**密码学第二次作业参考答案**

**1.**【Caesar密码】仿射Caesar密码，即Caesar密码的一种推广，具有如下定义：对于每一个明文，用密文代替，其中。对加密算法的一个基本要求是算法是单射的，即如果，则有。否则，就会因为有很多的明文映射成相同的密文而不能解密。仿射Caesar密码并不是对所有的都满足上述的一对一映射，例如。

1. 共有 种合法取值，分别为 。
2. 共有 种合法取值。
3. 仿射Caesar密码的密钥共有 种合法取值。
4. 若用仿射Caesar密码加密英文文本得到一份密文，发现其中频率最高的字母为H，次高的字母为Y，则密钥最有可能的取值为 。

**2.**【证明题】对于乘法代替密码，当且仅当时，才是一一映射。

充分性？

必要性？

**3.**【单表代替密码】某明文采用单表代替的方法加密产生的密文为FMHC NI ABC MGC ABNGR ABEA ASEGIQCGPI ANJC EGP IUEQC，密钥的助记词句（简单处理助记词句以得到密钥）为书中的第一句话：The fallen leaves may symbolize the decline of the Tang Dynasty and the rolling waves predict the revival of the past glory.

* 1. 试破译该密文，给出明密文对照表，并写出分析过程。

2）简述单表代替密码的安全性及一般性的破译方法（可以结合所给例句进行分析）。

3）【选做】该单表代替方法中，用于密钥助记的句子往往很长，原因为何？

**4.**【Playfair密码】使用Playfair密码加密消息：Be at the third pillar from the left outside the pyceum theatre.

1. 采用如下的Playfair矩阵加密该消息，写出密文：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| M | F | H | I/J | K |
| U | N | O | P | Q |
| Z | V | W | X | Y |
| E | L | A | R | G |
| D | S | T | B | C |

2）使用密钥largest构造Playfair矩阵加密该消息，写出构造的Playfair矩阵及密文。

3）对比前两问的结果，可以得到什么可一般性推广的结论？（提示：请详细观察矩阵）

4）【选做】计算Playfair密码密钥空间的大小，用2的幂表示（有重复加密结果的密钥只计数一次，最终结果取最佳逼近）。

**5.**【Hill密码】Hill密码是利用矩阵进行加解密运算的一种算法，可以抵御唯密文攻击。

1）使用密钥为的Hill密码加密消息“Meet me at buaa”，写出密文并以第一个单词meet为例写出加密的计算过程。

2）以从密文中恢复出明文第一个单词meet为例，写出从密文恢复明文所做的解密计算。

3）请描述Hill密码的已知明文攻击方案。

4）【选做】Hill密码不足以抵抗已知明文攻击；若采用选择明文攻击，则有更高效的方法攻破Hill密码。对于行列的合法密钥矩阵，试构建不超过组明文破译其密钥矩阵。

**6.**【多表代替密码与OTP(One-Time Padding,一次一密)】Vigenère密码是最简单的多表代替密码。若密钥长度与明文长度相同，可起到一次一密的效果。

1. 用Vigenère密码加密单词“explanation”，密钥为“hand”。

2)使用密钥流[9,0,1,7,23,15,21,14,11,11,2,8,9,13]加密明文pleasevmefifty。

3)找到另一个密钥流，可使上一问的加密结果解密为idonthavemoney。

4)【选做】用Vernam密码加密句子“kfccrazythursday”，密钥为“!@#$%^&”，请给出加密后的结果。

**7.**【习题3.16】已知Hill密码里的矩阵需要满足(ad-bc)与26互素，即(ad-bc)与26的唯一正整数因子是1。因此，如果(ad-bc)为13或偶数，这样的矩阵不合格。用下列方法可推算出2阶Hill密码密钥的个数。

1. 判定如下矩阵的个数：判别式为偶数，且其一行或两行都是偶的（称一行为偶的是指该行的所有元素为偶数）。
2. 判定如下矩阵的个数：判别式为偶数，且其一列或两列都是偶的。
3. 判定如下矩阵的个数：判别式为偶数，且其所有元素为奇数。

4)考虑重叠情况，找出判别式为偶的矩阵总数。

5)【选做】判定如下矩阵的个数：判别式为13的倍数，且其第一列为13的倍数。

6)【选做】判定如下矩阵的个数：判别式为13的倍数，且其第一列不为13的倍数，但第二列在模13的意义下是第一列的倍数。

7)【选做】计算判别式为13的倍数的所有矩阵个数。

8)【选做】判定如下矩阵的个数：判别式为26的倍数，且满足情况1）和5），2）和5），3）和5），1）和6），等等。

9)【选做】计算出判别式既不是2的倍数也不是13的倍数的矩阵总数。

**注意：**

以上作业请使用**pdf**文档格式提交，于**2022年3月17日（星期五）23:59**之前在OJ系统上提交，并将作业命名为“**学号\_姓名\_密码学第二次作业**”。如“21371234\_张三\_密码学第二次作业”。