Example

Stian Onarheim

November 11, 2020

1 Input

For this example, I have chosen a relative small prime number and a short message. My implementation of the Elgamal encryption algorithm includes the option to enable detailed printing, which is enabled in this example. I tried creating an example with a 250 digit prime number and the file *elgamal.py* as the input message. Even though it was done rapidly, the output took 35 pages. Therefor I have chosen to use a smaller example.

1.1 Parameters

Message: Diskret? Dette er et lite eksempel som beviser at koden fungerer.

Detailed Printing: True

Prime Number: 5579503

Generator: 7

2 Output

Success!
Plaintext: Diskret? Dette er et lite eksempel som beviser at koden fungerer.
Prime Number: 579503

Blocks: (33)
068105 115107 114101 116063 032068 101116 116101 032101 114032 101116
032108 105116 101032 101107 115101 109112 101108 032115 111109
032098 101118 105115 101114 032097 116032 107111 100101 110032
102117 110103 101114 101114 046

Encrypted Blocks:
[261697, 265147] [501644, 106395] [64002, 143736] [280841, 316354] [258083,
95146] [301004, 133834] [298368, 69693] [299594, 501608] [435854, 563120]
[548863, 494303] [106614, 270611] [146777, 383893] [571003, 513873]
[237075, 81942] [473705, 560143] [64572, 322873] [452491, 146117]
[279390, 399689] [388946, 514543] [299584, 351655] [372779, 422118]
[261402, 256980] [302667, 397835] [414253, 129671] [527143, 44982]
[368365, 527400] [265221, 410218] [209299, 354355] [174431, 478922]
[352750, 221315] [540037, 171966] [383188, 419416] [496356, 210860]

Decrypted Blocks:
068105 115107 114101 116063 032068 101116 116101 032101 114032 101116
032108 105116 101032 101107 115101 109112 101108 032115 111109
032098 101118 105115 101114 032097 116032 107111 100101 110032
102117 110103 101114 101114 046

Decrypted Message:
Diskret? Dette er et lite eksempel som beviser at koden fungerer.