HW4

1. 在 RSA 密码体制中，已知 p=3，q=7，同时选择 e=5 则其私钥 d 是多少？

答案：5。

2. 利用仿射加密破解密文：

Pu yfo of oin hvy ufa hrpkpyb, jlar ph hopkk py oin hvy oinan, svo jnjpkk klvbi rfan zfyupgnyo zlkr; pu ovayng of ufvyg iph fjy hilgfj, lmmafmaplon nhzlmn, oin hvy jpkk sn oiafvbi oin inlao,jlar nlzi mklzn snipyg oin zfayna; pu ly fvohoanozing mlkr zlyyfo ulkk svoonaukx, oiny zknyzing jlcpyb larh, bpcny mfjna; pu P zly'o ilcn sapbio hrpkn, po jpkk ulzn of oin hvyhipyn, lyg hvyhipyn hrpkn ofbnoina, py uvkk skffr.（大小写无关）

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

频数分布

字母	频数	字母	频数
A	18	N	37
B	7	O	30
C	3	P	26
D	0	Q	0
E	0	R	10
F	19	S	6
G	8	T	0
H	17	U	11
I	23	V	13
J	10	W	0
K	22	X	1
L	21	Y	27
M	7	Z	12

请补充完整下表：

密文	p	U	y	f	o	o	F
Y	15	20	24	5	14	14	5
x=1/a(y-b)							
x mod 26							
明文							

答案：

根据密文的频率统计，假设服从英文字母的频率分布特性，密钥为(a,b)。e 和 n; t 和 o 具有映射关系，根据加密表达式 y=ax+b，求得 a=7,b=11。

(A 用 0 代替，B 用 1 代替，以此类推；a,b 求解注意要在 Z26 上满足公约数要求，且需要提前求出 a 的逆元)：

密文	p	U	y	f	o	o	F
Y	15	20	24	5	14	14	5
x=1/a(y-b)	60	135	195	-90	45	45	-90
x mod 26	8	5	13	14	19	19	14
明文	I	F	N	O	T	Y	O

HW5

1. **阅读下面的程序，分析其中的漏洞及其成因，并写出建议的改进方式。**

```
#0   #include <stdio.h>
#1
#2    int main(void){
#3         int size;
#4         char buf[100];
#5
#6         printf(“input length:\n”);
#7         scanf(“%d”, &size);
#8
#9         printf(“input context:\n”);
#10        read(0, buf, size);
#11
#12        return 0;
#14   }
```

答案：#7 和#10 存在缓冲区溢出漏洞，原因：#7 中用户可以控制 size 大小，但是程序没有检查 size 大小是否超过缓冲区大小，int 类型的 size 可以远大于 100，导致 read 时缓冲区溢出。

改进方式：在#10 代码之前，加入针对 size 的检查：

```
if (size>100) {
      printf(“error”);
      … }
```