

考生信息

姓名 基本信息
部门 其它信息

考试题型

考试单选 考试判断
考试多选 单项填空
多项填空 简答题
多项简答 考试文件
考试绘图 完型填空
多项文件

分页说明

分页 段落说明

其他题型

批量添加

* 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 transposition 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 MEMATRH TGPRTYETEFETEOAAT 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, length 1 with 30% probability and length 2 with 30% and length 3 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

Handwritten calculation for Question 5:

Key length distribution:

- length=1: $\frac{1}{26}$
- length=2: $\frac{1}{26} \times \frac{1}{26}$
- length=3: $\frac{1}{26} \times \frac{1}{26} \times \frac{1}{26}$

Plaintext distribution:

- aa: 0.4
- ab: 0.6

Calculation for $\Pr[C = 'bb']$:

For length=1: $\frac{1}{26} \times 0.4 \times \frac{1}{26}$

For length=2: $\frac{1}{26} \times \frac{1}{26} \times 0.6 \times \frac{1}{26}$

For length=3: $\frac{1}{26} \times \frac{1}{26} \times \frac{1}{26} \times 0.6 \times \frac{1}{26}$

Final calculation:

$$0.4 \left(\frac{1}{26} \times 0.3 + \frac{1}{26} \times 0.7 \right) + 0.6 \left(\frac{1}{26} \times 0.7 \right) + \frac{1}{26} \times 0.12 + \frac{1}{26} \times 0.7$$