

Метод RSA

Завдання (Самостійна робота №1)

Розшифрувати фразу з латинських символів (кодування ASCII), зашифровану алгоритмом RSA.

Варіант 1.

(модуль $n=305900099$, відкритий ключ $e=17257$).

Фраза(56 символів):

303218210 235737614 12049114 65976054 47339400 162873714 93971996 78285016 65976054
199688088 162873714 93971996 94490313 188004229 162873714 94490313 65721581 231894123
65976054 78285016 235737614 188004229 65976054 122655609 93971996 235737614 12049114
15620496 65976054 231894123 235737614 65976054 47339400 162873714 93971996 78285016
65976054 298936679 2925556 47339400 65721581 231894123 65976054 78285016 235737614
188004229 65976054 162873714 151170868 65721581 65976054 162873714 65976054 47339400
162873714 93971996

Варіант 2.

(модуль $n=306005033$, відкритий ключ $e=17257$).

Фраза(43 символа):

128350614 6703033 257174402 130325230 176156754 53707912 79940138 176156754 153919375
79940138 257174402 209444216 51176413 176156754 53707912 265505402 130325230 6703033
176156754 41983609 153919375 79940138 257174402 190182858 153061207 209444216 79940138
176156754 53707912 79940138 176156754 51176413 79940138 291259034 79940138 209444216
176156754 9046462 117651886 209444216 73486024 79940138 130325230

Варіант 3.

(модуль $n=383872193$, відкритий ключ $e=32657$).

Фраза(45 символів):

12978094 169899896 100265847 41583759 138093163 234453534 308269565 175631787
182062217 72025863 169223483 182062217 41583759 6921485 175631787 81489883 81489883
41583759 234453534 169223483 169911266 175631787 182062217 158317953 182062217
41583759 195313862 282103049 100265847 182062217 41583759 308269565 169911266
234453534 72025863 41583759 282103049 169899896 100265847 41583759 199951051 282103049
100265847 169223483 182062217

Варіант 4.

(модуль $n=686530157$, відкритий ключ $e=33721$).

Фраза(42 символа):

484531375 336760179 509690251 505258072 355612286 676188508 123505334 490569067
539618080 505258072 130404878 676188508 409409484 355612286 505258072 13390192
539618080 123505334 355612286 505258072 508868492 336760179 509690251 505258072
482789597 336760179 409409484 355612286 505258072 534296388 676188508 676188508
576324693 505258072 355612286 336760179 505258072 423266821 676188508 123505334
644743513 534296388

Варіант 5.

(модуль $n= 310021783$, відкритий ключ $e= 17657$).

Фраза(64 символа):

201195786 19776506 261357195 165422523 303340842 235403339 19776506 303340842
134720377 19776506 273556237 165422523 185323849 19776506 165422523 266888596 4485104
24041966 180050949 4485104 19776506 303340842 261357195 19776506 261357195 266888596
149562732 185323849 166476210 19776506 24041966 306024810 273556237 19776506 273556237
165422523 266888596 273556237 19776506 303340842 261357195 19776506 134720377
180050949 273556237 19776506 284192102 165422523 266888596 273556237 19776506
266888596 19776506 261357195 165422523 303340842 235403339 19776506 303340842
261357195 19776506 149562732 180050949 4485104

Варіант 6.

(модуль $n= 308737337$, відкритий ключ $e= 17657$).

Фраза(40 символів):

279604812 23295830 153283840 227200722 44931545 105047949 23295830 306850011 197827502
227200722 152539466 69010571 23295830 211670599 227200722 5595583 197827502 227200722
105047949 23295830 3071939 18553803 19316748 153283840 184458268 227200722 44931545
105047949 23295830 306850011 197827502 227200722 18553803 184458268 153283840
105047949 197827502 69010571 184458268 153283840