Criptografia RSA

A segunda parte da avaliação deverá ser construído um módulo de criptografia RSA que será postado no github, com data final de entrega em 12 de abril, também deverá ser feito um relatório em LaTeX explicando o método usado para construir o módulo de criptografia além da documentação do código, a classe RSA deverá ter no mínimo as seguintes especificações:

1. Função setup, não recebe nenhum parâmetro e cria as chaves públicas e privadas aleatórias (seguindo as restrições do algoritmo, sugere-se números pequenos).
2. Uma função encrypt, que recebe uma string consistindo na mensagem a ser criptografada e devolve uma string a mensagem criptografada.
3. Uma função decrypt, que recebe uma string consistindo na mensagem a ser descriptografada e devolve uma string a mensagem descriptografada.

As mensagens de entrada do algoritmo sempre serão compostas por caracteres do alfabeto inglês em letras minúsculas, o código deverá incluir tratamento de erros (por exemplo o uma tentativa de passar um texto inválido como entrada para a criptografia).

O esquema para a conversão de caracteres em inteiro(e vice versa) seguirá o padrão UTF-8. Esse padrão pode converter inteiros menores que 1 milhão em caracteres(por isso o incentivo a números pequenos para a formação das chaves), por padrão as funções ord e chr do python já usam UTF-8.