# 2024 物联网安全 HW1

1. 利用仿射加密破解密文：

xsnusanmxxcnicjnmasjgwjbbsachbuhsjgvwhtsimxwhtsquwvwhtsimxwhxciwtscjbctzuwhhwjgubtzsjgcntujqsxxscjtsqusjtzuphwsjatuvpkatuvtzuxsnusazwhbtcwfcsbbuxsiwikwjbatsnnjuaajcujtzmaswaqnchufuhjcmjurvuitubzwvvujsjgcnamhvhsasjgwjbvxuwasjgaccjxkasxujtxkwaeqkauxnsjqsjbjurtzwvvsjuaayzujysxxicqu

英文字母词频如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| 字母  | 概率  | 字母  | 概率  |
| A  | 0.082  | N  | 0.067  |
| B  | 0.015  | O  | 0.075  |
| C  | 0.028  | P  | 0.019  |
| D  | 0.043  | Q  | 0.001  |
| E  | 0.127  | R  | 0.060  |
| F  | 0.022  | S  | 0.063  |
| G  | 0.020  | T  | 0.091  |
| H  | 0.061  | U  | 0.028  |
| I  | 0.070  | V  | 0.010  |
| J  | 0.002  | W  | 0.023  |
| K  | 0.008  | X  | 0.001  |
| L  | 0.040  | Y  | 0.020  |
| M  | 0.024  | Z  | 0.001  |

密文字母词频统计如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| 字母  | 概率  | 字母  | 概率  |
| A  | 20 | N  | 11 |
| B  | 12  | O  | 0  |
| C  | 17 | P  | 2  |
| D  | 0  | Q  | 7  |
| E  | 1  | R  | 2  |
| F  | 2  | S  | 30  |
| G  | 7  | T  | 18  |
| H  | 14  | U  | 28  |
| I  | 8  | V  | 11  |
| J  | 29  | W  | 20  |
| K  | 5  | X  | 17  |
| L  | 0  | Y  | 2  |
| M  | 7  | Z  | 9  |

请补充下表：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 密文 | x | s | n | u | s | a | n |
| Y | 23 | 18 | 13 | 20 | 18 | 0 | 13 |
| x=1/a(y-b) |  |  |  |  |  |  |  |
| x mod 26 |  |  |  |  |  |  |  |
| 明文 |  |  |  |  |  |  |  |

2. 根据下面DES加密流程图填空

1）初始明文M=0123456789ABCDEF，经过初始IP置换后的比特明文分组是\_\_\_\_\_\_\_（16进制）

2）明文分组R0经过扩展置换之后的长度是\_\_\_\_\_\_，置换后的R0是\_\_\_\_\_\_\_(16进制)

3）假定第一轮子密钥K1=1B02EFFC7072，则根据以下S盒，计算S盒输出的结果的前4位是\_\_\_\_\_\_\_（2进制）

初始置换IP和扩展置换E:



S盒变换：



3.在RSA加密中，给定p=7，q=11，e=7，计算解密密钥d=\_\_\_\_\_\_\_\_