UNISENAI – Banco de dados 8ºp – Cifra assimétrica (RSA).

1) Utilize o algoritmo RSA para realizar o processo de **encriptação** e **decriptação** de uma mensagem curta, aplicando os conceitos estudados sobre geração de chaves, uso de chaves pública e privada, e representação numérica de caracteres.

Use a seguinte correspondência simples para converter o texto em valores numéricos:
a = 1, b = 2, c = 3, ..., z = 26, espaço = 27.

O texto plano a ser criptografado é:

M = aula de seguranca

Realize a encriptação e a decriptação **letra por letra** utilizando o algoritmo RSA para cada um dos conjuntos de parâmetros abaixo:

a) p = 3, q = 11, e = 7
b) p = 7, q = 11, e = 17

Criptografe com a chave privada (d, n) e decripte com a chave pública (e, n), representando o caso de autenticidade.

2) Tociente de Euller sendo 160. Qual dos seguintes valores **não** poderia ser escolhido como expoente público (e)?
   a) 7
   b) 10
   c) 9
   d) 23

3) A expressão de $\equiv 1 \pmod{\phi(n)}$ é fundamental para encontrar a chave privada. Se $\phi(n) = 160$, e = 19, qual é o valor de d?
   a) 161
   b) 7
   c) 59
   d) 160
   e) 58

4) Qual é o princípio de segurança fundamental do RSA?
   a) A dificuldade em calcular M^e (mod n).
   b) A dificuldade em fatorar n em seus componentes primos p e q.
   c) A dificuldade em gerar números primos grandes p e q.
   d) A dificuldade em encontrar d conhecendo e e $\phi(n)$.

5) Quais são os componentes da Chave Pública (PU) e da Chave Privada (PR)?

   a) PU = {d, n} e PR = {e, n}.
   b) PU = {e, n} e PR = {d, n}.
   c) PU = {p, n} e PR = {q, n}
   d) PU = {e, $\phi(n)$} e PR = {d, $\phi(n)$}

6) Qual é um dos principais pontos críticos das cifras simétricas que a criptografia assimétrica, como o RSA, visa resolver?

   a) A necessidade de compartilhamento seguro de uma chave única.
   b) A dificuldade de descriptografar a mensagem.
   c) A falta de confidencialidade na mensagem.
   d) A lentidão no processo de criptografia.

7) No contexto da criptografia assimétrica, qual é o principal objetivo de se criptografar uma mensagem com a *chave privada* do remetente?

   a) Garantir a autenticação.
   b) Aumentar a velocidade da transmissão.
   c) Garantir a confidencialidade da mensagem.
   d) Gerar um par de chaves públicas.

8) No contexto da criptografia assimétrica, qual é o principal objetivo de se criptografar uma mensagem com a *chave pública* do destinatário?

   a) Garantir a autenticação.
   b) Aumentar a velocidade da transmissão.
   c) Garantir a confidencialidade da mensagem.
   d) Gerar um par de chaves públicas.