UNIVERSIDADE FEDERAL DO CEARÁ

**Campus Quixadá**
**Disciplina: Segurança - Período 2024:1**
**Prof. Marcos Dantas Ortiz - mdo@ufc.br**
**Lista - Cripto. Assimétrica e Hash - entrega 27/03/24**

---

**RSA - Geração de Chaves**

1. Escolha dois números primos grandes p, q.

2. Calcule **n** = pq, **z** = (p - 1)(q - 1)

3. Escolha **e** (com e < n) que não tenha fatores comuns com z. (e, z são "relativamente primos").

4. Escolha **d** tal que ed - 1 seja divisível exatamente por z.

(em outras palavras: **ed mod z = 1** ).

5. Chave pública é (n,e)

6. Chave privada é (n,d).

**RSA - Cifragem e Decifragem**

1. Para criptografar a mensagem m (<n), calcule $\mathbf{c = m^e \bmod n}$

+2. Para descriptografar o padrão de bits recebido, c, calcule $\mathbf{m = c^d \bmod n}$

---

**Questão 1)** Usando o algoritmo de chave pública RSA, faça:

a) Se $p = 7$ e $q = 11$, liste 5 valores válidos para $e$.

R- e = [7, 11, 13, 17, 19]

b) Se $p = 13$, $q = 31$, e $e = 7$, encontre $d$.

R- d = 103

c) Usando $p = 5$, $q = 11$, e $e = 27$, encontre $d$ e criptografe "RSA". Utilize A = 1, B = 2, C = 3... , Z = 26

R- C1 = 18 ^ 27 mod 55 = 17

C2 = 19 ^ 27 mod 55 = 24

C3 = 1 ^ 27 mod 55 = 1

**Questão 2)** Em um sistema de chave pública usando RSA, você intercepta o texto cifrado C = 10 enviado a um usuário cuja chave pública é (e = 5, n=35). Qual é o texto claro M?

R- Como n=35, descobrimos que p = 5 e q = 7 e que z = 24. Para decifrar, precisamos de D, descoberto com ed mod z = 1. D = 5, pois 5.5-1 mod 24 = 0. Usando M = c ^d mod n, descobrimos que m = 5.

**Questão 3)** Quais são os requisitos que devem ser atendidos pelos algoritmos de chave pública?

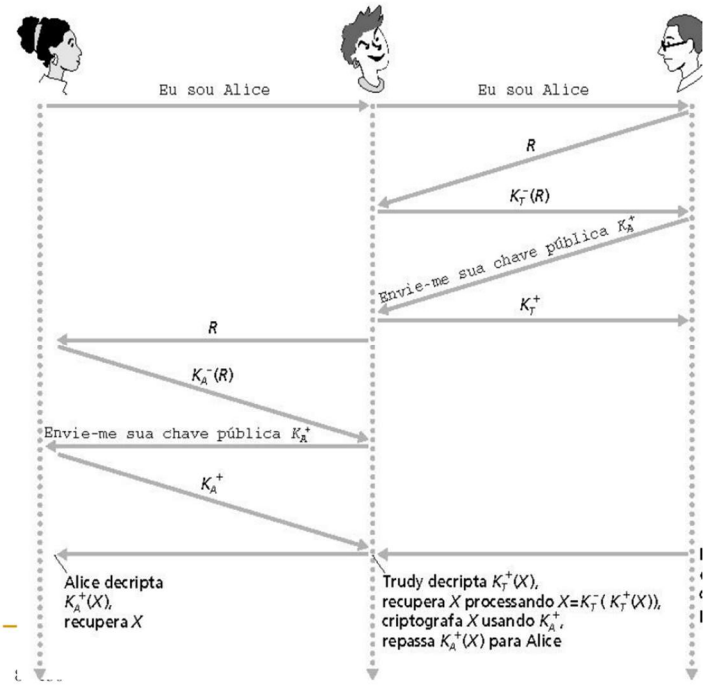
R- 1: tendo Kb+ (.) e Kb-(.), Kb-(Kb+(m)) = m.

2: Não é possível calcular a chave privada Kb- a partir da chave privada Kb+.

3: Tendo a chave pública Kb+ e o texto cifrado C, deve ser inviável encontrar um texto M.

**Questão 4)** Explique, através de um diagrama com troca de mensagens, o ataque man-in-the-middle (homem do meio) sobre autenticação com criptografia assimétrica. Qual a falha é explorada por este ataque? Ele também pode ocorrer quando utilizado criptografia simétrica? Justifique sua resposta.

R-




A falha explorada é a falta de autenticação das chaves públicas. Alice e Bob não têm garantia de que as chaves públicas que receberam realmente pertencem um ao outro, permitindo que Trudy intercepte e manipule a comunicação. Embora o ataque man in the middle possa teoricamente ocorrer com criptografia simétrica, sua execução é mais difícil. Isso ocorre pois na criptografia simétrica ambas as partes precisam compartilhar

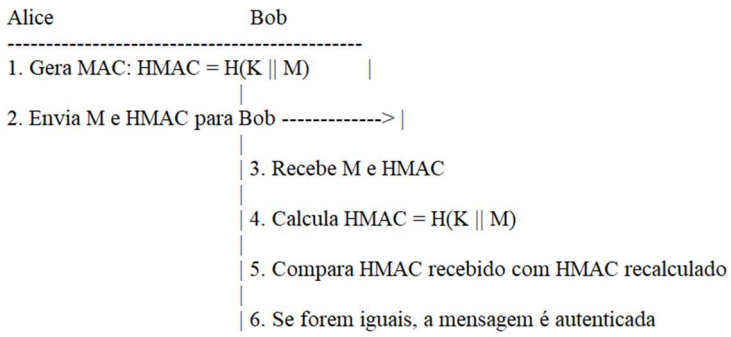
a mesma chave secreta, e um atacante precisaria interceptar essa chave para realizar o ataque.

**Questão 5)** Explique como funções Hash são usadas para fornecer integridade.

R- Funções Hash garantem a integridade pelo seu mecanismo rápido, irreversível e determinístico. O código hash sempre será o mesmo para uma entrada específica, e muda a qualquer alteração, tendo um código irreversível.

**Questão 6)** Descreva como o protocolo HMAC (Message Authentication Code) fornece autenticação. Faça um diagrama com a troca de mensagens.

R- usando uma combinação de uma função de hash criptográfica e uma chave secreta compartilhada entre as partes envolvidas na comunicação. A autenticação é alcançada através da geração e verificação de um código de autenticação de mensagem (MAC) anexado à mensagem original.




**Questão 7 (**FCC-2009-TJ-PI-Analista Judiciário-Análise de Sistemas) - O usuário torna a sua chave **I** disponível para todos os que podem eventualmente enviar-lhe informações criptografadas. Essa chave pode apenas codificar os dados, mas não pode descodificá-los, ou seja, não pode abrir as informações criptografadas, mas é capaz de criptografar um arquivo. No envio da informação criptografada, a chave **II** é utilizada, e quem recebe o texto cifrado, descodifica-o com a chave **III** . O algoritmo de criptografia **IV** rata o texto como se fosse um número muito grande, eleva-o à potência de outro número também enorme e, então, calcula o restante depois de dividido por um terceiro número igualmente gigantesco. Por fim, o número resultante de todo este processo é convertido de novo em texto. Na criptografia **V** o algoritmo divide os dados em pequenos pedaços chamados de blocos, depois coloca letras em volta, muda a informação presente em cada bloco para números, comprime e expande esses dados e coloca esses números em fórmulas matemáticas que incluem a chave. Então o algoritmo repete todo o processo, até mesmo dúzias de vezes, se necessário.

**Completam correta e respectivamente as lacunas I a V:**

a) pública; privada; privada; simétrica; assimétrica.

b) pública; privada; pública; assimétrica; simétrica.

c) privada; privada; pública; assimétrica; simétrica.

d) pública; privada; pública; simétrica; assimétrica.

e) **pública; pública; privada; assimétrica; simétrica.**

R- letra e.

**Bom Trabalho!**