No.

Date / /

密码.

作业1.

1. ①机密性：信息不泄露给非授权实体.

②认证性：消息来源或实体本身被正确标识.

③完整性：未经授权不可篡改消息.

④可用性：保障资源随时可提供服务.

⑤不可抵赖性：用户不能否认事后否认信息生成行为.

事件：~~2024年7月 CrowdStrike大规模蓝屏事件~~.

2020年 SolarWinds 供应链攻击，危害机密性，完整性，认证性.

2. 加密：$1\times9+3\equiv12 \bmod 26$. $20\times9+3\equiv1 \bmod 26$

$15\times9+3\equiv8 \bmod 26$ $19\times9+3\equiv18 \bmod 26$

密文(12,1,8,18) = ~~cbhs~~. mbis

解密：$9^{-1}\equiv3 \bmod 26$

$(12-3)\times3\equiv1 \bmod 26$ $(1-3)\times3\equiv20 \bmod 26$

$(8-3)\times3\equiv15 \bmod 26$ $(18-3)\times3\equiv19 \bmod 26$.

明文(1,20,15,19) = bupt.

3. 明文(15,11,4,0,18,4,10,4,4,15,19,7,8,18,12,4,18,18,0,6,4,8,13,18,4,2,17,4,19)

密钥(2,14,12,15,20,19,4,17).

密文：(17,25,16,15,12,23,14,21,6,3,5,22,2,11,16,21,20,6,12,21,24,1,17,9,6,16,3,19,13).

= rzqpmxovgdfwclqvugmvybrjgqdtn.

No.

Date / /

4. 明文 bupt = (1, 20, 15, 19).

加密: $(1,20,15,19)\times\begin{pmatrix}8&6&9&5\\6&9&5&10\\5&8&4&9\\10&6&11&4\end{pmatrix}\equiv(3,4,14,0) \mod 26$

密文为 deoa.

5. 明文 friday: $\begin{pmatrix}5&17\\8&3\\0&24\end{pmatrix}$ 密文 PQCFKU: $\begin{pmatrix}15&16\\2&5\\10&20\end{pmatrix}$.

密钥 $k=\begin{pmatrix}k_{11}&k_{12}\\k_{21}&k_{22}\end{pmatrix}$. 即 $\begin{pmatrix}5&17\\8&3\\0&24\end{pmatrix}\times\begin{pmatrix}k_{11}&k_{12}\\k_{21}&k_{22}\end{pmatrix}\equiv\begin{pmatrix}15&16\\2&5\\10&20\end{pmatrix} \mod 26$.

解得 $k=\begin{pmatrix}7&19\\8&3\end{pmatrix}$

6. 证明: $H(X,Y)=H(X)+H(X|Y)\leq H(X)+H(Y)$.

$\because H(X|Y)\leq H(X)$

$\therefore H(X,Y)\leq H(Y)+H(X)$.

当 X, Y 独立时, $H(X|Y)=H(X)$ $\therefore H(X,Y)=H(X)+H(Y)$ 等号成立.

综上, 得证结论.