# 密码学基础-作业1

提交截止时间：2022年9月28日24：00； 提交方式：邮箱发送至crypto\_2022@163.com

命名格式：邮件、文件均为学号-姓名

1. 用维吉尼亚算法加密某明文，已知密钥是：zelda，加密所得密文为：AVPDTGSQWHDATOD，请问该密文对应的明文是？

解：

首先将密钥扩展为与密文同样的长度（15位）：zeldazeldazelda

然后根据加密解密规则，查表知，明文为：

BREATHOFTHEWILD

1. 已知密码体制为普莱菲尔密码（Playfair Cipher），密钥为：davidbowie，明文为ground control to major tom，请问该明文对应的密文为？（注：不需要考虑空格）

解：

根据密钥编制密码表为：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| d | a | v | i(j) | b |
| o | w | e | c | f |
| g | h | k | l | m |
| n | p | q | r | s |
| t | u | x | y | z |

明文两两分组为：gr ou nd co nt ro lt om aj or to mx

由加密规则知，密文为：

lnwttofwtdncgyfgvbcndgkz

1. 给定比特串，记为的按位取反。证明以下有关DES算法的结论：
   1. 如果，那么。其中，为明文，为经过DES加密得到的密文，为密钥。（提示：对于任意的比特串A和B，）
   2. 假设攻击者Malice可以进行选择明文攻击，获得*X*及的密文。若Malice对DES加密进行穷举攻击(Brute-force attack)，则可以根据（1）中的结论将搜索空间减半至。

解：

（1）

1. 求有限域*GF* (2)上多项式，和的和与乘积。
2. 设有限域的不可约多项式为，求多项式和在中的乘积。