1）给出机密性、完整性、认证性、可用性及不可抵赖性的名词解释；列举出至少一个近年来的发生的信息安全事件，并说明该事件是危害了哪个（或哪几个）特性；

2）令仿射密码的密钥 k=(9,3), 且 gcd(9,26)=1.

明文 bupt=(1,20,15,19)，求加解密过程。

3）用维吉尼亚密码加密明文“please keep this message in secret”，其中使用的密钥为“computer”，试求其密文。

4） 用 Hill 密码加密明文“bupt”，使用的密钥是

$$k=\begin{pmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{pmatrix}$$

试求其密文。

5) 明文“friday”用 m=2 的 Hill 密码加密后得到密文“PQCFKU”，求 Hill 密码的密钥。

6）证明：$H(X,Y) \le H(X) + H(Y)$，当且仅当 X 和 Y 统计独立时等号成立。