后5位