202[redacted]密码行业职[redacted]技能竞赛
技术[redacted]件

一、赛项[redacted]

本赛[redacted]面[redacted]为企事[redacted]单位职工[redacted]高等院校在校学生，聚焦密[redacted]技术应[redacted]员（职[redacted]编码：4[redacted]7-05-06[redacted]应具备[redacted]和识[redacted]技能，[redacted]该密[redacted]领域[redacted]法律[redacted]规、标准规范、操作技能[redacted]。本文件[redacted]据《密[redacted]技术应用员国家职业技能标准（2022年[redacted]）》和[redacted]于组织开[redacted]“江苏工匠”岗位练兵职业技能竞赛[redacted]的通[redacted]》（苏人社函[2022〕65号）编制。

二、竞赛形式

本赛项为“三人赛制”，分“职工组”和“学生组”两个组别，举办选拔赛和决赛。

（一）选拔赛

比赛时间为2024年10月13日15：00—16：00

选拔赛由各设区市（赛区）组织参赛，全省统一通过竞赛平台进行答题。选拔赛进行理论知识考核，时间60分钟，共90

每名参赛选手需分别独立完成理论答题；操作技能部分考核时间为180分钟，占总成绩70%，由每支队伍的三名选手共同完成。

三、竞赛规则

（一）选拔赛

1.采用竞赛平台答题，题目以试卷形式显示在竞赛系统上，选手须使用各自的账号和口令登录竞赛系统，独立完成题目作答并提交答案。答题超过规定时间，系统将自动提交试卷，成绩以提交时答题情况为准。

2.禁止各参赛队伍或选手之间交流、分享答案，严禁使用任何方式查阅资料。

3.参赛选手不得使用任何方式对竞赛系统进行攻击和入侵。组委会将对所有行为进行实时监控，一旦发现并核实为参赛选手或竞赛有关人员恶意攻击的，将封禁攻击源IP地址，取消该选手及所在队伍参赛资格并通报相关单位。同时，保留进一步追究相关人员法律责任的权利。

4.组委会组织线上监考，赛前组织赛前说明会，相关信息通过邮件或短信通知。

5.选拔赛每支队伍成绩为队伍3名选手的总分，排名按队伍总分从高到低排序。

（二）决赛

1.在竞赛前组织抽签，竞赛时各参赛队伍按照抽签编号入座。

2.竞赛开始后每名参赛选手需独自完成理论考核，然后

以队伍为单位，3 名选手规定时间内协同完成操作技能考核。

3.决赛系统限制提交答案次数，答对累加积分，答错不扣分。竞赛排名按队伍总成绩从高到低进行排序，成绩相同的，则按时间进行排序，先得分的排名在前。

4.竞赛过程中，现场裁判将视情况要求选手复现答题过程，不能复现的本题成绩无效并给予警告。比赛结束前各队伍需要把详细解题思路及截图提交裁判组，否则视为成绩无效。

5.决赛评分以队伍为单位，“

*30%+ *70%”

四、晋级方式

（一）晋级资格

职工组和学生组晋级决赛名额各为 20 支队伍。

职工组和学生组选拔赛成绩在各赛区排名第一的晋级决赛，其余名额按全省选拔赛成绩排名确定。

（二）评分办法

选拔赛由系统自动评分。每组参赛队伍总成绩为队伍中 3 名选手的总分。选手未在规定时间内参加答题的，按 0 分计入队伍总成绩。

（三）排名细则

选拔赛成绩产生后，如存在因成绩相同而无法确定晋级队伍的，则取相同成绩队伍中最高的个人成绩进行比较，分数高者所在队伍排名靠前；如最高的个人成绩相同，则比较各队伍中次高的个人成绩，以此类推。如队伍成绩和个人成绩完全相

同的，则总答题用时较少的队伍排名靠前。若答题用时也相同，将进行附加赛决出晋级队伍和选手。

（四）晋级公布

决赛晋级名单将于10月16日24:00前发布在江苏省国家密码管理局网站。

（五）参赛确认及资格复审

晋级决赛队伍按相关要求完成决赛参赛确认，并提交相应资格证明材料，组委会将进行资格复审。

五、竞赛提纲

（一）提纲概述

选拔赛理论题目数量为90题，竞赛题目内容包括密码领域相关法律法规、标准规范等内容。

决赛阶段理论考核内容与选拔赛相同，操作技能竞赛题目数量约为15题，竞赛题目考核选手密码破译、流量分析、算法攻击、编码转换、综合密码场景分析等能力。

理论题库在省密码管理局网站公布。竞赛内容权重表如下表所示。

科目	模块	权重（%）
理论知识		5
	密码政策法规	10
	密码技术基础及相关标准	15
	密码产品原理、应用及相关标准	20
	密码安全理论、技术及相关标准	20

	密码应用与实践场景	30
	合计	100
操作技能	编码与解码	18
	密码流量分析	20
	密码破译	18
	密码算法攻击	23
	密码安全综合场景	21
	合计	100

（二）参考资料

1.理论知识

（1）《中华人民共和国密码法》、《中华人民共和国网络安全法》《商用密码管理条例》等法律法规

（2）《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》

（3）《GB/T 43207-2023 信息安全技术 信息系统密码应用设计指南》

（4）《GM/T 0001-2012 祖冲之序列密码算法》

（5）《GM/T 0002-1012 SM4 分组密码算法》

（6）《GM/T 0003-2012 SM2 椭圆曲线公钥密码算法》

（7）《GM/T 0004-2012 SM3 密码杂凑算法》

（8）《GM/T 0028-2014 密码模块安全技术要求》

（9）《图解密码技术》

（10）《应用密码学》

（11）《深入浅出密码学》

（12）《商用密码应用与安全性评估》

（13）其他密码相关密码国家标准、行业标准，及正式出版物

2.操作技能

（1）密码破译。选手在不知道密钥的情况下，恢复出密文中隐藏的明文信息。

（2）流量分析。从协议、算法、证书等方面对数据流量包进行综合分析，获得结果。

（3）算法攻击。基于某些算法在实现过程中存在的脆弱性对算法开展攻击，恢复明文，获得结果。

（4）编码转换。使用常见的编码方式，对明/密文实现多重转换，获得明/密文结果。

（5）场景分析。结合实际应用场景（某应用系统），设置数据泄露，使用攻击方法获得口令明文，登录应用后台，使用密钥对数据库中业务数据进行明文恢复等。

（三）竞赛样题

【单选】1.以下关于非对称密码的说法，错误的是（ ）

A.加密算法和解密算法使用不同的密钥

B.非对称密码也称为公钥密码

C.非对称密码可以用来实现数字签名

D.非对称密码不能用来加密数据

答案：D

【单选】2.假如甲想使用公钥密码算法发送一个加密信息给乙，此信息只有乙可以解密，甲使用哪个密钥来加密这

个信息（ ）

A.甲的公钥 B.甲的私钥 C.乙的公钥 D.乙的私钥

答案：C

【单选】3.下列哪一项不属于公钥基础设施（PKI）的组件（ ）

A.CRL B.RA C.KDC D.CA

答案：C

【多选】4.安全的哈希算法应该具有的特点包括（ ）

A. 单向性 B.弱抗碰撞性

C.强抗碰撞性 D.解密时间短

答案：ABC

【多选】5.关于对称加密算法和非对称加密算法，下列哪些说法是不正确的（ ）

A.对称加密算法更快，因为使用了替换密码和置换密码

B.对称加密算法更慢，因为使用了替换密码和置换密码

C.非对称加密算法的密钥分发比对称加密算法更困难

D.非对称加密算法不能提供认证和不可否认性

答案：BCD

【多选】6.下列说法正确的有（ ）

A.简单的说，密码学中的“明文”是指没有经过加密的信息；而“密文”是指已经加了密的信息

B.二战时期著名的“隐谜”密码打字机是英国军队使用的

C. Vigenere 密码是古典密码体制比拟有代表性的一种密

码，其密码体制采用的是多表代换密码

D.Vigenere 密码是由法国密码学家提出来的

答案：ACD

【判断】7.伪造、冒用、盗用其他人的电子签名，构成犯罪的，依法追究刑事责任；给他人造成损失的依法承担民事责任（ ）

答案：√

【判断】8.字母频率分析法对多表代替密码算法最有效果（ ）

答案：×

【判断】9.任何单位或者个人都可以使用商用密码产品（ ）

答案：×

【操作题】10.密文: DQHES AVIZC LCKOE VJZCP MWQTS HVMPR DQX

明文：VUJVW TNMBT PVCSG MNSUT ONUMK LXDTK VUZ

请破解密钥（大写字母）

答案：SECRET

【操作题】11.通过使用各种加解密技术,包括古典密码、机械密码、现代密码等，根据题目要求获取需要的明/密文信息。

题目示例：

密文：toosoeaorwatrymrinhd，猜猜有几栅。

请获得 flag 值并提交（以 flag{}形式提交）。

基础知识：

栅栏密码是一种简单的移动字符位置的加密方法，规则简单，容易破解。栅栏密码的加密方式：把文本按照一定的字数分成多个组，取每组第一个字连起来得到密文 1，再取每组第二个字连起来得到密文 2……最后把密文 1、密文 2……连成整段密文。

解题思路：

根据提示，初步判断本题考点为栅栏加/解密。

1、确定每行的字符数。根据密文的长度和栅栏的行数，可以确定每行的字符数。

每行字符数 = 密文的长度 / 栅栏组数，余数 n，不能整除，结果还需要+1。

2、按照每行字符数，将密文 toosoeaorwatrymrinhd 重新排列：

尝试 1 栅：

toosoeaorwatrymrinhd

将上述数组由上至下，由左至右读取，从而恢复明文。结果为：toosoeaorwatrymrinhd

尝试 2 栅：

toosoeaorw

atrymrinhd

将上述数组由上至下，由左至右读取，从而恢复明文。结果为：taotorsyomeraionrhwd

尝试 3 栅为：

toosoea

orwatry

mrinhd

将上述数组由上至下，由左至右读取，从而恢复明文。结果为：tomorrowisanotherday

根据题目要求，以 flag{}形式提交。

答案：flag{tomorrowisanotherday}

【通过代码实现】

```
# coding:utf-8

import math

def encrypt(message,key):
    translate_text = ''
    for i in range(key):
        translate_text += message[i::key]
    return(translate_text)

def decrypt(message,key):
    translate_text = ''
    n = math.ceil(len(message)/key)
    for i in range(n):
        translate_text += message[i::n]
    return(translate_text)
```

```
if __name__ == '__main__':
------------------------')
 1. 栅栏密码加密          ')
 2. 栅栏密码解密          ')
------------------------')
put('请选择:'))


 input('请输入需要加密的信息：').replace(' ','')
_text = encrypt(message,key)
密结果：',translate_text)
2:
 input('请输入需要解密的信息：')
_text = decrypt(message,key)
密结果：',translate_text)
```

```
    print('------
    print('
    print('
    print('------
    mode = int(in
    key = 3
    if mode == 1:
        message =
        translate
        print('加
    elif mode ==
        message =
        translate
        print('解
```

六、纪律要求

所有参赛者必须服从组委会统一安排，遵守竞赛纪律。

理论考核时每名选手须独立完成全部答题过程，对于违反竞赛规则的，一经发现，将取消队伍比赛成绩。

竞赛期间禁止请求外界援助、使用 DoS 攻击或非法攻击其他选手，不得对比赛系统服务器发动任何恶意攻击行为，一经发现按退赛处理。

七、申诉与仲裁

1.

2. 2

3.

4.

八、其他事项

1.竞赛相关文件，请访问江苏省国家密码管理局网站（在线服务-下载中心 https://www.jsmm.gov.cn/xzzx/index.jhtml）查看和下载。

2.竞赛其他有关事项将通过邮件、短信或电话方式通知。

3.本次竞赛的解释权归大赛组委会。