《计算机网络安全》重点内容 2

1.在凯撒密码中，密钥 k=6，制造一张明文字母与密文字母对照表。

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

2.已知线性替代密码的变换函数为：f(a)=ak mod 26；设已知明码字符 J(9)对应于密文字母 P(15)；即 9k mode 26=15，试求密钥 k 以破译此密码。

答：k = 19
解：9k ≡ 15 (mod 26)。
设整数 x，使得 9x ≡ 1 (mod 26)。
根据扩展欧几里得算法，求得 x=3 为 9 在模数 26 下的逆元。
得 k ≡ 15x ≡ 15*3 ≡ 45 ≡ 19 (mod 26)。
因此，密钥 k=19，可以用它对密文进行解密。

3.对于给定的明文“computer”，使用加密函数 E(m)=(3m+2) mod 26 进行加密，其中 m 表示明文中被加密字符在字符集合{a，b，c，d，e，f，g，h，i，j，k，l，m，n，o，p，q，r，s，t，u，v，w，x，y，z}中的序号，序号依次为 0 到 25，请写出加密后的密文，并给出相应的加密过程。

将明文转化为数字序列，即：

c	o	m	p	u	t	e	r
2	14	12	15	20	19	4	17

加密过程：

加密字符	序号 m	(3m+2) mod 26	密文字母
c	2	8	i
o	14	44 ≡ 18	s

m	12	38 ≡ 12	m
p	15	47 ≡ 21	m
u	20	62 ≡ 10	v
t	19	59 ≡ 7	k
e	4	14	h
r	17	53 ≡ 1	b

得，明文“computer”经过加密后的密文为“ismmvkhb”。

4.在凯撒密码中，密钥 k=8，制造一张明文字母与密文字母对照表。

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

5.对于给定的明文“internet”，使用加密函数 E(m)=(3m+6) mod 26 进行加密，其中 m 表示明文中被加密字符在字符集合{a，b，c，d，e，f，g，h，i，j，k，l，m，n，o，p，q，r，s，t，u，v，w，x，y，z}中的序号，序号依次为 0 到 25，请写出加密后的密文，并给出相应的加密过程。

将明文转化为数字序列，即：

i	n	t	e	r	n	e	t
8	13	19	4	17	13	4	19

加密过程：

加密字符	序号 m	(3m+2) mod 26	密文字母
c	8	30 ≡ 4	e
o	13	45 ≡ 19	t
m	19	63 ≡ 11	l
p	4	18	s
u	17	57 ≡ 5	f
t	13	45 ≡ 19	t
e	4	18	s
r	19	63 ≡ 11	l

得，明文“internet”经过加密后的密文为“etlsftls”。