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:

* 1. p = 3, q = 11, e = 7
  2. 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.

1. Tociente de Euller sendo 160. Ǫual dos seguintes valores **não** poderia ser escolhido como expoente público (e)?
   1. 7
   2. 10
   3. 9
   4. 23
2. A expressão de ≡ 1 (mod φ(n)) é fundamental para encontrar a chave privada. Se φ(n) = 160, e = 19, qual é o valor de d?
   1. 161
   2. 7
   3. 59
   4. 160
   5. 58
3. Ǫual é o princípio de segurança fundamental do RSA?
   1. A dificuldade em calcular Mᵉ (mod n).
   2. A dificuldade em fatorar n em seus componentes primos p e q.
   3. A dificuldade em gerar números primos grandes p e q.
   4. A dificuldade em encontrar d conhecendo e e ϕ(n).
4. Ǫuais são os componentes da Chave Pública (PU) e da Chave Privada (PR)?
   1. PU = {d, n} e PR = {e, n}.
   2. PU = {e, n} e PR = {d, n}.
   3. PU = {p, n} e PR = {q, n}
   4. PU = {e, φ(n)} e PR = {d, φ(n)}
5. Ǫual é um dos principais pontos críticos das cifras simétricas que a criptografia assimétrica, como o RSA, visa resolver?
   1. A necessidade de compartilhamento seguro de uma chave única.
   2. A dificuldade de descriptografar a mensagem.
   3. A falta de confidencialidade na mensagem.
   4. A lentidão no processo de criptografia.
6. No contexto da criptografia assimétrica, qual é o principal objetivo de se criptografar uma mensagem com a *chave privada* do remetente?
   1. Garantir a autenticação.
   2. Aumentar a velocidade da transmissão.
   3. Garantir a confidencialidade da mensagem.
   4. Gerar um par de chaves públicas.
7. No contexto da criptografia assimétrica, qual é o principal objetivo de se criptografar uma mensagem com a *chave pública* do destinatário?
   1. Garantir a autenticação.
   2. Aumentar a velocidade da transmissão.
   3. Garantir a confidencialidade da mensagem.
   4. Gerar um par de chaves públicas.