No.

Date.　　/　　/

1、(1) 对于仿射密码，$P=C=\mathbb{Z}_{26}$，$K=\{(a,b)\in \mathbb{Z}_{26}\times \mathbb{Z}_{26};\ \gcd(a,26)=1\}$

$e_k(x)=(ax+b) \bmod 26$

∵ $x,y\in \mathbb{Z}_{26}$　∴ $Pr[Y=y]=\sum_{k\in\cdots} Pr[K=k]\ Pr[x=d_k(y)]$

$=\sum_{k\in\cdots}\frac{1}{312} Pr[x=a^{-1}(y+b)]$

$=\frac{1}{312}\sum_{k\in\cdots} Pr[x=a^{-1}(y-b)]$

易知，$a\in A$，$|A|=12$，$b\in \mathbb{Z}_{26}$，$K=(a,b)\in A\times \mathbb{Z}_{26}$

∴固定y,a，则$a^{-1}(y-b)$构成$\mathbb{Z}_{26}$的一個置换

固定y,b，则$a^{-1}(y-b)$构成A的一个置换

∴ $\sum_{k\in A\times \mathbb{Z}_{26}} Pr[x=a^{-1}(y-b)]=\sum_{x\in \mathbb{Z}_{26}} Pr[X=x]\times 12=12$

∴ $\forall y\in \mathbb{Z}_{26}$，有 $Pr[y]=\frac{1}{26}$

∴ $\forall x,y\in \mathbb{Z}_{26}$，$Pr[y|x]=Pr[K=(y-x) \bmod 26]\times 12$

$=\frac{1}{312}\times 12=\frac{1}{26}$

∴ $Pr[x|y]=\frac{Pr[x]Pr[y|x]}{Pr[y]}$

$=\frac{Pr[x]\frac{1}{26}}{\frac{1}{26}}=Pr[x]$

∴仿射密码是完善保密的

(2) $\forall x\in P, y\in C$

$Pr[y|x]=\sum_{(a,b)\in K} Pr[(a,b)]=\sum_{a\in A} Pr[a]\cdot\frac{1}{26}=\frac{1}{26}\sum_{a\in A} Pr[a]=\frac{1}{26}$

∴ $Pr[y]=\sum_{x'\in P} Pr[x']Pr[y|x']=\frac{1}{26}$

$Pr[x|y]=\frac{Pr[y|x]Pr[x]}{Pr[y]}=Pr[x]$

∴成立