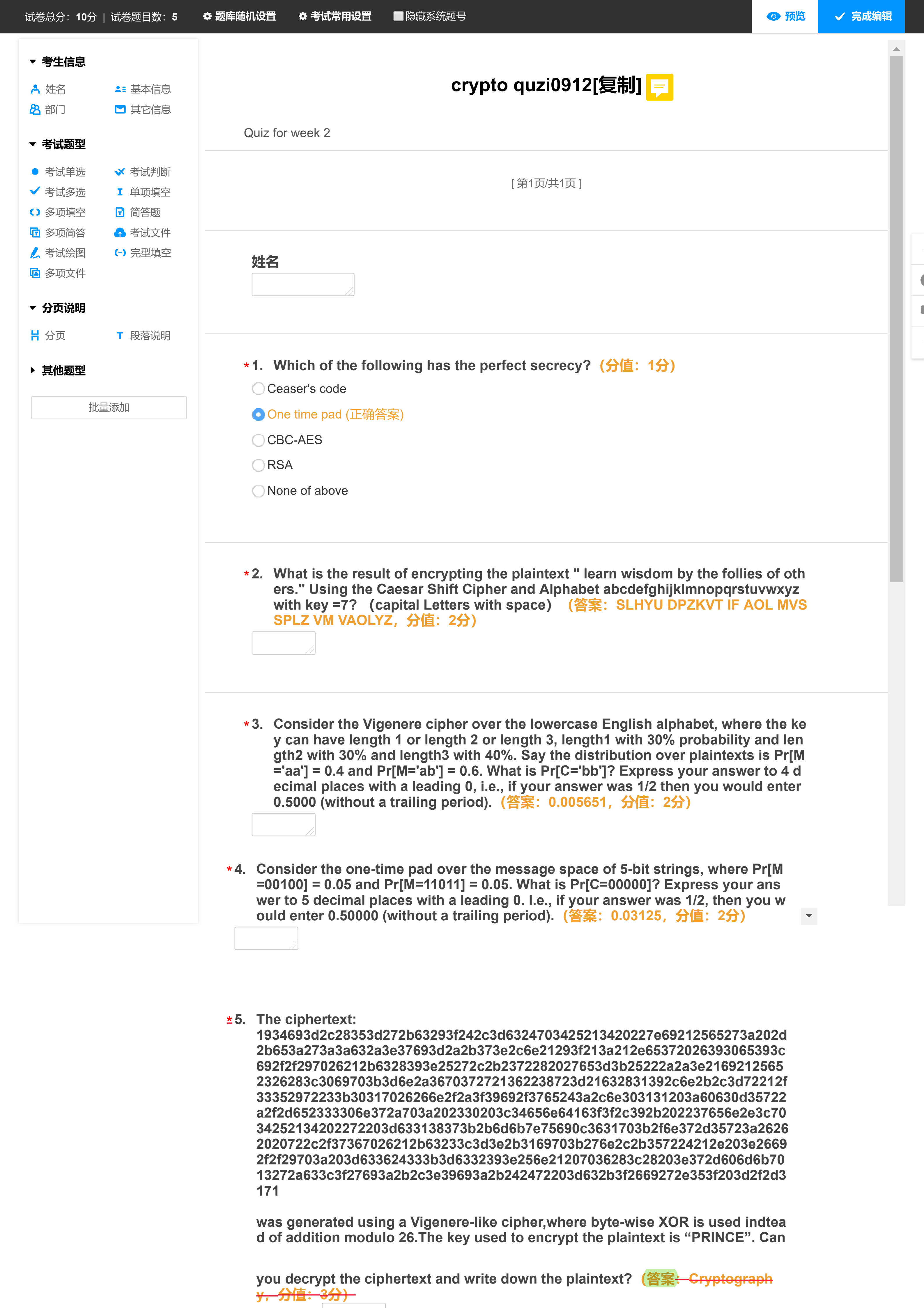

试卷总分：10分 | 试卷题目数：5 | 题库随机设置 | 考试常用设置 | □隐藏系统题号 | 预览 | 完成编辑

▾ 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

# crypto quzi0912[复制]

Quiz for week 2

[ 第1页/共1页 ]

姓名

*1. Which of the following has the perfect secrecy? （分值：1分）

○ Ceaser's code

● One time pad (正确答案)

○ CBC-AES

○ RSA

○ None of above

*2. What is the result of encrypting the plaintext " learn wisdom by the follies of others." Using the Caesar Shift Cipher and Alphabet abcdefghijklmnopqrstuvwxyz with key =7? (capital Letters with space) （答案：SLHYU DPZKVT IF AOL MVS SPLZ VM VAOLYZ，分值：2分）

*3. 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）

*4. 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）

*5. The ciphertext:

```
1934693d2c28353d272b63293f242c3d63247034252134202 27e69212565273a202d
2b653a273a3a632a3e37693d2a2b373e2c6e21293f213a212e6537202639306539 3c
692f2f297026212b6328393e25272c2b2372282027653d3b25222a2a3e2169212565
2326283c3069703b3d6e2a367037272136223872 3d21632831392c6e2b2c3d72212f
33352972233b30317026266e2f2a3f39692f3765243a2c6e303131203a60630d35722
a2f2d652333306e372a703a202330203c34656e64163f3f2c392b202237656e2e3c70
342521342022722 03d633138373b2b6d6b7e75690c3631703b2f6e372d35723a2626
2020722c2f37367026212b63233c3d3e2b3169703b276e2c2b357224212e203e2669
2f2f29703a203d633624333b3d6332393e256e21207036283c28203e372d606d6b70
13272a633c3f27693a2b2c3e39693a2b242472203d632b3f2669272e353f203d2f2d3
171
```

was generated using a Vigenere-like cipher,where byte-wise XOR is used indtead of addition modulo 26.The key used to encrypt the plaintext is “PRINCE”. Can

you decrypt the ciphertext and write down the plaintext? （答案~~：Cryptography，分值：3分）~~