# Общие задачи

1) Найти открытый текст. Шифртекст:

KQEREJEBCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUP

KRIOFKPACUZQEPBKRXPEIIEABDKPBCPFCDCCAFIEABDKP

BCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFF

ERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPERK

IVKSCPICBRKIJPKABI

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

Решить систему уравнений афинного шифра:

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

a = 19, b = 14

2) Шифр простой замены

EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCK

QPKUGKMGOLICGINCGACKSNISACYKZSCKXECJCKSHYSXCG

OIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZU

GFZCCNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNS

ACIGOIYCKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNC

IACZEJNCSHFZEJZEGMXCYHCJUMGKUCY

C -> E

ZC -> HE

UZC -> THE (FZC/UZC)

NC -> LE

F -> W -> (WHEEL)

S -> O -> (LOW)

O -> N

Y -> R (LOWER)

D -> B

G -> A (/U) (WHEELBARROW)

W -> G (GARDEN, GROW)

H -> F (FLOWERS)

I -> D (WHEELED, DEAD)

X -> P, L -> Y, M -> M (ROPE, RESPECTED, MASTER, MAY)

A -> V (LOVED, OVER)

…

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) KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD

DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC

QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL

SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV

GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFS

PEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI

FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY

CWHJVLNHIQIBTKHJVNPIST

Находим длину ключа максимизацией I: 6

Находим наиболее подходящий ключ, такой, что среднее I близко к I открытых текстов языка (0.0644): CRYPTO

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 YOUALLOW THE OTHER HALF FOR MATCHING THE PATTERN THEN YOU DOUBLE THE WHOLE THING AGAIN TO GIVE A MARGIN OF ERROR AND THEN YOU ORDER THE PAPER.

4)

Неизвестный шифртекст:

BNVSNSIHQCEELSSKKYERIFJKXUMBGYKAMQLJTYAVFBKVT

DVBPWRJYYLAOKYMPQSCGDLFSRLLPROYGESEBUUALRWXM

MASAZLGLEDFJBZAVVPXWICGJXASCBYEHOSNMULKCEAHTQ

OKMFLEBKFXLRRFDTZXCIWBJSICBGAWDVYDHAVFJXZIBKC

GJIWEAHTTOEWTUHKRQVVRGZBXYIREMMASCSPBNLHJMBLR

FFJELHWEYLWISTFVVYFJCMHYUYRUFSFMGESIGRLWALSWM

NUHSIMYYITCCQPZSICEHBCCMZFEGVJYOCDEMMPGHVAAUM

ELCMOEHVLTIPSUYILVGFLMVWDVYDBTHFRAYISYSGKVSUU

HYHGGCKTMBLRX

Найдём индекс совпадения текста: 0.040575818539026365 (полиалфавитный подстановочный шифр)

Предположим, что это шифр Виженера. Найдём длину и шифр (аналогично 3): 6, THEORY

I GREW UP AMONG SLOW TALKERS, MEN IN PARTICULAR, WHO DROPPED WORDS AFEW AT A TIME LIKE BEANS IN A HILL, AND WHEN I GOT TO MINNEAPOLISWHEREPEOPLE TOOK A LAKE WOBEGON COMMA TO MEAN THE END OF A STORY, I COULDN’TSPEAK A WHOLE SENTENCE IN COMPANY AND WAS CONSIDERED NOT TOO BRIGHT. SO IENROLLED IN A SPEECH COURSE TAUGHT BY ORVILLE SAND, THE FOUNDER OF REFLEXIVERELAXOLOGY, A SELF-HYPNOTIC TECHNIQUE THAT ENABLED A PERSON TO SPEAK UP TOTHREE HUNDRED WORDS PER MINUTE.

# Индивидуальные задачи

**1.6.12** Шифртекст:

TNOSSKAIMAGAEITMHETHTSRHXXIHEUXDX

NUEIDSATDTDDSARAHHENTTTDSOUIOEART

FHDAOMWYWFERTNEONFDYAHSEIMEDGRWTA

TISURUARTHJ

|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **0** | T | N | O | S | S | K | A | I | M | A | G |
| **1** | A | E | I | T | M | H | E | T | H | T | S |
| **2** | R | H | X | X | I | H | E | U | X | D | X |
| **3** | N | U | E | I | D | S | A | T | D | T | D |
| **4** | D | S | A | R | A | H | H | E | N | T | T |
| **5** | T | D | S | O | U | I | O | E | A | R | T |
| **6** | F | H | D | A | O | M | W | Y | W | F | E |
| **7** | R | T | N | E | O | N | F | D | Y | A | H |
| **8** | S | E | I | M | E | D | G | R | W | T | A |
| **9** | T | I | S | U | R | U | A | R | T | H | J |

Найдём методом Hill Climbing перестановку столбцов. В качестве функции оценки возьмём разницу частот квадграмм. Найдём имя ARTHUR, поймём, что X – это паддинг для сообщения. Повторим до тех пор, пока не получится правильная перестановка столбцов (все X должны быть в конце в строке 2). Найдём перебором или методом Hill Climbing перестановку строк (строка 2 должна быть в конце).

Столбцы=[6, 4, 0, 9, 5, 7, 1, 10, 3, 2, 8]

Строки=(9, 4, 8, 0, 1, 3, 7, 5, 6, 2)

Открытый текст:

ARTHURIJUSTHADTHESTRANGESTDREAMIWASTAKINGSOMEMATHTESTIHADNTSTUDIEDFORANDTHENYOUTRIEDTOSAWOFFMYHEADWEIRDHUHXXXX

ARTHUR, I JUST HAD THE STRANGEST DREAM. I WAS TAKING SOME MATH TEST I HADN’T STUDIED FOR AND THEN YOU TRIED TO SAW OFF MY HEAD! WEIRD, HUH…

(The Tick, Season 1: The Tick vs. the Uncommon Cold)

**2.6.5** How many pairs of cycles are required in order to uniquely determine

the Enigma rotor settings?

NumPairs >= log(K)/log(26), K – Enigma Key space ~ 2^30 (26^2\*26^3\*5!/2!) >= 7

# Задачи из зачёта

1. Задача 83:

ШИФР ПЕРЕСТАНОВКИ СТОЛБЦОВ:

ДОЛГОЕ ВРЕМЯ ЗАНЯТИЕ КРИПТОГРАФИЕЙ БЫЛО УДЕЛОМ ОДИНОЧЕК ТЧК СРЕДИ НИХ БЫЛИ ОДАРЕННЫЕ УЧЕНЫЕ ЗПТ ДИПЛОМАТЫ ЗПТ СВЯЩЕННОСЛУЖИТЕЛИ ТЧК ------

(Hill Climbing, триграммы и квадрграммы в качестве оценки расшифрованного текста)

1. Задача 92:

БЕГАЮТ ПО ЛЕСУ СТАИ ЗВЕРЕЙ - НЕ ЗА ДОБЫЧЕЙ , НЕ НА ВОДОПОЙ ДЕННО И НОЩНО ОНИ ЕГЕРЕЙ ИЩУТ ВЕСЕЛОЙ ТОЛПОЙ.

(перебор всех слов из двух букв, потом нашлось НОЩНО, ДЕННО, а дальше уже стало совсем просто)

1. Задача 104:

ПОЗПРЯВЛЯЮСНОВЫМГОГОМ

ПОЗДРАВЛЯЮ С НОВЫМ ГОДОМ (перебор всех дат с метрикой логарифма частот квадграмм. 31.12.07)

1. Problem 10:

Нет. Предположим атаку выбранного шифртекста (для взламываемых ключей известна пара открытый текс-шифртекст):

Ева может параллельно создать пары для каждого возможного ключа: открытый текст -> шифртекст возможным ключом. На это ей потребуется 2^64 итераций.

Во время генерации пар Ева может построить две таблицы соответствия пар: для первой таблицы индексом будет шифртекст, для второй таблицы индексом будет открытый текст. На это ей потребуется: 2\*log(2^64)\*2^64.

Временная сложность выполнения всех итераций: 2^64+2\*log(2^64)\*2^64=2^64\*(1+128) ~ 2^72(так как сортировку можно выполнять во время генерации).

Взлом происходит по нахождению совпадения известного открытого и шифртекстов в двух таблицах.

1. Задача 118

MAX = 12 => Есть всего 2 сцепки кнопок

7\_7\_7|2|5\_5|8|9\_9\_9\_9\_9

Позиций вставки сцепок: 7

C(7, 2) = 21

1. Задача 173

Полёт состоится завтра в семь часов

(1,14,2,5,10,11,13)^6(3,9,12,6,4,15,8,7)^7

(1,14,2,5,10,11,13)(1,14,2,5,10,11,13) = (1,2,10,13,14,5,11)

(1,2,10,13,14,5,11)(1,2,10,13,14,5,11) = (1,10,14,11,2,13,5)

(1,14,2,5,10,11,3)^6 = (1,2,10,13,14,5,11)(1,10,14,11,2,13,5) = (1,13,11,10,5,2,14)

(3,9,12,6,4,15,8,7)^7 = (3,7,8,15,4,6,12,9)

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

14 5 9 15 10 4 3 7 12 11 13 6 1 2 8

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

п о л е т с о с т о и т с я з

а в т р а в с е м ь ч а с о в

1. Task 8. The following ciphertext is from a columnar transposition cipher:

TSEHVAIESSRYIYQ

THISISVERYEASYQ

(Hill Climbing, сначала триграммы в качестве оценке дешифрования и нахождение THIS, VERY и EAS, затем перебор квадграмм и нахождение EASY.)

1. Block Cipher Mode 1:



Правило дешифрования:

1. Parallel decryption
2. Semi parallel encryption (compute E(Pi, K) separately) and then XOR them in chain.
3. Looks very similar to CFB
4. Self-synchronizing
5. **No advantages over CBC in terms of security**
6. Task 10. Consider two ciphers, Cipher A and Cipher B, and suppose that Cipher A has a 64-bit key, while Cipher B has a 128-bit key. Alice prefers Cipher A, while Bob wants the additional security provided by a 128-bit key, so he insists on Cipher B. As a compromise, Alice proposes that they use Cipher A, but they encrypt each message twice, using two independent 64-bit keys. Assuming that no shortcut attack is available for either cipher, is Alice's approach sound?

It depends on the use case. If they will be communicating lots of data over the secured channel using the same set of keys with **reduced block size of 64 bits**, Cipher A will be exposed to Sweet32 attack since the block size of the message is reduced and birthday paradox would happen sooner.