Exercícios – RSA, Hash, Assinatura digital

CELSO PEREIRA DO VALE JÚNIOR

1) Chaves públicas, que podem ser amplamente disseminadas, e chaves privadas que são conhecidas apenas pelo proprietário. Autenticação, onde a chave pública verifica que um portador da chave privada enviou a mensagem, e encriptação, onde apenas o portador da chave privada pode realizar a decriptação da mensagem encriptada com a chave pública.
2) A chave pública garante que todos que queiram se comunicar com o receptor possam criptografar uma mensagem e enviá-la para comunicação, já o receptor da mensagem deve possuir uma chave secreta que somente ele terá acesso, denominada chave privada, esta chave será utilizada para decifrar a mensagem original e assim somente o receptor legítimo poderá ter acesso ao conteúdo. O mesmo acontece caso o receptor desta mensagem queira enviar uma resposta a quem enviou lhe esta mensagem ele deve possuir a chave pública do emissor da mensagem e o emissor tem de possuir uma chave secreta para decifrar a resposta da mensagem.
3) Deve ser fácil gerar uma chave pública a partir da chave privada, mas computacionalmente intratável o processo inverso. O algoritmo deve ser público e o processo de encriptação deve ter a propriedade da avalanche, no qual uma pequena mudança no texto puro gera uma grande diferença no texto cifrado.
4) No contexto da teoria matemática, significa dizer que a função não tem inversa. Na prática, ser unidirecional representa que não é possível recuperar o dado original a partir do resumo gerado.
5) Uma função unidirecional é com segredo, se existe uma informação que torna a computação da sua inversa possível.
6) Dados p=7, q=19 e mensagem M=23

   N = pxq = 133

   Fi(n) = (p–1)(q–1) = 108

   Escolher um **e** aleatório, tal que gcd(fi(n) ,e) = 1; 1 < e < fi(n)

   e = 47

   d = e^{-1} mod 108 = 47^{-1} mod 108 = 23

   KU = {e, n} = {47, 133}

$C = M^e$ mod $n = 23^{47}$ mod 133 = 130

Prova: $M = C^d$ mod $n = 130^{23}$ mod 133 = 23

7) 53 é primo, logo preciso fatorar 49

Fatoração de 49 = 7^2 e $49^{13} \equiv 7^{26}$ mod 53

M.D.C(7,53) = 1 (Primos entre si)

7^{52} = 1 mod 53 = 1

(7^{26} mod 53) (7^{26} mod 53) = 1

Então, 7^{26} mod 53 = 1

$(7^2)^{13}$ mod 53 = 1

49^{13} mod 53 = 1

8) Dados C=10, e=5, n=35

Para achar p e q, fatorei o 35 em 5x7

p=5 e q=7

Fi(n) = 4x6 = 24

$d = e^{-1}$ mod Fi(n) = 5

M = C^e mod $n = 10^5$ mod 35 = 5

9) Dados e=31, n=2491 encontrar d.

Para encontrar p e q, irei utilizar a raiz quadrada de n.

Sqrt(2491) ~= 49. O primeiro primo abaixo é 47 e o primeiro primo acima é 53.

p=47 e q=53 se pxq = 2491 (Satisfeito)

Fi(n) = 46x52 = 2392

d= 31^{-1} mod 2392 = 463

10) Dados p=7, q=19, e=49 e M=31, calcular C.

n=pxq = 133

$C = M^e$ mod $n = 31^{49}$ mod 133 = 31

11) Dado n = 3552377 e Fi(n) = 3548580, encontrar p e q.

Para encontrar p e q precisamos fatorar n.

```csharp
using System;

public class Program
{
    public static void Main()
    {
        int num = 3552377;
        int divi = 1;

        while (divi < num)
        {
            if ( num % divi == 0 )
                Console.WriteLine($"{divi}");
            divi++;
        }

    }
}
```

```
1
1667
2131
```

Os únicos divisores diferentes de 1 são **1667 e 2131**, então estes serão os valores de p e q.

12) Dados n=10403, e=8743.

Fatorando a partir de sua raiz quadrada (~=101) n, temos que p = 101 e q = 103.

Fi(n) = 10200

d = 8743^{-1} mod 10200 = 7

4746^7 mod(10403) = 1514 = FE

8214^7 mod(10403) = 2722 = RM

9372^7 mod(10403) = 1029 = AT

9009^7 mod(10403) = 9931 = (ESPAÇO) V

4453^7 mod(10403) = 1831 = IV

8198^7 mod(10403) = E

FERMAT VIVE

13) Dados n=7597, e=4947, Fi(n) = 7420. Decodificar M = 6355-5075.

d = 4947^{-1} mod 7420 = 3

Plain = M^d mod n

Plain1 = 6355^3 mod 7597 = 151

Plain2 = 5075^3 mod 7597 = 822

x = 15 18 22 = FIM

14) Dados e= 9047, n= 7085

Como 83 divide 9047, p=83

Logo q= 9047/83 = 109

Fi(n) = 82x108 = 8856

d = e^{-1} mod Fi(n)

d = 7085^{-1} mod 8856 = 5

M1 = 8655^5 mod 9047 = 2930 = TU

M2 = 1969^5 mod 9047 = 1220 = CK

M3 = 1563^5 mod 9047 = 1427 = ER

M = TUCKER

15) Dados p = 127, q = 211, e = 4811.

n = pxq = 26797

Fi(n) = 126x210 = 26460

d = 4811^{-1} mod 26460 = 11

M1 = 17523^{11} mod 26797 = 272

M2 = 9183^{11} mod 26797 = 810

M = 27 28 10 = RSA

16) Dados n=7171, e=4667, Fi(n)=7000

d = 4667^{-1} mod 7000 = 3

M1 = 2196^3 mod 7171 = 301

M2 = 3791^3 mod 7171 = 510

M = 30 15 10 = UFA

17) Considerando que cada usuário terá “p”, “q” e “e” (que são primos gerados aleatoriamente), deverá ter 3xN primos.

18) Chaves de sessão são chaves temporárias usadas em algoritmos simétricos, sendo trocadas constantemente. Chaves mestras são usadas para encriptar e distribuir chaves de sessão dentro de um criptossistema de chaves públicas.

19) Troca de Chaves por Diffie-Hellman, Protocolo de Distribuição de Chaves.

20) Dado p=19, encontrar uma raiz primitiva.

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Para alfa = 2, temos todas as potências distintas e formam a sequência de 1 a p-1 (18), logo, é 2 é uma raiz primitiva.

21) q = 11 x = 2

a)

a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}
2	4	8	5	10	9	7	3	6	1	V

Todas as potências são distintas e forma a sequência de 1 a p-1. 2 é uma raiz primitiva.

b) Dados alfa = 2 e q=11, $Y_A = 9$.

$Y_A = \text{alfa}^{XA} \bmod q$

$9 = 2^{XA} \bmod 11$

A dificuldade é encontrar o logaritmo discreto de $\text{Log}_2(9) \bmod 11$. Por tentativa e erro encontramos que $\mathbf{X_A = 6}$, pois $2^6 = 64$ e $64 \bmod 11 = 9$.

c) Se $Y_B = 3$ e $X_A = 6$, logo:

$\mathbf{K = Y_B^{XA} \bmod q = 3^6 \bmod 11 = 3}$

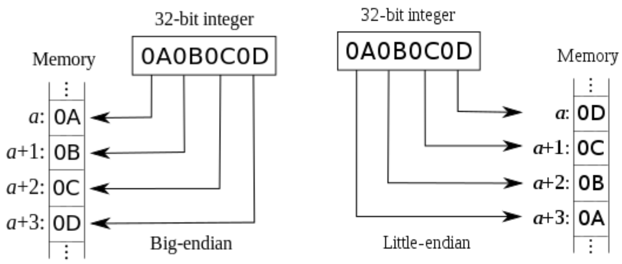
22) A resistência à colisão fala que deve ser difícil encontrar duas mensagens diferentes m1 e m2 tal que hash(m1) = hash(m2), mas não impossível.

23) A função de dispersão pode calcular o mesmo índice para duas chaves diferentes, uma situação chamada colisão, onde duas mensagens diferentes m1 e m2 tal que hash(m1) = hash(m2).

24) Uma pequena mudança na mensagem gera uma grande mudança na hash gerada. É importante pois dificulta ataques que tentam mapear caracteres mais recorrentes na hash a caracteres recorrentes em alguma linguagem humana.

25) Os bytes são guardados por ordem crescente do seu "peso numérico" em endereços sucessivos da memória (extremidade menor primeiro ou little-endian).

Os bytes são guardados por ordem decrescente do seu "peso numérico" em endereços sucessivos da memória (extremidade maior primeiro ou big-endian)



26) Lógicas: and, or, xor e not. Aritiméticas: Adição modular e inversa modular.

27) Porque as funções hash utilizam algoritmos de chave pública que têm a segurança baseada na dificuldade computacional de fatorar números primos de grande ordem, que, apesar de mais custoso para utilizar, não necessita de uma performance tão grande que os algoritmos de chave privada fornecem (em troca de algoritmo não tão robusto).

28) *Autenticidade*: o receptor deve poder confirmar que a assinatura foi feita pelo emissor;

Integridade: qualquer alteração da mensagem faz com que a assinatura não corresponda mais ao documento;

Irretratabilidade ou não-repúdio: o emissor não pode negar a autenticidade da mensagem.

29) São diversos requisitos que são definidos pelo ICP Brasil (Infra-Estrutura de Chaves Públicas Brasileira) e podem ser encontrados em https://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/15.1/DOC-ICP-15.01_v.1.0.pdf

30) Vantagens: A chave usada para criptografar os dados é diferente da que é usada para descriptografá-los, e achar a chave privada através da chave pública é computacionalmente inviável. Com a assimétrica você consegue não só descriptografar a mensagem, mas também relacionar quem foi o remetente.

A simétrica continua sendo usado por conta de sua melhor performance.

31) Dados e=5, n=35 e C=10, encontrar p.

Como n é muito pequeno, podemos encontrar p e q a partir da raiz quadrada de n.

Sqrt(35) ~= 5.9

Os primos mais próximos são 5 e 7, que são exatamente os valores de p e q. **Logo p = 5.**

32) Para geração da chave, escolhe aleatoriamente dois primos p e q tal que:

-> Os números p e q devem diferir em alguns bits de comprimento (caso contrário p e q ficarão muito próximos da RAIZ(n)).

-> Os números p-1 e q-1 devem conter fatores primos grandes.

-> O mdc(p-1,q-1) deve ser pequeno.

Então é calculado n=pxq e fi(n) = (p -1)(q-1) utilizado para calcular “e” e “d”, que são inversos mod fi(n): e.d = 1 mod fi(n)

O processo de cifragem é realizado com a operação C = M^e (mod n), onde M é o texto plano e C é o texto cifrado.

O processo de decifragem é realizado com a operação M = C^d (mod n).

33)

a) p = 3; q = 11; d = 7; P = 5

n = 3x11 = 33

fi(n) = 2x10 = 20

e = 11^{-1} mod 20 = 11

M = 5^{11} mod 33 = 5

C = 5^{11} mod 33 = 5

b) p = 5; q = 11; e = 3; P = 9

n = 5x11 = 55

fi(n) = 4x10 = 40

d = 3^{-1} mod 40 = 27

M = 9^{27} mod 55 = 4

C = 4^3 mod 55 = 9

c) p = 7; q = 11; d = 17; P = 8

n = 7x11 = 77

fi(n) = 6x10 = 60

e = 17^{-1} mod 60 = 53

M = 8^{17} mod 77 = 57

C = 57^{53} mod 77 = 8

d) p = 11; q = 13; e = 11; P = 7

n = 11x13 = 143

fi(n) = 10x12 = 120

d = 11^{-1} mod 120 = 11

M = 7^{11} mod 143 = 106

C = 106^{11} mod 143 = 7

e) p = 17; q = 31; d = 7; P = 2
n = 17x31 = 527

fi(n) = 16x30 = 480

e = 7^{-1} mod 480 = 343

M = 2^{7} mod 527 = 128

C = 128^{343} mod 527 = 2

f) p= 19, q = 11, e = 17; P=8
n = 19x11 = 209

fi(n) = 18x10 = 180

d = 17^{-1} mod 180 = 53

M = 8^{53} mod 209 = 50

C = 50^{17} mod 209 = 8

g) p=31, q=37, e=17

Não há mensagem para criptografar?

34)

```
static void Main(string[] args)
{
    Console.WriteLine("Insira o valor de n:");
    int n = int.Parse(Console.ReadLine()); // Dado

    /* Fatorar */
    int base2 = 0;
    int resto = n - 1;

    int m = 0, k = 0;

    while (resto >= 1)
    {
        for (int i = 2; i < resto; i++)
        {
            if (resto % i == 0)
            {
                if (i == 2)
                {
                    base2++;
                }
                else if (resto % 2 != 0 && base2 > 0)
                {
                    k = base2;
                    m = resto;
                    Console.WriteLine($"2^{base2} + {resto}");

                    resto = 0;
                    break;
                }

                resto /= i;
                break;
            }
        }
    }

    var random = new Random();
    var a = random.Next() % (n - 1);
    Console.WriteLine($"Testando com a={a}");
    testaPrimo(a, m, n, k);

    a = random.Next() % (n - 1);
    Console.WriteLine($"Testando com a={a}");
    testaPrimo(a, m, n, k);

    a = random.Next() % (n - 1);
    Console.WriteLine($"Testando com a={a}");
    testaPrimo(a, m, n, k);
}

static void testaPrimo(int a, int m, int n, int k)
{
    double b = Math.Pow(a, m) % n;

    if (b == 1)
    {
        Console.WriteLine("É primo");
        return;
    }

    for (int i = 0; i < k - 1; i++)
    {
        if (b == n - 1)
        {
            Console.WriteLine("É primo");
            return;
        }

        b = Math.Pow(b, 2) % n;
    }

    Console.WriteLine("É composto");
}
```

Algoritmo criado para fatorar n de modo que encontre n-1 = $2^k m$, com m ímpar.

a)

```
Insira o valor de n:
101
2^2 + 25
Testando com a=63
É composto
Testando com a=50
É composto
Testando com a=78
É composto
```

b)

```
Insira o valor de n:
103
2^1 + 51
Testando com a=99
É composto
Testando com a=22
É composto
Testando com a=84
É composto
```

c)

```
Insira o valor de n:
887
2^1 + 443
Testando com a=248
É composto
Testando com a=230
É composto
Testando com a=718
É composto
```

d)

```
Insira o valor de n:
907
2^1 + 453
Testando com a=370
É composto
Testando com a=733
É composto
Testando com a=216
É composto
```

e)

```
Insira o valor de n:
911
2^1 + 455
Testando com a=248
É composto
Testando com a=37
É composto
Testando com a=434
É composto
```

f)

```
Insira o valor de n:
24533
2^2 + 6133
Testando com a=6451
É composto
Testando com a=18101
É composto
Testando com a=19785
É composto
```

g)

```
Insira o valor de n:
24547
2^1 + 12273
Testando com a=3340
É composto
Testando com a=17469
É composto
Testando com a=16955
É composto
```

h)

```
Insira o valor de n:
24551
2^1 + 12275
Testando com a=23790
É composto
Testando com a=13465
É composto
Testando com a=11495
É composto
```

i)

```
Insira o valor de n:
786769
2^4 + 49173
Testando com a=113649
É composto
Testando com a=374199
É composto
Testando com a=570469
É composto
```

35)

a) Dados e = 23, n=39

Adotando A = 10, como no exercício 15, temos:

V 31 A 10 M 22 O 24 S 28 (ESPACO) 32 E 14 S 28 T 29 U 30 D 13 A 10 R 27

31^{23} mod 39 = 34

10^{23} mod 39 = 04

22^{23} mod 39 = 16

24^{23} mod 39 = 06

28^{23} mod 39 = 07

32^{23} mod 39 = 11

14^{23} mod 39 = 14

28^{23} mod 39 = 7

29^{23} mod 39 = 35

30^{23} mod 39 = 36

13^{23} mod 39 = 13

10^{23} mod 39 = 04

27^{23} mod 39 = 27

B) Dados p = 3, q = 11, n = 33, e=7

Fi(n) = 20

d = 7^{-1} mod 20 = 3

B 11 O 24 L 21 A 10

Decifrar:

11^7 mod 33 = 11 = B

24^7 mod 33 = 18 = I

21^7 mod 33 = 21 = L

10^7 mod 33 = 10 = A

Cifrar:

11^3 mod 33 = 11 =B

18^3 mod 33 = 24 = O

21^3 mod 33 = 21 = L

10^3 mod 33 = 10 = A

C) Não, pois uma vez que a chave privada foi exposta, Fi(n) é encontrado. Então, qualquer “e” e “d” poderão ser descobertos a partir de um sistema de duas equações e duas incógnitas.

D) Dados p=11, q=17, e=23

L 21 E 14 I 18

C = 21^{23} mod 187 = 98

C = 14^{23} mod 187 = 159

C = 18^{23} mod 187 = 35

D = 98^7 mod 187 = 21

D = 159^7 mod 187 = 14

D = 35^7 mod 187 = 18

36)

a) Fi(n) = 40x16 = 640

E1 não é coprimo com 640, pois tem 2 como divisor, por exemplo, e não pode ser utilizado.

E2 = é coprimo com fi(n), logo pode ser utilizado.

b) 49^{-1} mod 640 = 209

37) Dados p = 31, q = 37, e = 17

n = 31x37 = 1147

Fi(n) = 30x36 = 1080

d = 17^{-1} mod 1080 = 953

M = 2^{17}mod 1147 = 314

38) Porque seria necessário o calculo do logaritmo discreto modular, que é onde mora a dificuldade de se obter a chave privada.

39) p = 467, Alfa = 2

a) Dados XA = 3, XB = 5.

YA = 2^3 mod 467 = 8

YB = 2^5 mod 467 = 32

K = $(YB)^{XA}$ = 32^3mod 467 = 78

K = $(YA)^{XB}$ = 8^5mod 467 = 78

B) Dados XA = 400, XB = 134

YA = 2^{400} mod 467 = 137

YB = 2^{134}mod 467 = 84

K = 84^{400}mod 467 = 90

K = 137^{134} mod 467 = 90

C) Dados XA = 228, XB = 57

YA = 2^{228} mod 467 = 394

YB = 2^{57}mod 467 = 131

K = 313^{228}mod 467 = 206

K = 394^{57}mod 467 = 206

40) Dados n = 9797, e = 131

Encontrando p e q através da raiz quadrada de n:

Sqrt(9797) ~= 98.9

p = 97 e q = 101

Fi(n) = 96x100 = 9600

d = 131^{-1} mod 9600 = 3371

A) 123^{3371} mod 9797 = 6292 **é valido**

B) 4333^{3371} mod 9797 = 1464 **é inválido**

C) 4333^{3371} mod 9797 = 1464 **é válido**