report

陈张萌 2017013678

1.21(2)Virginia密码

得到密钥长度

先计算单词出现概率：

{'C': 24, 'K': 20, 'T': 19, 'V': 18, 'G': 16, 'F': 16, 'D': 16, 'R': 16, 'P': 15, 'S': 15, 'B': 14, 'H': 14, 'A': 14, 'I': 14, 'W': 14, 'Q': 12, 'L': 11, 'N': 10, 'E': 10, 'J': 10, 'Y': 8, 'X': 7, 'Z': 7, 'M': 6, 'O': 6, 'U': 5, ' ': 1} {'HJ': 5, 'JV': 5, 'KF': 4, 'YC': 4, 'SP': 4, 'KC': 3, 'FD': 3, 'GC': 3, 'AC': 3, 'CW': 3, 'FT': 3, 'CG': 3, 'FS': 3, 'VL': 3, 'RW': 3, 'BB': 3, 'PK': 2, 'GU': 2, 'DP': 2, 'TY': 2, 'NR': 2, 'TM': 2, 'MV': 2, 'VG': 2, 'DN': 2, 'BV': 2, 'VF': 2, 'ET': 2, 'LT': 2, 'DD': 2, 'DK': 2, 'TF': 2, 'CK': 2, 'KQ': 2, 'QR': 2, 'CQ': 2, 'WD': 2, 'AW': 2, 'WC': 2, 'XC': 2, 'HK': 2, 'ON': 2, 'JU': 2, 'QD': 2, 'DY': 2, 'AH': 2, 'HC': 2, 'CT': 2, 'RL': 2, 'LS': 2, 'SV': 2, 'ZQ': 2, 'AF': 2, 'RJ': 2, 'FP': 2, 'IS': 2, 'EB': 2, 'WX': 2, 'VY': 2, 'KA': 2, 'WB': 2, 'BI': 2, 'LN': 2, 'NH': 2, 'HI': 2, 'TK': 2, 'QI': 2, 'CC': 1, 'CP': 1, 'KB': 1, 'BG': 1, 'UF': 1, 'PH': 1, 'HQ': 1, 'QT': 1, 'YA': 1, 'AV': 1, 'VI': 1, 'IN': 1, 'RR': 1, 'RT': 1, 'GR': 1, 'RK': 1, 'KD': 1, 'NB': 1, 'DE': 1, 'TD': 1, 'DG': 1, 'GI': 1, 'IL': 1, 'TX': 1, 'XR': 1, 'RG': 1, 'UD': 1, 'KO': 1, 'OT': 1, 'FM': 1, 'MB': 1, 'BP': 1, 'PV': 1, 'GE': 1, 'EG': 1, 'GL': 1, 'TG': 1, 'RA': 1, 'QC': 1, 'NA': 1, 'CR': 1, 'RX': 1, 'XI': 1, 'IZ': 1, 'ZA': 1, 'AK': 1, 'TL': 1, 'LE': 1, 'EW': 1, 'WR': 1, 'RP': 1, 'PT': 1, 'QK': 1, 'KY': 1, 'YV': 1, 'VX': 1, 'CH': 1, 'TP': 1, 'PO': 1, 'NC': 1, 'CO': 1, 'OQ': 1, 'RH': 1, 'VA': 1, 'AJ': 1, 'UW': 1, 'WE': 1, 'MC': 1, 'CM': 1, 'MS': 1, 'YH': 1, 'VD': 1, 'DA': 1, 'TR': 1, 'VS': 1, 'SK': 1, 'CZ': 1, 'QQ': 1, 'DZ': 1, 'ZX': 1, 'XG': 1, 'GS': 1, 'SF': 1, 'FR': 1, 'SW': 1, 'WS': 1, 'SJ': 1, 'JT': 1, 'TB': 1, 'BH': 1, 'HA': 1, 'SI': 1, 'IA': 1, 'AS': 1, 'PR': 1, 'JA': 1, 'KJ': 1, 'JR': 1, 'UM': 1, 'V ': 1, ' G': 1, 'GK': 1, 'KM': 1, 'MI': 1, 'IT': 1, 'TZ': 1, 'ZH': 1, 'HF': 1, 'PD': 1, 'DI': 1, 'PZ': 1, 'ZL': 1, 'LV': 1, 'LG': 1, 'GW': 1, 'WT': 1, 'PL': 1, 'LK': 1, 'KK': 1, 'KE': 1, 'BD': 1, 'PG': 1, 'CE': 1, 'BS': 1, 'SH': 1, 'TU': 1, 'UR': 1, 'XB': 1, 'BA': 1, 'PE': 1, 'EZ': 1, 'QN': 1, 'CV': 1, 'GA': 1, 'AO': 1, 'NW': 1, 'IK': 1, 'TI': 1, 'IO': 1, 'OV': 1, 'VK': 1, 'GG': 1, 'GH': 1, 'IF': 1, 'FF': 1, 'SQ': 1, 'QE': 1, 'ES': 1, 'CL': 1, 'LA': 1, 'CN': 1, 'NV': 1, 'VR': 1, 'IR': 1, 'RE': 1, 'EP': 1, 'PB': 1, 'FE': 1, 'EX': 1, 'XO': 1, 'OS': 1, 'SC': 1, 'CD': 1, 'YG': 1, 'GZ': 1, 'ZW': 1, 'WP': 1, 'PF': 1, 'DT': 1, 'FQ': 1, 'IY': 1, 'WH': 1, 'IQ': 1, 'IB': 1, 'BT': 1, 'KH': 1, 'VN': 1, 'NP': 1, 'PI': 1, 'ST': 1} {'HJV': 5, 'KFT': 3, 'BVF': 2, 'DDK': 2, 'HCT': 2, 'RLS': 2, 'KCG': 2, 'AFS': 2, 'RWX': 2, 'VYC': 2, 'WBB': 2, 'BBI': 2, 'JVL': 2, 'VLN': 2, 'LNH': 2, 'NHI': 2, 'KCC': 1, 'CCP': 1, 'CPK': 1, 'PKB': 1, 'KBG': 1, 'BGU': 1, 'GUF': 1, 'UFD': 1, 'FDP': 1, 'DPH': 1, 'PHQ': 1, 'HQT': 1, 'QTY': 1, 'TYA': 1, 'YAV': 1, 'AVI': 1, 'VIN': 1, 'INR': 1, 'NRR': 1, 'RRT': 1, 'RTM': 1, 'TMV': 1, 'MVG': 1, 'VGR': 1, 'GRK': 1, 'RKD': 1, 'KDN': 1, 'DNB': 1, 'NBV': 1, 'VFD': 1, 'FDE': 1, 'DET': 1, 'ETD': 1, 'TDG': 1, 'DGI': 1, 'GIL': 1, 'ILT': 1, 'LTX': 1, 'TXR': 1, 'XRG': 1, 'RGU': 1, 'GUD': 1, 'UDD': 1, 'DKO': 1, 'KOT': 1, 'OTF': 1, 'TFM': 1, 'FMB': 1, 'MBP': 1, 'BPV': 1, 'PVG': 1, 'VGE': 1, 'GEG': 1, 'EGL': 1, 'GLT': 1, 'LTG': 1, 'TGC': 1, 'GCK': 1, 'CKQ': 1, 'KQR': 1, 'QRA': 1, 'RAC': 1, 'ACQ': 1, 'CQC': 1, 'QCW': 1, 'CWD': 1, 'WDN': 1, 'DNA': 1, 'NAW': 1, 'AWC': 1, 'WCR': 1, 'CRX': 1, 'RXI': 1, 'XIZ': 1, 'IZA': 1, 'ZAK': 1, 'AKF': 1, 'FTL': 1, 'TLE': 1, 'LEW': 1, 'EWR': 1, 'WRP': 1, 'RPT': 1, 'PTY': 1, 'TYC': 1, 'YCQ': 1, 'CQK': 1, 'QKY': 1, 'KYV': 1, 'YVX': 1, 'VXC': 1, 'XCH': 1, 'CHK': 1, 'HKF': 1, 'FTP': 1, 'TPO': 1, 'PON': 1, 'ONC': 1, 'NCO': 1, 'COQ': 1, 'OQR': 1, 'QRH': 1, 'RHJ': 1, 'JVA': 1, 'VAJ': 1, 'AJU': 1, 'JUW': 1, 'UWE': 1, 'WET': 1, 'ETM': 1, 'TMC': 1, 'MCM': 1, 'CMS': 1, 'MSP': 1, 'SPK': 1, 'PKQ': 1, 'KQD': 1, 'QDY': 1, 'DYH': 1, 'YHJ': 1, 'JVD': 1, 'VDA': 1, 'DAH': 1, 'AHC': 1, 'CTR': 1, 'TRL': 1, 'LSV': 1, 'SVS': 1, 'VSK': 1, 'SKC': 1, 'CGC': 1, 'GCZ': 1, 'CZQ': 1, 'ZQQ': 1, 'QQD': 1, 'QDZ': 1, 'DZX': 1, 'ZXG': 1, 'XGS': 1, 'GSF': 1, 'SFR': 1, 'FRL': 1, 'LSW': 1, 'SWC': 1, 'WCW': 1, 'CWS': 1, 'WSJ': 1, 'SJT': 1, 'JTB': 1, 'TBH':

1, 'BHA': 1, 'HAF': 1, 'FSI': 1, 'SIA': 1, 'IAS': 1, 'ASP': 1, 'SPR': 1, 'PRJ': 1, 'RJA': 1, 'JAH': 1, 'AHK': 1, 'HKJ': 1, 'KJR': 1, 'JRJ': 1, 'RJU': 1, 'JUM': 1, 'UMV': 1, 'MV ': 1, 'V G': 1, ' GK': 1, 'GKM': 1, 'KMI': 1, 'MIT': 1, 'ITZ': 1, 'TZH': 1, 'ZHF': 1, 'HFP': 1, 'FPD': 1, 'PDI': 1, 'DIS': 1, 'ISP': 1, 'SPZ': 1, 'PZL': 1, 'ZLV': 1, 'LVL': 1, 'VLG': 1, 'LGW': 1, 'GWT': 1, 'WTF': 1, 'TFP': 1, 'FPL': 1, 'PLK': 1, 'LKK': 1, 'KKE': 1, 'KEB': 1, 'EBD': 1, 'BDP': 1, 'DPG': 1, 'PGC': 1, 'GCE': 1, 'CEB': 1, 'EBS': 1, 'BSH': 1, 'SHC': 1, 'CTU': 1, 'TUR': 1, 'URW': 1, 'WXB': 1, 'XBA': 1, 'BAF': 1, 'FSP': 1, 'SPE': 1, 'PEZ': 1, 'EZQ': 1, 'ZQN': 1, 'QNR': 1, 'NRW': 1, 'WXC': 1, 'XCV': 1, 'CVY': 1, 'YCG': 1, 'CGA': 1, 'GAO': 1, 'AON': 1, 'ONW': 1, 'NWD': 1, 'WDD': 1, 'DKA': 1, 'KAC': 1, 'ACK': 1, 'CKA': 1, 'KAW': 1, 'AWB': 1, 'BIK': 1, 'IKF': 1, 'FTI': 1, 'TIO': 1, 'IOV': 1, 'OVK': 1, 'VKC': 1, 'CGG': 1, 'GGH': 1, 'GHJ': 1, 'HIF': 1, 'IFF': 1, 'FFS': 1, 'FSQ': 1, 'SQE': 1, 'QES': 1, 'ESV': 1, 'SVY': 1, 'YCL': 1, 'CLA': 1, 'LAC': 1, 'ACN': 1, 'CNV': 1, 'NVR': 1, 'VRW': 1, 'RWB': 1, 'BIR': 1, 'IRE': 1, 'REP': 1, 'EPB': 1, 'PBB': 1, 'BBV': 1, 'VFE': 1, 'FEX': 1, 'EXO': 1, 'XOS': 1, 'OSC': 1, 'SCD': 1, 'CDY': 1, 'DYG': 1, 'YGZ': 1, 'GZW': 1, 'ZWP': 1, 'WPF': 1, 'PFD': 1, 'FDT': 1, 'DTK': 1, 'TKF': 1, 'KFQ': 1, 'FQI': 1, 'QIY': 1, 'IYC': 1, 'YCW': 1, 'CWH': 1, 'WHJ': 1, 'HIQ': 1, 'IQI': 1, 'QIB': 1, 'IBT': 1, 'BTK': 1, 'TKH': 1, 'KHJ': 1, 'JVN': 1, 'VNP': 1, 'NPI': 1, 'PIS': 1}

计算重合指数：

```
m=1时重合指数为
[0.04052464312678875]
m=2时重合指数为
[0.046703296703296704, 0.038461538461538464]
m=3时重合指数为
[0.04665379665379665, 0.05501930501930502, 0.04858429858429859]
m=4时重合指数为
[0.047332185886402756, 0.03700516351118761, 0.043029259896729774,
0.037578886976477335]
m=5时重合指数为
[0.04251469923111714, 0.04296698326549073, 0.04296698326549073,
0.033921302578018994, 0.035278154681139755]
m=6时重合指数为
[0.06883116883116883, 0.06298701298701298, 0.08506493506493507,
0.04935064935064935, 0.06493506493506493, 0.04285714285714286]
m=7时重合指数为
[0.038120567375886524, 0.031914893617021274, 0.044326241134751775,
0.04343971631205674, 0.040780141843971635, 0.044326241134751775,
0.044326241134751775]
m=8时重合指数为
[0.04994192799070848, 0.0313588850174216, 0.041811846689895474,
0.03368176538908246, 0.04065040650406504, 0.03948896631823461,
0.04529616724738676, 0.04065040650406504]
m=9时重合指数为
[0.042042042042042045, 0.05105105105105105, 0.04054054054054054,
0.05855855855855856, 0.07057057057057058, 0.04054054054054054,
0.03453453453453453, 0.04354354354354354, 0.04804804804804805]
```

可以看到m=6时重合指数接近0.68，因此推测密钥长度为6

确定密钥内容

根据书上的算法，计算M_g，选择距离0.065最近的g即可。得到密钥为CRYPTO。 虽然我们发现误差仍然很大，推测是因为密文长度不够长导致的。

```
key=24  loss=0.00028571428571426416
C
key=9   loss=0.005196428571428574
R
key=2   loss=0.0062678571428571375
Y
key=11  loss=0.0010000000000000148
P
key=7   loss=0.009214285714285717
T
key=12  loss=0.005428571428571435
O
```

得到明文为：

ILEARNEDHOWTOCALCULATETHEAMOUNTOFPAPERNEEDEDFORAROOMWHENIWASATSCHOOLYOUMULTIPLYTHESQUAREFOOTAGEOFTHEWALLSBYTHECUBICCONTENTSOFTHEFLOORANDCEILINGCOMBINEDANDDOUBLEITYOUTHENALLOWHALFTHETOTALFOROPENINGSSUCHASWINDOWSANDDOORDTHENYOUALLOWTHEOTHERHALFFORMATCHINGTHEPATTERNTHENYOUDOUBLETHEWHOLETHINGAGAINTOGIVEAMARGINOFERRORANDTHENYOUORDERTHEPAPER