加密过程:

普通模拟, 略;

解密过程:

第一步,采用一定样本进行训练,整合出高频词。这里我用 nature、science、Time 上的一些文章、《百年孤独》英文版节选大约一万多个单词为样本进行训练、整合出前 1000 的高频词。

SampleText.txt - Notepad - X

Some 70 years ago, John Cade, an Australian psychiatrist, discovered a medication for bipolar disorder that helped many patients to regain stability swiftly. Lithium is now the standard treatment for the condition, and one of the most consistently effective medicines in psychiatry. But its rise was riddled with obstacles. The intertwined story of Cade and his momentous finding is told in Lithium, a compelling book by US psychiatrist Walter Brown.

Bipolar disorder, labelled manic-depressive illness until 1980, affects around 1 in 100 people globally. Without treatment, it can become a relentless cycle of emotional highs and lows. Suicide rates for untreated people are 10–20 times those in the general population. Fortunately, lithium carbonate — derived from the light, silvery metal lithium — can reduce that figure tenfold.

Brown's telling of Cade's eventful life covers much of the same ground as Finding Sanity (2016), a rather hagiographic biography by Greg de Moore and Ann Westmore. What Brown does superbly well is to show that Cade made his discovery without access to advances in technology or to modern facilities — and almost despite them. His finding was the happy result of being forced to work with the simplest of means.

During the Second World War, Cade was interred for more than three years in the notorious Japanese prisoner-of-war camp at Changi in Singapore. He was put in charge of the psychiatric section, where he began to note the decisive link between certain food deficiencies and diseases in his fellow prisoners. A lack of B vitamins, for instance, caused beriberi and pellagra.

After the war, he pursued his investigations. Working from an abandoned pantry in Bundoora Repatriation Mental Hospital near Melbourne, Australia, he began to collect urine samples from people with depression, mania and schizophrenia, aiming to discover whether some secretion in their urine could be correlated to their symptoms. With no access to sophisticated chemical analysis and largely unguided by theory, Cade injected the urine into the abdominal cavities of guinea pigs, raising the dose until they died. The urine of people with mania proved especially lethal to the

Figure 1 训练样本

Hash.txt - Notepad П File Edit Format View Help sample[0] = "the", sample[1] = "of", sample[2] = "to", sample[3] = "and", sample[4] = "a", sample[5] = "in", sample[6] = "in", sample[6][6] = "that", sample [7] = "was", sample [8] = "his", sample [9] = "for", sample [10] = "with", sample [11] = "he", sample [12] = "had", sample [13] = "on", sample [14] = "as", sample [15] = "by", sample [16] = "The", sample [17] = "it", sample [18] = "by", sample [18] = "the", sample [18] = "the"[18] = "said", sample[19] = "is", sample[20] = "an", sample[21] = "have", sample[22] = "be", sample[23] = "its", sample[21] = "its", sample[22] = "be", sample[23] = "its", sample[23] =[24]="Johnson", sample[25]= at", sample[26]= from", sample[27]= would", sample[28]= him", sample[29]= not", sample [30]="they",sample[31]="but",sample[32]="this",sample[33]="their",sample[34]="who",sample[35]="up",sample [36] = "which", sample [37] = "been", sample [38] = "grow", sample [39] = "has", sample [40] = "were", sample [41] = "more", sampl[42] = "one", sample [43] = "ln", sample [44] = "time", sample [45] = "could", sample [46] = "first", sample [47] = "He", sample [47] = "ln", sa[48] = "Jos", sample [49] = "years", sample [50] = "Buendía", sample [51] = "into", sample [52] = "book", sample [53] = "them", sample [54]="where",sample[55]="state",sample[56]="city",sample[57]="will",sample[58]="year",sample [59] = "Pittsburgh", sample [60] = "some", sample [61] = "all", sample [62] = "last", sample [63] = "l", sample [64] = "other", sample [65]="than", sample[66]="two", sample[67]="are", sample[68]="out", sample[69]="only", sample[70]="just", sample [71]="so", sample[72]="back", sample[73]="like", sample[74]="most", sample[75]="people", sample[76]="become", sample [77]="season", sample[78]="when", sample[79]="about", sample[80]="also", sample[81]="say", sample[82]="over", sample[80]="also", sample[81]="say", sample[82]="over", sample[80]="also", sample[81]="say", sample[81]="over", sample[80]="also", sample[81]="say", sample[81]="over", sample[81]", sample[81]="over", sample[81]", sample[81]="over", sample[81]", sample[81]="over", sample[81]", sample[81]="over", sample[81]", sample[81]="over", sample[81]", sample[81]", sample[81]="over", sample[81]", sample[8[83]="get",sample[84]="village",sample[85]="new",sample[86]="But",sample[87]="did",sample[88]="It",sample [89]="Oklahoma",sample[90]="Brazil",sample[91]="trade",sample[92]="put",sample[93]="no",sample [94] = "public", sample [95] = "Melquíades", sample [96] = "case", sample [97] = "her", sample [98] = "million", sample [99] = "climate", sample [100] = "set", sample [101] = "lost", sample [102] = "what", sample [103] = "without", sample [104] = "went", sample [105] = "if", sample [106] = "carbon", sample [107] = "during", sample [108] = "Judge", sample [107] = "during", sample [108] = "Judge", sample [107] = "during", sample [108] = "Judge", sample [108[109]="world",sample[110]="there",sample[111]="found",sample[112]="same",sample[113]="Point",sample [114]="built",sample[115]="she",sample[116]="made",sample[117]="down",sample[118]="while",sample

具体训练过程就是对样本 hash 然后计数,想法比较简单。

第二步,利用训练出来的高频词集进行解密,具体操作就是对密文进行 25 次 k 值尝试破译,每一次破译计算出高频词破解的次数,最后选取高频词破解次数最多的 k 作为密钥,因为凯撒密码较为简单,所以在密文足够长的情况下正确率可以达到百分之百。

CipherText.txt - Notepad

- u х

File Edit Format View Help

Naq va na vebavp naq harkcrpgrq ghea bs riragf, vg nccrnef gung qrfcvgr gnxvat gur H.F bhg bs gur vagreangvbany rssbeg gb pbzong pyvzngr punatr, Cerfvqrag Gehzc' f qrfgehpgvba bs genqr abezf znl unir pyrnerq gur jnl sbe n cbjreshy arj jrnoba va gur sytug nf pbhagevrf vapernfyatyl penpx gbja ba ebthr pyvzngr pbhagreonegf. Gur grfgehpgyba bs gur Nznmba abg bayl guerngraf gb grfgebl ovbgvirefvgl nag nssrpg gur yvirf bs vagytrabhf crbcyr ohg nyfb gb encygyl nppryrengr pyvzngr punatr. Gur Nznmba nofbeof pneoba gybkygr gung jbhyg bgurejyfr genc urng va gur ngzbfcurer. Oheavat gerrf eryrnfrf gur urng-genccvat tnf. Naq, juvyr sverf unir ohearq jvgu gur fnzr be terngre vagrafvgl va gur cnfg, fpvragvfgf jnea gung gur ertvba pbhyq or qnatrebhfyl pybfr gb n gvccvat cbvag gung jbhyq znxr vg vzcbffvoyr gb erfgber gur envasberfg nag fhfgnva gur ertvba' f novyvgl gb nofbeo pneoba gvbkvgr. Obyfnaneb unf cerivbhfyl dhrfgvbarg gur fpvrapr bs pyvzngr punatr, juvyr yrngref va gur RH unir ybat erwrpgrg uvf cbfvgvba. Nebhag gur jbeyg, cbyvplznxref unir fbhtug abg bayl gb pyrna hc gurve bja pneoba sbbgcevagf ohg nyfb gb chfu bgure pbhagevrf gb npg. Ohg gur engr bs qrfqehpqvba va gur Nznmba nppryrengrq gubfr bsgra-fhogyr qvcybzngvp rssbegf. Va fgngrzragf va gur qnlf yrnqvat hc gb gur T-7 fhzzvg, Senapr naq Verynaq obgu fhttrfgrq gung gurl zvtug jvguubyq fhccbeg sbe n ynaqznex genqr grny orgirra gur Rheberna Havba nag n unagshy bs Fbhgu Nzrevpna pbhagevrf vs Óbyfnaneb gvg abg gnxr gur znggre frevbhfyl. "Haqre gurfr pbaqvgvbaf, Senapr vf bccbfrq," Serapu Cerfvqrag Rzznahry Znpeba' f bssvpr fnvq va na Nht. 23 fgngrzrag, Gur grny, xabja nf gur Rhebcrna Havba–Zrepbfhe Serr Gengr Nterrzrag, jbhyg ryvzvangr gur znwbevgl bs gnevssf orgjrra gur RH nag gur Zrepbfhe pbzzba znexrg, juvpu vapyhqrf Oenmvy, Netragvan nag bguref. Bssvpvnyf naabhaprg n grny va Whar nsgre gjb grpngrf bs artbgyngybaf, ohg vg fgyyy erdhyerf nccebiny sebz pbafgyghrag pbhagevrf. Rhebcrna Pbhapvy Cerfvqrag Qbanyq Ghfx fnvq vg jnf "uneq gb vzntvar" gur qrny tbvat guebhtu vs Obyfbaneb qvq abg gnxr npgvba. Svaynaq, juvpu pheeragyl punvef gur Pbhapvy bs gur Rhebcrna Havba, fhttrfgrq n qvssrerag cngu: erfgevpgvat Oenmvyvna orrs vzcbegf. Oenmvy pheeragyl rkcbegf 120,000 gbaarf bs orrs naahnyyl gb gur RH, n syther Oenmyyyna cebqhpref ubcr qb tebi va gur pbzyat Irnef. Svaynag' f syanapr zyayfgre fnyg va n fgngrzrag

Figure 3 密文

PlainText.txt - Notepad

File Edit Format View Help

And in an ironic and unexpected turn of events, it appears that despite taking the U.S out of the international effort to combat climate change, President Trump's destruction of trade norms may have cleared the way for a powerful new weapon in the fight as countries increasingly crack down on roque climate counterparts. The destruction of the Amazon not only threatens to destroy biodiversity and affect the lives of indigenous people but also to rapidly accelerate climate change. The Amazon absorbs carbon dioxide that would otherwise trap heat in the atmosphere. Burning trees releases the heat-trapping gas. And, while fires have burned with the same or greater intensity in the past, scientists warn that the region could be dangerously close to a tipping point that would make it impossible to restore the rainforest and sustain the region's ability to absorb carbon dioxide. Bolsanaro has previously questioned the science of climate change, while leaders in the EU have long rejected his position. Around the world, policymakers have sought not only to clean up their own carbon footprints but also to push other countries to act. But the rate of destruction in the Amazon accelerated those often-subtle diplomatic efforts. In statements in the days leading up to the G-7 summit, France and Ireland both suggested that they might withhold support for a landmark trade deal between the European Union and a handful of South American countries if Bolsanaro did not take the matter seriously. "Under these conditions, France is opposed," French President Emmanuel Macron's office said in an Aug. 23 statement. The deal, known as the European Union-Mercosur Free Trade Agreement, would eliminate the majority of tariffs between the EU and the Mercosur common market, which includes Brazil, Argentina and others. Officials announced a deal in June after two decades of negotiations, but it still requires approval from constituent countries. European Council President Donald Tusk said it was "hard to imagine" the deal going through if Bolsonaro did not take action. Finland, which currently chairs the Council of the European Union, suggested a different path: restricting Brazilian beef imports. Brazil currently exports 120,000 tonnes of beef annually to the EU, a figure Brazilian producers hope to grow in the coming years. Finland's finance minister said in a statement late last week that he would raise the possibility of banning Brazilian beef at a meeting with his EU