UNIVERSIDADE
FEDERAL DO CEARÁ

Segurança - 2022.1

Prof. Marcos Dantas Ortiz - mdo@ufc.r

Aluno:_____

1) Considerando o RSA com ***p*** = 3, ***q*** = 11 e ***e*** = 7, faça:
   a) Quais são os valores para ***n*** e ***z.***
   b) Encontre ***d.***
   c) Criptografe a mensagem: ***Hello***

n = pq
z = (p-1)(q-1)
$c = m^e \bmod n$
ed mod z = 1
$m = c^d \bmod n$

2) Realize a criptografia e decriptografia usando o algoritmo RSA, para os itens abaixo:

a) p = 5, q = 7, e = 5, M = 5
b) p = 17, q = 11, e = 7, M = 9
c) p = 11, q = 13, e =11, M = 8
d) p = 17, q = 31, e = 7, M = 2