**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 12 种合法取值，分别为1，3，5，7，9，11，15，17，19，21，23，25。（要满足互素）
2. 共有26种合法取值。（没有限制）
3. 仿射Caesar密码的密钥共有311种合法取值。

（去除的1种是平凡密钥）

1. 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[15，25]。

**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：若;说明存在整数,使得，在模的意义下则有存在使得，存在逆元为。在模意义下是唯一的：反证存在在模意义下都是的逆元，那么作差应有,由于，则有，由于在模意义下是小于的，若和在模意义下不相等，则显然不成立。可见的逆元唯一，且该映射为单射。对于乘法密码,只需将等式两侧同时乘以逆元，有，即由知，对于任给的都能解密出唯一的，该映射为满射。得证对的映射是一一映射

必要性：若是一一映射，则对于每一个密文，都有，暨在模意义下有唯一逆元，记为，暨，由带余除法可求使得。由恒等变换，有，可知。

（批改关键点为证明单射，证明满射，）

**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。

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

按照此表进行翻译，结果为：LOVE IS THE ONE THING THAT TRANSCENDS TIME AND SPACE.

* 1. 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）。

单表代替密码安全性不足以抵抗唯密文攻击，明文稍长时只需要通过字母频率统计，再对双音节、多音节词根词缀或密文单词进行频率统计，形成对应关系，就能基本破译其内容。

* 1. 【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？

长句句式丰富，覆盖到的字母范围大且较为均匀，形成的密钥较长，可以避免尾部依次排列的字母过多。

\*从破译难度上出发，合理即可

**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 |

DRTHHOADIKEBXPRVARLIAPHDMAALHSPNBTMBADMAQKDGZUHOLRBARZ

1. 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。

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

加密结果也为：

DRTHHOADIKEBXPRVARLIAPHDMAALHSPNBTMBADMAQKDGZUHOLRBARZ

1. 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）

（1）的矩阵循环下移两行左移一行就成了（2）的矩阵。Playfair矩阵上下、左右平移不影响加密结果。

1. 【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）。

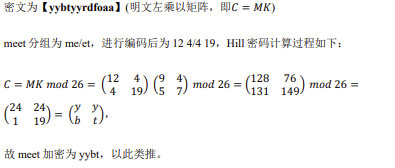
全排列共计，矩阵循环移位共有25种可能，故密钥空间大小。

**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。

标准答案：UKIXUKYDLPAA（需有第一个词的计算过程）

\*本题由于教材对左乘右乘存在前后不一致性，可能出现其他答案（或排列明文的方法差别也可能导致答案不同），应结合其过程判断正误，如下图所示。



1. 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。

逆矩阵为，要求同上。

1. 请描述Hill密码的已知明文攻击方案。

设密钥矩阵为阶方阵，选取通过已知明文攻击获得的明密文对组成明密文矩阵（如果矩阵不可逆则重新选择），计算密钥矩阵。

1. 【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。

选择这样一组明文（按照映射关系，1代表B, 0代表A）：,满足第个明文只有第个元素为1，其它均为0，则Hill密码对第个明文加密出来的密文对就是Hill密码密钥矩阵的第列，只需要把这些结果按顺序拼起来，就获得了Hill密码的密钥矩阵。

**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”。

LXCOHNNWPOA

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

ylfhptqapqkncl

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

[16,8,17,20,22,12,16,5,11,4,22,0,24,13]

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

J&@GW?\X4KQW-B@9

**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）。

如果有一行是偶的，那么必然满足判别式ad-bc是偶的。不妨假设第一行是偶的，则第一行两个元素的取值为{0,2,...,22,24}共13个，第二行取值不做限制，各个元素之间取值不相关，共有种可能；第二行是偶的第一行不做限制同理。两种情形加和，将“两行都是偶的”这种情况计算了两次，需要减去一次，两行都是偶的，即四个元素都是偶的，共有种可能，故总计有种可能。

1. 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。

同(1)，也为种可能。

1. 判定如下矩阵的个数：判别式为偶数，且其所有元素为奇数。

所有元素为奇数，自然判别式也为偶的。每个元素共有13种取值[1,3,...,23,25]，总计有种可能。

1. 考虑重叠情况，找出判别式为偶的矩阵总数。

(1)和(2)中会将有不少于三个偶数元素的情况重复统计。先考虑3偶1奇的情况，存在一个位置为奇数，这样的位置共有4个，剩下的位置为偶数，不论是奇数还是偶数，都有13种选择，故这样的可能共有，再考虑4个位置都为偶数的情况，和4个位置都为奇数一样，共有种可能。因此总的判别式为偶数的个数为个。

1. 【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。

第一列的两个值有两个选择{0,13}，第二列的两个值各有26种选择，故总计有种可能。

1. 【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。

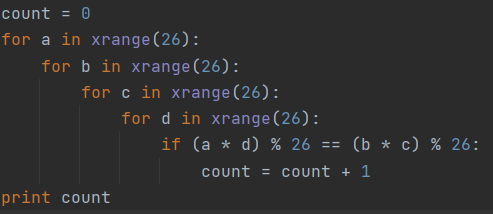
第二列在模13的意义下是第一列的倍数，即为0到12倍，共13种可能。也就是说给定第一列的值，第二列在模13的意义下共有13种取值。由于数字的选取区间是[0,25],因此给定倍数之后，每个元素依旧有两种取值(如果取值合法，那么取值必然也合法且二者在模26意义下不相等)。第一列的两个值是任取的，但不得都取0和13，否则第一列是13的倍数，故第一列的选取可能有，总的可能数为。

1. 【选做】计算判别式为13的倍数的所有矩阵个数。

6）已经包含了第二列为13的倍数的情况（如果第二列为13的倍数，则其在模13意义下一定是第一列的0倍），因此（5）和（6）构成了互斥的、判别式为13的倍数的全集，只需将二者加和，共计37648种可能。

1. 【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。

要找到所有的使 成立的值，其中。可以穷举：



结果为：23530种。

1. 【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。

答案为：。

1. 概念题
   1. 一个保密系统一般是 明文 、 密文 、 密钥 、 加密算法 、 解密算法 5部分组成的
   2. 密码攻击的五种类型分别是唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击、选择文本攻击
   3. 密码体制是指实现加密和解密功能的密码方案，从使用密钥策略上，可分为 对称密码 和 非对称密码 。
   4. 对称密码体制包括 分组密码 和 流密码

**注意：**

以上作业请使用**pdf**文档格式提交，于**2022年3月20日（星期日）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“20371234\_张三\_密码学第二次作业”。