第二次作业

1. 使用穷尽密钥搜索方法破译如下利用移位密码加密的密文

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD

1. （a）设下列的π是集合{1, 2, … , 8}上的置换：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| π(x) | 4 | 1 | 6 | 2 | 7 | 3 | 8 | 5 |

求出逆置换π-1。

（b）解密下列使用置换密码加密的密文，密钥是（a）中的置换π。

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM

1. 一下给出的四段密文，第一个是由代换密码加密而成，第二个是由维吉尼亚密码加密而成，第三个是由仿射密码加密而成，最后一个不知其具体的密码体制，试从密文确定明文。要求给出清晰的分析过程，包括统计分析和你进行的计算。
2. 代换密码

EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCK

QPKUGKMGOLICGINCGACKSNISACYKZSCKXECJCKSHYSXCG

OIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZU

GFZCCNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNS

ACIGOIYCKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNC

IACZEJNCSHFZEJZEGMXCYHCJUMGKUCY

提示：F解密为w。

（b）维吉尼亚密码

KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD

DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC

QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL

SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV

GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFS

PEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI

FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY

CWHJVLNHIQIBTKHJVNPIST

（c）仿射密码

KQEREJEBCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUP

KRIOFKPACUZQEPBKRXPEIIEABDKPBCPFCDCCAFIEABDKP

BCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFF

ERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPERK

IVKSCPICBRKIJPKABI

(d)未知具体密码

BNVSNSIHQCEELSSKKYERIFJKXUMBGYKAMQLJTYAVFBKVT

DVBPVVRJYYLAOKYMPQSCGDLFSRLLPROYGESEBUUALRWXM

MASAZLGLEDFJBZAVVPXWICGJXASCBYEHOSNMULKCEAHTQ

OKMFLEBKFXLRRFDTZXCIWBJSICBGAWDVYDHAVFJXZIBKC

GJIWEAHTTOEWTUHKRQVVRGZBXYIREMMASCSPBHLHJMBLR

FFJELHWEYLWISTFVVYEJCMHYUYRUFSFMGESIGRLWALSWM

NUHSIMYYITCCQPZSICEHBCCMZFEGVJYOCDEMMPGHVAAUM

ELCMOEHVLTIPSUYILVGFLMVWDVYDBTHFRAYISYSGKVSUU

HYHGGCKTMBLRX