1) Аффинный шифр. Найти открытый текст. Шифртекст:

KQEREJEBCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUP
KRIOFKPACUZQEPBKRXPEIIEABDKPBCPFCDCCAFIEABDKP
BCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFF
ERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPERK
IVKSCPICBRKIJPKABI

Встречаемость символов			
В английском языке		**В шифртексте**	
E	12,150	C	16,160
T	8,999	B	10,600
A	8,399	P	10,100
O	7,493	K	10,100
...	...	...	...

E(x) = (a*x+b) mod 26
'C' = ('E'a+b) mod 26 = 2 = (4a+b) mod 26
'B' = ('T'a+b) mod 26 = 1 = (19a+b) mod 26
a = 19, b = 4
D(x) = a-1(x-b) mod 26 = 11(x-4) mod 26

OCANADATIRRIDINOSAIIUXTONFRONTISTCIINTDIFLIUR
ONSGLORIIUXCARTONBRASSAITTORTIRLITIIILSAITTOR
TIRLACROIXTONHISTOIRIISTUNIITOTIIDISTLUSBRILL
ANTSIXTLOITSITTAVALIURDIFOITRIMTIITROTIGIRANO
SFOYIRSITNOSDROITS

O CANADA TERRE DE NOS AIEUX TON FRONT EST CEINT DE FLEURONS
GLORIEUX CAR TON BRAS SAIT PORTER L EPEE IL SAIT PORTER LA CROIX
TON HISTOIRE EST UNE EPOPEE DES PLUS BRILLANTS EXPLOITS ET TA
VALEUR DE FOI TREMPEE PROTEGERA NOS FOYERS ET NOS DROITS

2) Дешифровать простой подстановочный шифр. Алфавит открытого и шифрованного текстов английский. Шифртекст:

EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCK
QPKUGKMGOLICGINCGACKSNISACYKZSCKXECJCKSHYSXCG
OIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZU
GFZCCNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNS
ACIGOIYCKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNC
IACZEJNCSHFZEJZEGMXCYHCJUMGKUCY

Кол-во вхождений = [C:37, G:24, S:20, K:18, I:15, Y:15, U:14, Z:13, N:13, E:12, O:10, F:9, D:8, J:7, L:7, X:7, P:6, H:5, W:5, A:5, M:5, Q:1]

Биграммы = [CG:7, ZC:7, GO:5, CN:5, AC:5, CK:5, NC:5, YS:5, FZ:4, CY:4, SF:4, GK:4, GY:4, OI:3, KG:3, SI:3, IC:3, ZE:3, GL:3, CC:3, US:3, SH:3, KU:3, XE:3, XC:3, CJ:3, CI:3, KS:3, MG:3, JC:2, KX:2, IG:2, DG:2, GI:2, NS:2, OL:2, LK:2, SA:2, UC:2, UG:2, DP:2, YK:2, CF:2, YY:2, CS:2, EJ:2, UM:2, IU:2, UZ:2, EU:2, JN:2, WY:2, KZ:2, DS:2, PK:2, ND:2, JU:2, EO:2, GA:2, PW:1, IW:1, OJ:1, WG:1, SZ:1, OC:1, UP:1, LW:1, CO:1, QP:1, ZS:1, EC:1, KQ:1, YC:1, GM:1, FH:1, SC:1, OS:1, ED:1, FU:1, CZ:1, FE:1, FG:1, SP:1, EZ:1, PJ:1, NI:1, IL:1, ML:1, WE:1, NF:1, UD:1, GD:1, HF:1, KK:1, DC:1, NX:1, SO:1, ZG:1, YG:1, WZ:1, LO:1, CU:1, DN:1, IS:1, XY:1, EM:1, MX:1, HI:1, SX:1, PU:1, HY:1, YI:1, IY:1, YE:1, GN:1, NK:1, JZ:1, KN:1, PX:1, KM:1, LD:1, IN:1, GF:1, EK:1, EG:1, ID:1, UE:1, SU:1, IP:1, HN:1, KD:1, YH:1, ZU:1, LI:1, OX:1, HC:1, LE:1, OW:1, SW:1, SN:1, FC:1, IA:1]

Триграммы = [YSF:3, GOI:3, ZCC:3, CCN:3, FZC:3, GYY:2, YYS:2, CND:2, CGI:2, JNC:2, ICG:2, CKX:2, ZCN:2, GOL:2, KGO:2, JCK:2, KSH:2, NCG:2, GAC:2, ZEJ:2, CFZ:2, SAC:2, CJU:2, CYK:2, CKS:2, NDG:2, UZC:2, DGY:2, KXE:1, EJN:1, YSI:1, GKK:1, SHY:1, NSA:1, OIY:1, CIU:1, CNC:1, XCY:1, CUS:1, YIC:1, CSO:1, PJC:1, XEZ:1, ZCF:1, KUC:1, SIL:1, EOJ:1, GLK:1, IYC:1, KDP:1, SWY:1, LWG:1, DSI:1, JUM:1, SIG:1, USZ:1, MGK:1, EMG:1, COX:1, GIW:1, KSN:1, KZS:1, MGO:1, FUS:1, ACG:1, NFG:1, IPJ:1, PWZ:1, GFZ:1, ICO:1, IWY:1, WEU:1, OLI:1, WYG:1, OLD:1, LKN:1, HNS:1, SHI:1, CYH:1, WYS:1, YCK:1, ZUG:1, QPK:1, CGA:1, USI:1, WZU:1, OJN:1, LED:1, FEU:1, GIN:1, HIC:1, SXC:1, OCF:1, CNX:1, GNF:1, GLE:1, XYS:1, UGK:1, PXE:1, HFZ:1, SIP:1, KGK:1, NIS:1, YSX:1, NKS:1, EGM:1, GDN:1, GYI:1, KZC:1, DCG:1, SNI:1, IUZ:1, KUZ:1, ZCS:1, NCS:1, ISA:1, NXE:1, FGL:1, GMX:1, NSF:1, HYS:1, SZC:1, GKM:1, LKG:1, XEO:1, GYE:1, CIG:1, EJZ:1, CGD:1, CGO:1, KMG:1, EKU:1, FZE:1, KUG:1, IGO:1, UMG:1, PKZ:1, JUC:1, SCK:1, ZGA:1, OXY:1, MLW:1, DPK:1, SFE:1, SFC:1, FCY:1, CGN:1, KNS:1, ACZ:1, KQP:1, ILK:1, IUS:1, EUE:1, MXC:1, FHN:1, KKG:1, CNK:1, SHF:1, DPU:1, ECJ:1, XCJ:1, UEK:1, YKZ:1, SFU:1, UML:1, YEO:1, UCI:1, LIC:1, CJC:1, SPW:1, CGY:1, IAC:1, YHC:1, DSP:1, XCG:1, XEC:1, OID:1, CSH:1, JZE:1, OSU:1, DNC:1, CIA:1, SFH:1, EOW:1, GKU:1, USW:1, NCI:1, PUM:1, SUD:1, ACY:1, IGL:1, UCY:1, UPX:1, LOS:1, PKU:1, ACI:1, EUP:1, LDS:1, YGK:1, GLO:1, EDS:1, IDP:1, INC:1, CZE:1, WGY:1, ZSC:1, MGL:1, KXC:1, EZG:1, OIU:1, UGF:1, HCJ:1, YKD:1, CKQ:1, NCU:1, SOC:1, GKG:1, OWE:1, UDC:1, ACK:1, ZEG:1]

Кол-во символов = 256

Распределение в английском языке:
E ~ 0.12
T, A, O, I, N, S, H, R ~ 0.06-0.09
D, L ~ 0.04
C, U, M, W, F, G, Y, P, B ~ 0.015-0.028
V, K, J, X, Q, Z < 0.01

30 самых встречаемых биграмм (в порядке уменьшения популярности): TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF

12 самых встречаемых триграмм (в порядке уменьшения популярности): THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

- Самая частая буква в шифртексте C -> E.
- Биграмма ZC встречается часто, а CZ вообще не встречается. Если учитывать, что C=E, то мы ищем биграмму, которая заканчивается на E, а её "перевертыш" не является популярным. Такая биграмма единственная – HE. Отсюда, Z -> H.

  ```
  ________E___E__________E__________E_______E_
  ___________E___E__E______E__H_E___E_E______E_
  _____HE_____E_____________________________H_
  __HEE_________HE______E__________H__E________
  _E_____E__E__E__HE_HEE____________HE__E_HEE_E
  __EH___E___H__H____E__E______E_
  ```

- Триграмма THE может быть на 4 позициях: KZC, SZC, UZC, UZC. Так как последняя триграмма встречается чаще, то предположим, что U -> T.
- Биграмма US состоит из T и очень популярной буквы в шифртексте S. В списке биграмм первой встречается биграмма TO. Положим S -> O.
  - Тригграмма ZCC всегда идем вместе с FZCCN = _HEE_, частоты F(0.03) и N(0.05) позволяют предположить, что это слово WHEEL.

    ```
    _____OT_E__LETO__OW_LOWE____T______E___O___E_
    ___T_______E__LE__E_OL_O_E__HOE___E_E_O__O_E_
    _____HEL_O__E_____________O______TO_____O__HT
    _WHEEL____OWTOHEL____LE______T___H__E_LW___LO
    _E_____E__E_TE_THEWHEEL____OW_T__THEO_EWHEELE
    __EH__LEO_WH__H____E__E_T___TE_
    ```

  - THEO_EWHEEL… -> THE ONE WHEEL…: O -> N
  - LOWE_ -> LOWER: Y -> R

    ```
    ____NOT_E__LETO_ROW_LOWER___T____R_EN_RO___E_
    ___T____N__E__LE__E_OL_O_ER_HOE___E_E_O_RO_E_
    N____HEL_O__E___R______N__O____N_TO_____O__HT
    _WHEEL__RROWTOHEL__N_LE_R_N__T___H__E_LW___LO
    _E__N_RE__E_TE_THEWHEEL__RROW_T__THEONEWHEELE
    __EH__LEO_WH__H____ER_E_T___TER
    ```

  - NOT_E -> NOT BE: D -> B

    ```
    ____NOTBE_BLETO_ROW_LOWER_B_T____R_EN_RO___E_
    ___T____N__E__LE__E_OL_O_ER_HOE___E_E_O_RO_E_
    N_B__HEL_O__E___R______N_BO____N_TO____BO__HT
    _WHEELB_RROWTOHEL__N_LE_R_N__T___H__E_LW___LO
    _E__N_RE__E_TE_THEWHEELB_RROW_T__THEONEWHEELE
    __EH__LEO_WH__H____ER_E_T___TER
    ```

- NOTBE_BLETO_ROW -> NOT BE ABLE TO GROW: G -> A, W -> G
  __A_NOTBEABLETOGROW_LOWER_B_T__GAR_EN_RO___E_
  ___TA__AN__EA_LEA_E_OL_O_ER_HOE___E_E_O_RO_EA
  N_B__HEL_O__EA_GRA__A_AN_BO___AN_TO_A__BO_GHT
  AWHEELBARROWTOHEL__N_LEAR_NG_T___HA_EALWA__LO
  _E_AN_RE__E_TE_THEWHEELBARROW_T__THEONEWHEELE
  __EH__LEO_WH__H_A__ER_E_T_A_TER

  Аналогично восстанавливаются остальные буквы.

  IMAYNOTBEABLETOGROWFLOWERSBUTMYGARDENPRODUCES
  JUSTASMANYDEADLEAVESOLDOVERSHOESPIECESOFROPEA
  NDBUSHELSOFDEADGRASSASANYBODYSANDTODAYIBOUGHT
  AWHEELBARROWTOHELPINCLEARINGITUPIHAVEALWAYSLO
  VEDANDRESPECTEDTHEWHEELBARROWITISTHEONEWHEELE
  DVEHICLEOFWHICHIAMPERFECTMASTER

  I MAY NOT BE ABLE TO GROW FLOWERS BUT MY GARDEN PRODUCES JUST AS
  MANY DEAD LEAVES OLD OVERSHOES PIECES OF ROPE AND BUSHELS OF DEAD
  GRASS AS ANYBODYS AND TODAY I BOUGHT A WHEELBARROW TO HELP IN
  CLEARING IT UP I HAVE ALWAYS LOVED AND RESPECTED THE WHEELBARROW IT
  IS THE ONE WHEELED VEHICLE OF WHICH I AM PERFECT MASTER

3) Дешифровать шифр Виженера. Алфавит открытого и шифрованного текстов английский. Шифртекст:

  KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD
  DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC
  QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL
  SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV
  GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFS
  PEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI
  FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY
  CWHJVLNHIQIBTKHJVNPIST

  Определим длину ключа по индексу совпадения:
  m = 1: I=(0.041)
  m = 2: I=(0.038, 0.047)
  m = 3: I=(0.056, 0.048, 0.048)
  m = 4: I=(0.037, 0.042, 0.037, 0.050)
  m = 5: I=(0.043, 0.043, 0.031, 0.035, 0.043)
  m = 6: I=(0.063, 0.084, 0.049, 0.065, 0.042, 0.071)
  m = 7: I=(0.031, 0.044, 0.043, 0.038, 0.044, 0.044, 0.041)

  Длина ключа 6. Определим ключ для первого блока.
  k = 0: 0.315
  k = 1: 0.352
  k = 2: 0.641
  k = 3: 0.394

k = 4: 0.340
k = 5: 0.411
k = 6: 0.369
k = 7: 0.309
…
k = 25: 0.338

Аналогично находим ключи для остальных блоков, итоговый ключ:
[2, 17, 24, 15, 19, 14] = CRYPTO

ILEARNEDHOWTOCALCULATETHEAMOUNTOFPAPERNEEDEDF
ORAROOMWHENIWASATSCHOOLYOUMULTIPLYTHESQUAREFO
OTAGEOFTHEWALLSBYTHECUBICCONTENTSOFTHEFLOORAN
DCEILINGCOMBINEDANDDOUBLEITYOUTHENALLOWHALFTH
ETOTALFOROPENINGSSUCHASWINDOWSANDDOORSTHENYOU
ALLOWTHEOTHERHALFFORMATCHINGTHEPATTERNTHENYOU
DOUBLETHEWHOLETHINGAGAINTOGIVEAMARGINOFERRORA
NDTHENYOUORDERTHEPAPER

I LEARNED HOW TO CALCULATE THE AMOUNT OF PAPER NEEDED FOR A ROOM
WHEN I WAS AT SCHOOL YOU MULTIPLY THE SQUARE FOOTAGE OF THE WALLS
BY THE CUBIC CONTENTS OF THE FLOOR AND CEILING COMBINED AND DOUBLE
IT YOU THEN ALLOW HALF THE TOTAL FOR OPENINGS SUCH AS WINDOWS AND
DOORS THEN YOU ALLOW THE OTHER HALF FORMAT CHING THE PATTERN THEN
YOU DOUBLE THE WHOLE THING AGAIN TO GIVE A MARGIN OF ERROR AND THEN
YOU ORDER THE PAPER

4) Дешифровать неизвестный тип шифра. Алфавит открытого и шифрованного текстов английский Шифртекст:

BNVSNSIHQCEELSSKKYERIFJKXUMBGYKAMQLJTYAVFBKVT
DVBPVVRJYYLAOKYMPQSCGDLFSRLLPROYGESEBUUALRWXM
MASAZLGLEDFJBZAVVPXWICGJXASCBYEHOSNMULKCEAHTQ
OKMFLEBKFXLRRFDTZXCIWBJSICBGAWDVYDHAVFJXZIBKC
GJIWEAHTTOEWTUHKRQVVRGZBXYIREMMASCSPBNLHJMBLR
FFJELHWEYLWISTFVVYFJCMHYUYRUFSFMGESIGRLWALSWM
NUHSIMYYITCCQPZSICEHBCCMZFEGVJYOCDEMMPGHVAAUM
ELCMOEHVLTIPSUYILVGFLMVWDVYDBTHFRAYISYSGKVSUU
HYHGGCKTMBLRX

I = 0.0413, значит это не простой подстановочный шифр.
Попробуем найти найти длину ключа, если это шифр Виженера.
…
m = 6: I=(0.051, 0.061, 0.054, 0.070, 0.055, 0.069)
…

Для каждого блока находим ключ:
k1 = 19('T'): I=0.600
K2 = 7('H'): I=0.672

k3 = 4('E'): I=0.607
K4 = 14('O'): I=0.684
k5 = 17('R'): I=0.628
k6 = 24('Y'): I=0.644

IGREWUPAMONGSLOWTALKERSMENINPARTICULARWHODROP
PEDWORDSAFEWATATIMELIKEBEANSINAHILLANDWHENIGO
TTOMINNEAPOLISWHEREPEOPLETOOKALAKEWOBEGONCOMM
ATOMEANTHEENDOFASTORYICOULDNTSPEAKAWHOLESENTE
NCEINCOMPANYANDWASCONSIDEREDNOTTOOBRIGHTSOIEN
ROLLEDINASPEECHCOURSETAUGHTBYORVILLESANDTHEFO
UNDEROFREFLEXIVERELAXOLOGYASELFHYPNOTICTECHNI
QUETHATENABLEDAPERSONTOSPEAKUPTOTHREEHUNDREDW
ORDSPERMINUTE

I GREW UP AMONG SLOW TALKERS MEN IN PARTICULAR WHO DROPPED WORDS A FEW AT A TIME LIKE BEANS IN A HILL AND WHEN I GOT TO MINNEAPOLIS WHERE PEOPLE TOOK A LAKE WOBEGON COMMA TO MEAN THE END OF A STORY I COULDNT SPEAK A WHOLE SENTENCE IN COMPANY AND WAS CONSIDERED NOT TOO BRIGHT SO I ENROLLED IN A SPEECH COURSE TAUGHT BY ORVILLE SAND THE FOUNDER OF REFLEXIVE RELAXOLOGY A SELF-HYPNOTIC TECHNIQUE THAT ENABLED A PERSON TO SPEAK UP TO THREE HUNDRED WORDS PER MINUTE

1.6.9) Виженер, ключ m=3.

CTMYRDOIBSRESRRRIJYREBYLDIYMLCCYQXSRRMLQFSDXFOWFKTCYJRRIQZSMX

Аналогичным способом как в 3) и 4) находим ключ:
k1 = 10('K'): I=0.682
k2 = 4('E'): I=0.658
k3 = 24('Y'): I=0.656

SPOONFEEDINGINTHELONGRUNTEACHESUSNOTHINGBUTTHESHAPEOFTHESPOON

SPOONFEEDING IN THE LONG RUN TEACHES US NOT HING BUT THE SHAPE OF THE SPOON