【例 14-1】仿射密码是替换密码的一个特例。

加密函数取形式为：

$e(x)=(ax+b)\bmod(26), a,b\in Z/(26)$

加密函数：$e_k(x)=(ax+b)\bmod(26)$

解密函数：$d_k(y)=a^{-1}(y-b)\bmod(26)$

$a,b,x,y\in Z/(26)$

设密钥 $K=(7,3),$　　注：$7^{-1}(\bmod 26)=15$

加密函数：$e_k(x)=7x+3$，若加密明文为 hot，请分别给出加密过程和解密过程

解：

解密函数：$d_k(y)=15(y-3)=15y-19$

易见 $d_k(e_k(x))=d(7x+3)=15(7x+3)-19$

$=105x+45-19(\bmod 26)$

$=x$

首先转换字母 hot 成为数字 7,14,19, 然后加密：

加密过程：

$$\left(7\begin{bmatrix}7\\14\\19\end{bmatrix}\right)+\begin{bmatrix}3\\3\\3\end{bmatrix}\bmod 26=\begin{bmatrix}0\\23\\6\end{bmatrix}=\begin{bmatrix}A\\X\\G\end{bmatrix}$$

即加密报文为 AXG

解密过程：

$$\left(15\begin{bmatrix}0\\23\\6\end{bmatrix}-\begin{bmatrix}19\\19\\19\end{bmatrix}\right)\bmod 26=\begin{bmatrix}7\\14\\19\end{bmatrix}=\begin{bmatrix}h\\o\\t\end{bmatrix}$$

【例 14-2】在 RSA 算法中，设 $p=11$，$q=23$，明文为 $m=165$，试设计公钥和私钥并求出所产生的密文。根据公开钥和秘密钥，若密文 $c=110$，试求明文。

解：由 RSA 算法，可得

$$n=p\times q=253,\ \varphi(n)=(p-1)(q-1)=10\times 22=220$$

可以选取加密密钥 $e=3$，显然满足 $\gcd(3,220)=1$，确定满足 $d\bullet e=1\bmod 220$ 且小于 220 的 d，因为 $3\times 147\equiv 1\bmod 220$，故解密密钥 $d=147$。

由于明文 $m=165$，可以得到密文 $c=165^3 \bmod 253=110$。

对于密文 $c=110$，可以得到明文 $m=110^{147} \bmod 253=165$。

所以对于此题，公钥为 $\{3,253\}$，私钥为 $\{147,253\}$。

【例 14-3】在 Diffie-Hellman 公共密钥分配系统中，密钥交换基于素数 $p=97$，和本原元 $\alpha=5$。A 和 B 分别选择随机数 $X_A=36$ 和 $X_B=58$。试求 A 和 B 的公开密钥，以及他们共享的会话密钥。

解：对于 A，其公开密钥为

$$Y_A=5^{36}\bmod 97=50\bmod 97=50$$

对于 B，其公开密钥为

$$Y_B=5^{58}\bmod 97=44\bmod 97=44$$

在他们交换了公开密钥后，A 计算共享的会话密钥为

$$K=Y_B{}^{X_A}\bmod p=44^{36}\bmod 97=75\bmod 97=75$$

A 计算共享的会话密钥为

$$K = Y_A^{X_B} \bmod p = 50^{58} \bmod 97 = 75 \bmod 97 = 75$$

由上可得，A 和 B 所得到并使用的会话密钥是一样的。知道了$\{97,5,50,44\}$，攻击者要计算出 75 是不容易的。