现代密码学

第二讲 作业

作业

1）令仿射密码的密钥k=(9,3), gcd(9,26)=1.
明文hot=(7,14,19)，求加解密过程。

2）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。

3）用Hill密码加密明文“hill”，使用的密钥是

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

作业

4）试设计实现仿射密码和单表代换密码：给出密钥生成（ 随机选择小于26的数、选择和26互素的密钥；以及生成0-25上的一个随机置换）、加解密的伪代码;

5）给出移位、仿射、单表代换、维吉尼亚密码、多表代换（每个密钥是一个单表代换）、置换密码 穷尽搜索的复杂度（即密钥空间大小）。

6）区分单表代换、多表代换、置换密码、希尔密码，哪个属于分组加密范畴，为什么？

作业

7) 已知下列密文是通过维吉尼亚密码加密得来的，试求其明文。

Per zlrracm, vxmcs r qipqlczhs. Qs fcv rihw sxx hblrxh sm nkidhvzphw. Ixxvn qsn, lysh sifecs uui jrrfyg, mk xj suvc kd ss wbrzrrz uqh jpp zyw qv ylgn osfz fin isi bpgyoj, fg dm zdqzap, cl sifecs qks cdfy iu xyxey iu tipp zcni dt. Sin lj nt rfy jszcx hi jik iyfixky iysmh hzuwwwxpk izayv; mw lv olh kfxeu nr gitrhy d afgcr qkiit vjyucsdum bdw kwv cjssiilbcwc kd wwhg e ads, ohg ewuffx fscavuy; lj nt rfy jszcx hi vemt kvy hrmxichpiei rbx giwtrh zxxlgv duqhvbzqm, wlvc ns uui xdzba ws ypms nr hf xk hijikwvf.