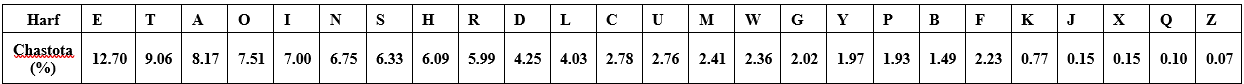
1. На какие основные направления делится криптология?
2. В чем различие между криптографией и криптоанализом?
3. Каковы основные задачи криптоанализа?
4. Какие существуют основные виды атак на криптосистемы?
5. Почему криптоанализ важен для современной криптографии?
6. Какие основные принципы лежат в основе криптоанализа?
7. Как проводится криптоанализ классических шифров?
8. Как частотный анализ используется для взлома шифров?
9. Чем полезен метод грубой силы в криптоанализе?
10. Что такое атакующий алфавит и как он используется?
11. Какие ограничения у криптоанализа классических шифров?
12. Какие простые методы криптоанализа применяются к классическим шифрам?
13. Какие методы используются для криптоанализа шифра Цезаря?
14. По каким критериям криптографические алгоритмы считаются устойчивыми?
15. Что понимается под криптографической стойкостью?
16. Как связаны теория сложности вычислений и криптоанализ?
17. В чем сложность алгоритмов современных шифров?
18. Что такое универсальные методы криптоанализа?
19. Как работает метод Полларда в криптоанализе?
20. В чем заключается метод «Встреча посередине»?
21. Что такое коллизии хэш-функций и как их находят?
22. Какие методы криптоанализа используются для блочных шифров?
23. Как применяется линейный криптоанализ для блочных шифров?
24. В чем суть дифференциального криптоанализа блочных шифров?
25. Что такое линейно-дифференциальный криптоанализ?
26. Как применяется алгебраический метод криптоанализа для блочных шифров?
27. В чем особенности интегрального криптоанализа блочных шифров?
28. Что такое слайдовая атака на блочные шифры?
29. Как работает метод криптоанализа с использованием аппаратной генерации ошибок?
30. Какие методы криптоанализа используются для асимметричных криптосистем?
31. Как проводится криптоанализ систем на основе задачи факторизации?
32. В чем сложность криптоанализа дискретного логарифмирования?
33. Как используется парадокс дней рождения в криптоанализе?
34. Какие преимущества имеют квантовые компьютеры для взлома RSA?
35. Какие методы используются для анализа эллиптических кривых?
36. В чем состоит сложность атак на асимметричные системы?
37. Какие атаки проводятся через электромагнитное излучение?
38. В чем преимущества симметричных шифров перед асимметричными?
39. Какие уязвимости были найдены в алгоритмах MD4 и MD5?
40. Как оценивается случайность генераторов случайных чисел?
41. Как проводится анализ генераторов случайных и псевдослучайных чисел?
42. Как атаки через временные задержки влияют на криптосистемы?
43. Какие статистические методы используются для оценки случайности данных?
44. В чем суть атак через акустический анализ?
45. Что представляет собой набор тестов NIST для проверки случайности?
46. В чем особенности набора тестов DIEHARD?
47. В чем особенности генераторов псевдослучайных чисел?
48. Какие атаки возможны на слабые генераторы случайных чисел?
49. Какие стандарты применяются для оценки случайности?
50. Как линейный криптоанализ применяется к потоковым шифрам?
51. В чем отличие криптографических генераторов от обычных?
52. Как дифференциальный криптоанализ используется в потоковых шифрах?
53. Что такое алгебраические методы криптоанализа потоковых шифров?
54. Какие существуют дополнительные каналы, использующиеся в криптоанализе?
55. В чем особенности криптоанализа шифра Атбаша?
56. Как используется частотный анализ для вскрытия шифра Полибия?
57. Какие методы применяются для криптоанализа шифра Виджинера?
58. В чем основные отличия криптоанализа одноключевых и многоключевых алгоритмов шифрования?
59. Какие подходы использовались для выполнения криптоанализа машины «Энигма»?
60. Как квантовая криптография защищает данные?
61. Какие примеры успешного применения AI в криптографии известны?
62. Как блокчейн используется для повышения безопасности хэш-функций?
63. Что такое постквантовые алгоритмы?
64. Как блокчейн может повысить устойчивость криптосистем?
65. Найти обратное число по заданному модулю. **;**
66. Расшифруйте зашифрованный текст методом магического квадрата 5×5:

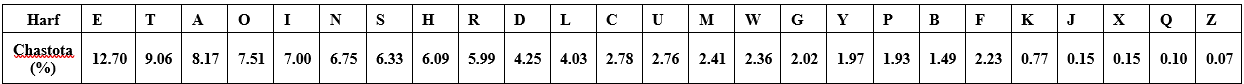
**“DEMUHPCQTOISERYRMOCGEFRAA”**

1. Расшифруйте зашифрованный текст, используя алгоритм шифрования RSA, описанный ниже. **C= 388236, N= 481391, e= 77;**
2. Расшифруйте заданный зашифрованный текст с помощью частотного криптоанализа? Частотные характеристики английского языка:



**“JXU MYDT YI SEBT, QDT JXU DYWXJ YI TQHA. OEKH EHTUHI QHU JE FHESUUT MYJX JXU CYIIYED MYJXEKJ QDO YDJUHHKFJYEDI. QDO TUBQO MYBB SQKIU JXU UDUCO JE HUQTO JXUYH VEHSUI. OEKH MEHA YI EV JXU KJCEIJ YCFEHJQDSU, QDT OEK CKIJ QSJ MYJX UNJHUCU SQKJYED.”**

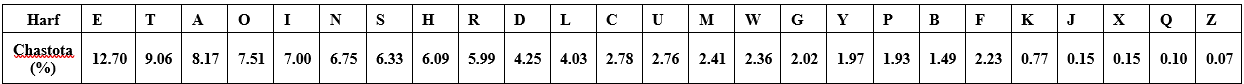
1. Найти обратное число по заданному модулю.**;**
2. Расшифруйте зашифрованный текст методом магического квадрата 5×5: **“YOWTCWOENRCMEINTETOLHPREO”**
3. Расшифруйте зашифрованный текст, используя алгоритм шифрования RSA, описанный ниже. **C= 31044, N= 37403, e= 53;**
4. Расшифруйте заданный зашифрованный текст с помощью частотного криптоанализа? Частотные характеристики английского языка:



**“PZOQY VCFGS WG ACJWBU WBHC HVS JOZZSM. KVSB HVS GCZRWSFG OFS OZZ WB DCGWHWCB, KS KWZZ GHOFH HVS OHHOQY. MCIF XCP WG HC ZSOR HVS QVOFUS OBR SBGIFS HVOH BC HFSBQVSG OFS PFCYSB. HVS SBSAM WG KOWHWBU TCF OB CDDCFHIBWHM HC QCIBHSFOHHOQY, GC PS DFSDOFSR.”**

1. Найти обратное число по заданному модулю. **;**
2. Расшифруйте зашифрованный текст методом магического квадрата 5×5: **“OCSASSEPDTRTRGISOAECWROES”**
3. Расшифруйте зашифрованный текст, используя алгоритм шифрования RSA, описанный ниже. **C= 31044, N= 37403, e= 53;**
4. Расшифруйте заданный зашифрованный текст с помощью частотного криптоанализа?

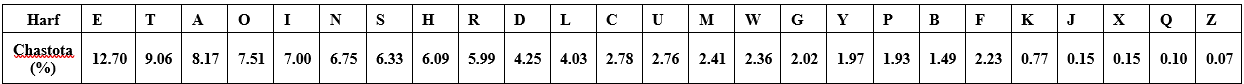
Частотные характеристики английского языка:



**“LZW HDSF AK KAEHDW. QGM OADD WFLWJ LZW TMADVAFY LZJGMYZ LZW ESXC OVG. QGMJ LSKC AK LG VAKSTDW LZW KWUMJALQ KQKLWE SFV ESCW KMJW SDD LZW WPALK SJW DGUCWV. SFQ MFWPHWULWV WNWFLK EMKL TW ZSFVDWV OALZGML VWDSQ. QGMJ KHWWV SFV USDUMDSLAGF OADD VWLWJEAFW LZW KMUUWKK GX LZW GHWJSLAGF.”**

1. Найти обратное число по заданному модулю. **;**
2. Расшифруйте зашифрованный текст методом магического квадрата 5×5: **“RYTSNBMSECSESTDGIPEIEYMHA”**
3. Расшифруйте зашифрованный текст, используя алгоритм шифрования RSA, описанный ниже. **C= 103982, N= 381847, e= 53;**
4. Расшифруйте заданный зашифрованный текст с помощью частотного криптоанализа?

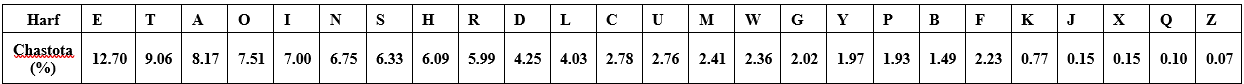
Частотные характеристики английского языка:



**“NDJ BJHI UXCS PLPN ID TCITG IWT QJXASXCV LXIWDJI QTXCV HTTC. IWTGT PGT BPCN VJPGSH XCHXST PCS PCN BXHIPZT RDJAS ATPS ID UPXAJGT. NDJ BJHI LDGZ LXIW NDJG ITPB ID HJRRTHHUJAAN RDBEATIT IWT BXHHXDC LXIWDJI PCN XCRXSTCIH. VTI XC PCS VTI DJI PH FJXRZAN PH NDJ RPC.”**

1. Найти обратное число по заданному модулю. **;**
2. Расшифруйте зашифрованный текст методом магического квадрата 5×5: **“CITCEDAIENMGRPEQAYTEURSHS”**
3. Расшифруйте зашифрованный текст, используя алгоритм шифрования RSA, описанный ниже. **C= 116533, N= 161803, e= 43;**
4. Расшифруйте заданный зашифрованный текст с помощью частотного криптоанализа?

Частотные характеристики английского языка:



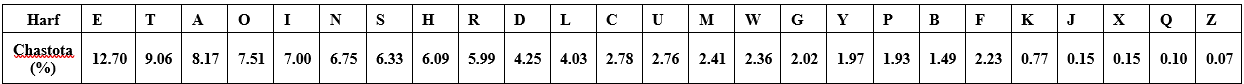
**“OEK XQLU RUUD SXEIUD JE SQHHO EKJ Q SHYJYSQB CYIIYED. JXU JQHWUJ YI XYWXBO FHEVUIIYEDQB, QDT OEK CKIJ RUJHQO DE JHQSU EV OEKH FHUIUDSU. QDO CYIJQAUI MYBB SEIJ OEK ULUHOJXYDW. JXU FBQD YI SQHUVKBBO SHQVJUT JE UDIKHU IKSSUII, RKJ MU DUUT OEK JE RU UNJHUCUBO SQHUVKB.”**

1. Найти обратное число по заданному модулю. **;**
2. Расшифруйте зашифрованный текст методом магического квадрата 5×5:

**“GAPRILOPMNHNMCOGASOTRITYO”**

1. Расшифруйте зашифрованный текст, используя алгоритм шифрования RSA, описанный ниже. **C= 128383, N= 333511, e= 43;**
2. Расшифруйте заданный зашифрованный текст с помощью частотного криптоанализа?

Частотные характеристики английского языка:



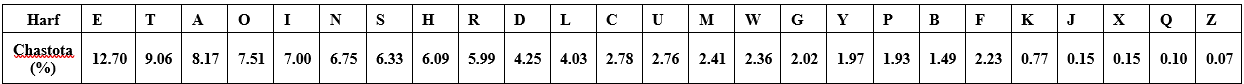
**“NYVE KYV JLE XFVJ UFNE, NV NZCC SVXZE KYV FGVIRKZFE. PFL DLJK SV RK KYV DRIBVU CFTRKZFE SVWFIV DZUEZXYK. KYV KIZTB ZJ KF XVK ZEHLZVK REU TFDGCVKVCP LEUVKVTKVU. NV TRIIP RCC KYV KFFCJ NV EVVU. KYV DZJJZFE DLJK JLTTVVU.”**

1. Найти обратное число по заданному модулю. **;**
2. Расшифруйте зашифрованный текст методом магического квадрата 5×5:

**“GIEIMSYTHARPTKYNICECWISNO”**

1. Расшифруйте зашифрованный текст, используя алгоритм шифрования RSA, описанный ниже. **C= 361708, N= 381923, e= 43;**
2. Расшифруйте заданный зашифрованный текст с помощью частотного криптоанализа?

Частотные характеристики английского языка:



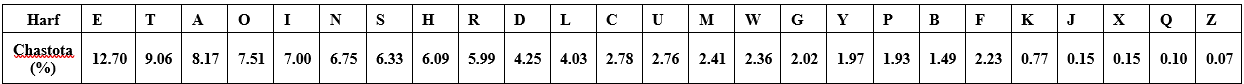
**“VOJS AWGGWCB TCF MCI. MCI BSSR HC TWBR HVS ZCQOHWCB CT HVS GSQFSH ASSHWBU. HVS ASSHWBU WG OH VWRRSB DZOQS HVOH BC CBS YBCKG OPCIH. MCI AIGH PS QOFSTIZ BCH HC ZSOJS OBM QZWSG PSVWBR. HVS SBSAM WG KOHQVWBU MCI.”**

1. Найти обратное число по заданному модулю. **;**
2. Расшифруйте зашифрованный текст методом магического квадрата 5×5:

**“POQOUDKRJMCBXVRNOOEIFSGUW”**

1. Расшифруйте зашифрованный текст, используя алгоритм шифрования RSA, описанный ниже. **C= 259064, N= 360329, e= 37;**
2. Расшифруйте заданный зашифрованный текст с помощью частотного криптоанализа?

Частотные характеристики английского языка:



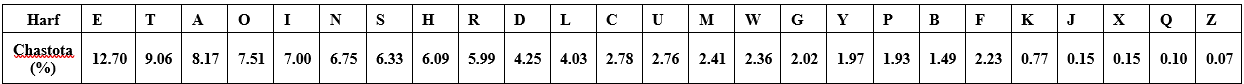
**“OZYE QZCRPE EZ MCTYR ESP AZWTNP. ESP AWLY TD EZ NLENS ESP DFDAPNE LE ESP DELETZY. HP HTWW RTGP ESP DTRYLW HSPY TE TD DLQP EZ XZGP TY. LYJ OPWLJ NZFWO RTGP ESP DFDAPNE ETXP EZ PDNLAP. XLVP DFCP LWW XPXMPCD LCP CPLOJ LE ESP DAPNTQTPO ETXP.”**

1. Найти обратное число по заданному модулю. **;**
2. Расшифруйте зашифрованный текст методом магического квадрата 5×5:

**“TIHGRGOAAELMUTNCQSILSESEI”**

1. Расшифруйте зашифрованный текст, используя алгоритм шифрования RSA, описанный ниже. **C= 177611, N= 474473, e= 37;**
2. Расшифруйте заданный зашифрованный текст с помощью частотного криптоанализа?

Частотные характеристики английского языка:



**“GUVF VF GRFG GB PNGPU IREL YNETR FUNEX. JR UNIR GB ZNXR FHER GUNG NYY GUR ARGF NER VA CYNPR. VS JR ZVFF NALGUVAT, GUR FUNEX ZVTUG RFPNCR. VA GUVF TNZR, GVZR VF BS GUR RFFRAPR, NAQ JR ZHFG NPG SNFG.”**