Изазов 1.

Анђела је послала Борису поруку написану на енглеском језику коју је шифровала RSA алгоритмом, својим јавним RSA кључем (e=509, n=64507). Порука је шифрована тако што су груписана два по два слова приказана у ASCII формату и претворена у бројеве (на пример: ‘ABCDEF’ је разбијено у двословне групе (‘AB’, ‘CD’ и ‘EF’), а онда је свака група претворена у бројеве ‘AB’=256*65+66=16706, ’CD’=256*67+68=17220 и ‘EF’=256*69+70=17734). Шифрована вредност је приказана као група од 4 хексадецималне вредности.

1. Одредити Анин приватни кључ d
2. Дешифровати поруку.

Шифровани текст:

```
'4209c15b6135828160d357324302b4b8b8b7563aa801d2b2c15b0cc1c15b082df1f2063e
ecbe618f0a72da373abae48460d30a724e4ae484266b68cdf27fa339545434d127a89094e
061035668cd266b5e5e61446562ccb060d31d0ae4e57df1618f384b6865266b68cd430255
eef1f2063ee6f75656739057321ce90898266bd7ea002073909a29604f2d403833790ce48
46c1560f060d394145e5ef06f1d4161448f1b0cc161cb6144ee55f0f13833495cf1f2063e
d9840f10f9d41ce9b4b81ce19aefdf03503c9d30e1a8f6063fc9f606ee5590946b055f5fc
190c15bc0612916c15b0cc1c15b8b6ba212de92c2c1c15b4c1034d10cc1c15b1e1b6969bf
37e91f29161ce9ba18618f4e4a80c4ab121d4161442d4000acf33e5f62e48460d3d937caa
aaf00a9e57b1da0d461351ce160d35732389e1ce19093f1f6f6bdee556144a2126969bf37
ecbe383324284ced38c8a80174942773ee5560d3f72a08981ce90898d5a7caaa1b02637f2
d40a2126144b9bcf958277360d3e746a2120ba438c8f27f2e21b975389ea929a21269690d
0cde381c8819f5a212de92b9bc1c88f0f1bffb61442d40ab12f6062e215e5e573275602b2
fcaaa75225f5fa1a8604fc2c1614465627390f9d456563801266b68cd7df1c8e238330cc1
61cb43021a2d0b410d0cb7abf27f48e10f43f27f8f1b1e3e7b7cde924dba73905f6231117
b6bc320bf37bd50c15b0fb26350e4846144656273902b8bcb0b61442d4061445732363561
4465627390b28df06fbf37d700b8b761445f6211b848e1f6063fc960d35732503c7e7e6c0
7e48460d3d7eaee550f430356839f5732604f61cb0bbeb4b8e1c11cb1b614a0d4ba1811b8
1d0acfbc0b410d0ca2a82d40bffb7390db1eaca8c15bcfbc1ce180dc60d357322627e1c1c
320'
```