Introdução à Criptografia

Aritmética Modular e Criptografia de Chave Pública

Prof. Rodrigo Minetto
Universidade Tecnológica Federal do Paraná
Baseado em: Understanding Cryptography by Paar e Pelzl

Sumário

Aritmética Modular

A aritmética modular é extremamente importante para a criptografia assimétrica (RSA, curvas elípticas, etc) e permite a descrição de cifras históricas de forma elegante.

A maioria dos sistemas criptográficos são baseados em conjuntos de números que são:

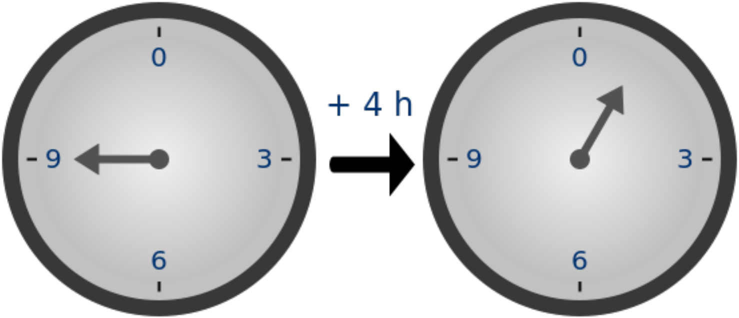
- discretos (conjunto dos números inteiros)
- finitos (conjunto finito de números)

Aritmética Modular

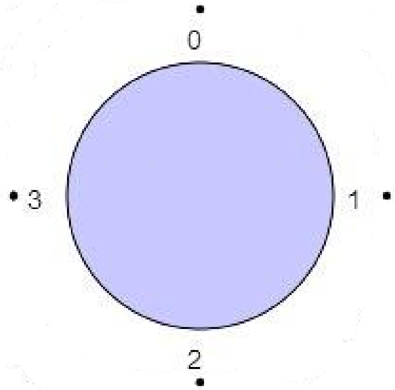
Encontramos a aritmética modular em todos os cantos. Por exemplo, os relógios trabalham com módulos 12 ou 24 para as horas e módulo 60 para os minutos e segundos. Calendários usam módulo 7 para os dias da semana e módulo 12 para os meses. Esse tipo de linguagem foi desenvolvida por Karl Friedrich Gauss no início do século XIX.

Aritmética Modular

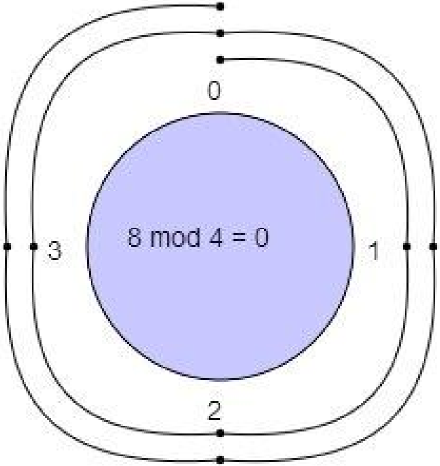
Nesse sistema os números "voltam pra trás" quando atingem um certo valor, o módulo (operação para manter os números dentro dos limites). O relógio abaixo usa a aritmética módulo **12**: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0, 1, . . .



Exemplo: $8 \textbf{ mod } 4 = ?$

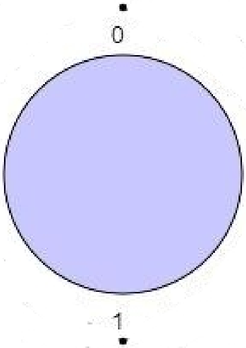


Exemplo: $8 \ \mathbf{mod} \ 4 = \mathbf{0}$!

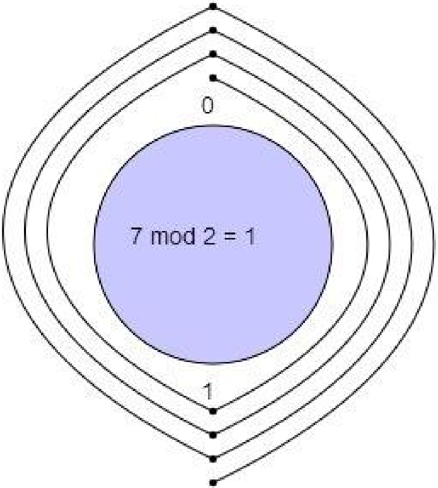


Aritmética Modular

Exemplo: 7 **mod** 2 = ?

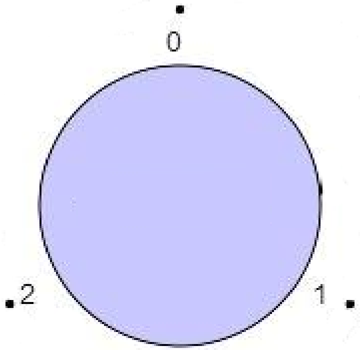


Exemplo: 7 **mod** 2 = **1**!

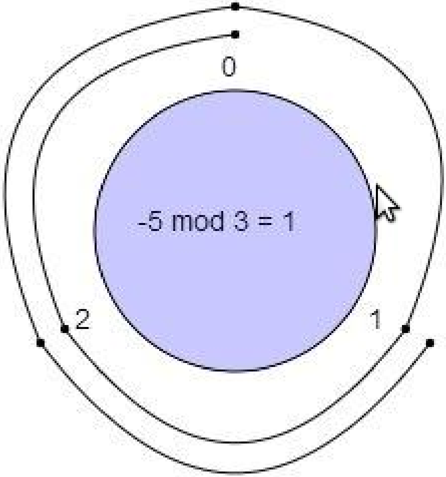


Aritmética Modular

Exemplo: -5 **mod** 3 = ?



Exemplo: -5 **mod** 3 = **1**!



Adição, subtração e multiplicação modular

Suponha a seguinte expressão: $(a+b)$ **mod** n. Podemos obviamente avaliá-la diretamente. No entanto, existe uma propriedade interessante

$$(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n.$$

A mesma propriedade existe para a **subtração**

$$(a-b) \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n.$$

e para **multiplicação**

$$(a \times b) \bmod n = ((a \bmod n) \times (b \bmod n)) \bmod n.$$

Questão: como calcular $q^{x} \bmod n$?

```
typedef long long int ulong;
ulong Naive (ulong q, ulong x, ulong n) {
  int i;
  ulong r = 1;
  for (i = 0; i < x; i++) {
     r = (r * q);
  }
  return r % n;
}
```

Quais os problemas?

Aritmética Modular

Questão: como calcular q^{x} mod n ?

Prop.: $a \times b \bmod n = (a \bmod n \times b \bmod n) \bmod n$

```
ulong Improved (ulong q, ulong x, ulong n) {
  int i;
  ulong r = 1;
  for (i = 0; i < x; i++) {
     r = (r * q) % n;
  }
  return r;
}
```

Aritmética Modular

Sejam dois número naturais **a** e **b** que após efetuadas as divisões por outro número **m**, não nulo, produzem o mesmo resto, ou seja,

$$\mathbf{a} \mod \mathbf{m} = \mathbf{b} \mod \mathbf{m}$$

Dizemos então que "**a** e **b** são **congruentes** módulo **m**", ou ainda, $\mathbf{a} \equiv \mathbf{b} \mod \mathbf{m}$.

Exemplo: $58 \equiv 43$ **mod** 5.

Aritmética Modular

Definição

Sejam $\mathbf{a}, \mathbf{r}, \mathbf{m}$ inteiros e $\mathbf{m} > 0$. Escreve-se

$$\mathbf{a} \equiv \mathbf{r} \bmod \mathbf{m}$$

se $(\mathbf{r} - \mathbf{a})$ é divisível por $\mathbf{m}$.

- $\mathbf{m}$ é chamado de **módulo**.
- $\mathbf{r}$ é chamado de **resto**.

Exemplos:

- $12 \equiv 3 \bmod 9 \rightarrow$ pois 9 divide (3-12)
- $34 \equiv 7 \bmod 9 \rightarrow$ pois 9 divide (7-34)
- $-7 \equiv 2 \bmod 9 \rightarrow$ pois 9 divide (2+7)

Aritmética Modular

Atenção: não confundir

$$a = b \bmod m$$

com

$$a \equiv b \bmod m$$

Exemplos

$$\begin{aligned} 12 &= 5 \bmod 7 \quad \textbf{(falso)} \\ 12 &\equiv 5 \bmod 7 \quad \textbf{(verdadeiro)} \end{aligned}$$

Aritmética Modular

A divisão euclidiana é estruturada da seguinte forma:

$$\begin{array}{r|l} (\textit{dividendo})\ a & m \quad\quad (\text{divisor}) \\ \cline{2-2} (\textit{resto})\ r & q\ (\textit{quociente}) \end{array}$$

Note que $a \equiv r \mod m$ se, e somente se, houver um inteiro q de modo que $a = qm + r$ para $0 \leq r < m$. Desta forma, as congruências podem ser transformadas em igualdades com a adição de uma incógnita.

Aritmética Modular

Note que se $a = qm + r$, então podemos achar facilmente com essa expressão o módulo de números negativos. Exemplo: calcule -5 **mod** 3.

$$\begin{aligned} a &= q * m + r \\ -5 &= q * 3 + r \\ -5 &= -2 * 3 + r \\ -5 &= -6 + r \\ -5 &= -6 + 1 \end{aligned}$$

escolhemos $q = -2$ para ter um valor suficientemente negativo para superar o valor de $a = -5$. Assim -5 **mod** $3 = 1$.

Aritmética Modular

Exemplo: calcule -5 **mod** 7.

$$\begin{aligned} a &= q * m + r \\ -5 &= q * 7 + r \\ -5 &= -1 * 7 + r \\ -5 &= -7 + r \\ -5 &= -7 + 2 \end{aligned}$$

escolhemos $q = -1$ para ter um valor suficientemente negativo para superar o valor de $a = -5$. Assim -5 **mod** $7 = 2$.

Aritmética Modular

Três propriedades importantes da congruência são:

Simetria

- se a é qualquer inteiro *então* $a \equiv a$ **mod** **m**.

Reflexividade

- se $a \equiv b$ **mod** **m** *então* $b \equiv a$ **mod** **m**.

Transitividade

- se $a \equiv b$ **mod** **m** e $b \equiv c$ **mod** **m** *então* $a \equiv c$ **mod** **m**.

Aritmética Modular

Se $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ e $\mathbf{d}$ são inteiros quaisquer tal que

- $\mathbf{a} \equiv \mathbf{b} \ \mathbf{mod} \ m$
- $\mathbf{c} \equiv \mathbf{d} \ \mathbf{mod} \ m$

então

- $\mathbf{a} + \mathbf{c} \equiv \mathbf{b} + \mathbf{d} \ \mathbf{mod} \ m$
- $\mathbf{a} - \mathbf{c} \equiv \mathbf{b} - \mathbf{d} \ \mathbf{mod} \ m$
- $\mathbf{ac} \equiv \mathbf{bd} \ \mathbf{mod} \ m$

Aritmética Modular

Inverso aditivo: para números inteiros $\mathbf{a}$ e $\mathbf{m}$, o inverso aditivo de $\mathbf{a}$ módulo $\mathbf{m}$ é o inteiro $-\mathbf{a}$ tal que

$$\mathbf{a} + (-\mathbf{a}) \equiv 0 \bmod \mathbf{m}$$

Inverso multiplicativo: para números inteiros $\mathbf{a}$ e $\mathbf{m}$, o inverso multiplicativo é definido tal que

$$\mathbf{a} \times \mathbf{a}^{-1} \equiv 1 \bmod \mathbf{m}$$

Aritmética Modular

O inverso multiplicativo não existe para todos os elementos. Um elemento $\mathbf{a}$ tem o inverso multiplicativo $\mathbf{a}^{-1}$ se e somente se o $\mathbf{mdc}(\mathbf{a}, \mathbf{m}) = 1$. Exemplo: calcule 3^{-1} **mod** 26

Aritmética Modular

O inverso multiplicativo não existe para todos os elementos. Um elemento **a** tem o inverso multiplicativo $\mathbf{a}^{-1}$ se e somente se o $\mathbf{mdc}(\mathbf{a}, \mathbf{m}) = 1$. Exemplo: calcule 3^{-1} **mod** $26 =$ **9**.

$$\begin{aligned} x &\equiv 3^{-1} \bmod 26 \\ x &\equiv 1/3 \bmod 26 \\ 3 * x &\equiv 1 \bmod 26 \\ 3 * 9 &\equiv 1 \bmod 26 \end{aligned}$$

Aritmética Modular

A aritmética modular pode ser definida em termos de conjuntos e operações sobre conjuntos. Na matemática, um **anel** é uma estrutura algébrica que consiste em um conjunto e duas operações binárias (adição e multiplicação):

Definição: anel inteiro $\mathbb{Z}_m$

Conjunto: $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$.

Operações: '$+$' e '$\times$' $\forall\ (a, b) \in \mathbb{Z}_m$ tal que

$a + b \equiv c \ \textbf{mod}\ m \ (c \in \mathbb{Z}_m)$

$a \times b \equiv d \ \textbf{mod}\ m \ (d \in \mathbb{Z}_m)$

Exemplos:

Se $m = 9$ então $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$6 + 8 = 14 \equiv 5$ **mod** 9

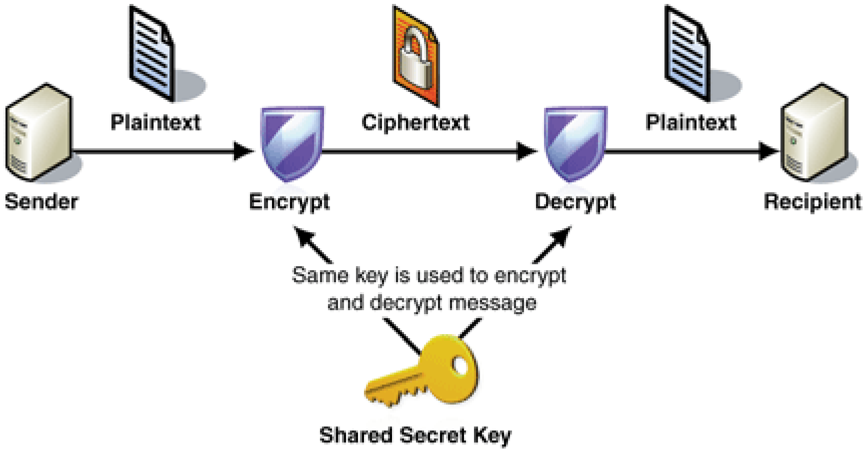
$6 \times 8 = 48 \equiv 3$ **mod** 9

Sumário

Distribuição de Chaves

A distribuição de chaves pode parecer uma questão banal, mas tornou-se um problema crucial: se governos com grandes quantias de recursos estavam com dificuldades para distribuir de forma segura chaves para comunicação, então como empresas civis poderiam esperar obter, um sistema confiável de entrega de chaves sem ir à falência?

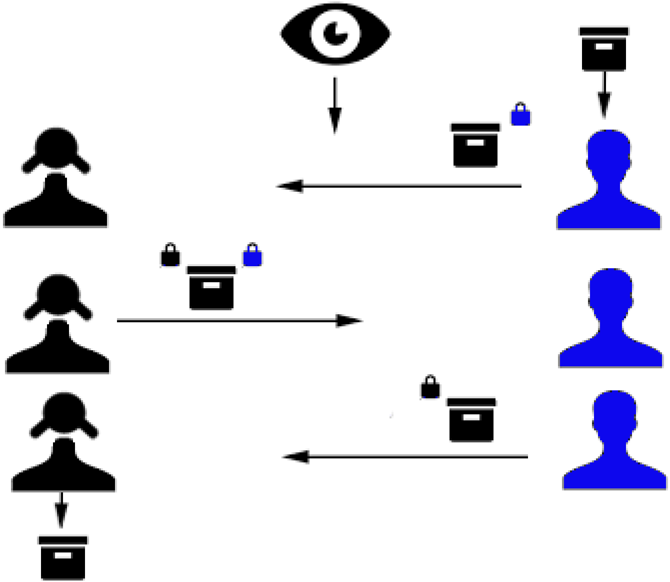
Distribuição de Chaves



Distribuição de Chaves

Cenário: imagine que Alice e Bob vivam em um país onde o serviço de correios é completamente corrupto e os empregados dos correios costumam ler qualquer correspondência desprotegida. Como Alice poderia enviar uma mensagem altamente pessoal a Bob em segurança sem que ambos se encontrem pessoalmente?

Distribuição de Chaves

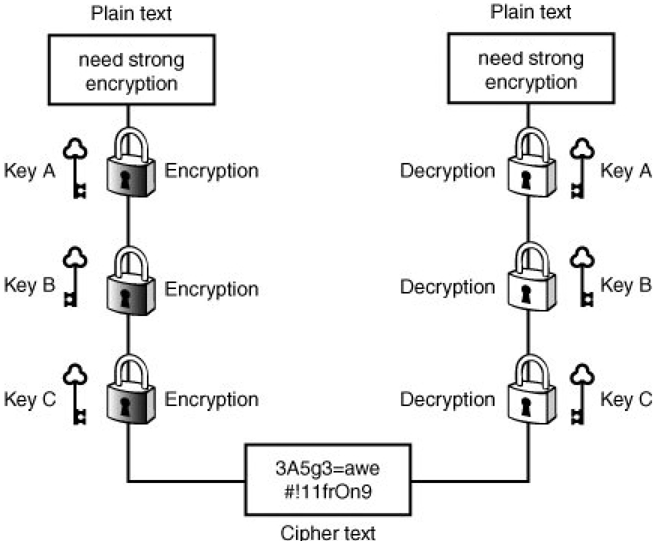


Distribuição de Chaves

As implicações desse cenário são enormes, ele demonstra que é possível trocar uma mensagem secreta em segurança, sem que seja necessário uma troca de chaves.

Problema: ordem pela qual as cifragens e decifragens são feitas: Alice cifra $\rightarrow$ Bob cifra $\rightarrow$ Alice decifra $\rightarrow$ Bob decifra. Note que Alice começou o processo mas Bob que finalizou!

A **ordem** não é importante para cadeados mas para cifras como DES e AES sim (regra do último dentro, primeiro fora).



Distribuição de Chaves

Embora o modelo da caixa com dois cadeados não funcione na criptografia, ele inspirou Diffie, Hellman e Merkle a procurarem um método prático de solucionar o problema da distribuição de chaves.

Diffie-Hellman Key Exchange (DHKE)

Problema: Alice e Bob desejam trocar uma chave secreta para utilizar em uma **cifra simétrica** como 3-DES ou AES, mas o único meio disponível para comunicação é um canal inseguro! Toda informação enviada pelo canal é interceptada por um espião Oscar.

A pesquisa de Diffie e Hellman concentrou-se no estudo de **funções matemáticas de mão única**.

Funções de Mão-Única (One-way functions)

Uma função $f()$ é de mão única se:

1) $y = f(x)$ é fácil de computar

2) $x = f^{-1}(y)$ é inviável de computar

Onde fácil de computar significa que existe um algoritmo polinomial para o cálculo.

Distribuição de Chaves

Uma **função de mão única** é fácil de realizar, mas muito difícil de desfazer.

Uma **função de mão única** é fácil de realizar, mas muito difícil de desfazer.

Uma **função de mão única** é fácil de realizar, mas muito difícil de desfazer.

Uma **função de mão única** é fácil de realizar, mas muito difícil de desfazer.

Funções de mão dupla: são funções fáceis de computar e fáceis de reverter.

Por exemplo: a função $\mathbf{y} = 2\mathbf{x}$ é uma função de mão dupla pois se eu disser que $y = 26$, facilmente você deduzirá que $x = 13$.

A função $\mathbf{y} = 3^{\mathbf{x}}$ é de mão dupla?

Distribuição de Chaves

A função $\mathbf{y} = 3^{\mathbf{x}}$ é de mão dupla? Suponha que $y = 729$ qual o valor de x?

Suposição 1) $x = 1 \rightarrow y = 3^1 \rightarrow y = 3$

Distribuição de Chaves

A função $\mathbf{y} = 3^{\mathbf{x}}$ é de mão dupla? Suponha que $y = 729$ qual o valor de x?

Suposição 1) $x = 1 \rightarrow y = 3^1 \rightarrow y = 3$

Suposição 2) $x = 2 \rightarrow y = 3^2 \rightarrow y = 9$

Distribuição de Chaves

A função $\mathbf{y} = 3^{\mathbf{x}}$ é de mão dupla? Suponha que $y = 729$ qual o valor de x?

Suposição 1) $x = 1 \rightarrow y = 3^1 \rightarrow y = 3$
Suposição 2) $x = 2 \rightarrow y = 3^2 \rightarrow y = 9$
Suposição 3) $x = 3 \rightarrow y = 3^3 \rightarrow y = 27$

Distribuição de Chaves

A função $\mathbf{y} = 3^{\mathbf{x}}$ é de mão dupla? Suponha que $y = 729$ qual o valor de x?

Suposição 1) $x = 1 \rightarrow y = 3^1 \rightarrow y = 3$
Suposição 2) $x = 2 \rightarrow y = 3^2 \rightarrow y = 9$
Suposição 3) $x = 3 \rightarrow y = 3^3 \rightarrow y = 27$
Suposição 4) $x = 4 \rightarrow y = 3^4 \rightarrow y = 81$

Distribuição de Chaves

A função $\mathbf{y} = 3^{\mathbf{x}}$ é de mão dupla? Suponha que $y = 729$ qual o valor de x?

Suposição 1) $x = 1 \rightarrow y = 3^1 \rightarrow y = 3$
Suposição 2) $x = 2 \rightarrow y = 3^2 \rightarrow y = 9$
Suposição 3) $x = 3 \rightarrow y = 3^3 \rightarrow y = 27$
Suposição 4) $x = 4 \rightarrow y = 3^4 \rightarrow y = 81$
Suposição 5) $x = 5 \rightarrow y = 3^5 \rightarrow y = 243$

Distribuição de Chaves

A função $\mathbf{y} = 3^{\mathbf{x}}$ é de mão dupla? Suponha que $y = 729$ qual o valor de x?

Suposição 1) $x = 1 \rightarrow y = 3^1 \rightarrow y = 3$
Suposição 2) $x = 2 \rightarrow y = 3^2 \rightarrow y = 9$
Suposição 3) $x = 3 \rightarrow y = 3^3 \rightarrow y = 27$
Suposição 4) $x = 4 \rightarrow y = 3^4 \rightarrow y = 81$
Suposição 5) $x = 5 \rightarrow y = 3^5 \rightarrow y = 243$
Suposição 6) $x = 6 \rightarrow y = 3^6 \rightarrow y = 729$

A **aritmética modular** é um campo da matemática rico em funções de mão única. Motivo: funções calculadas na aritmética modular tendem a se comportar de modo errático, o que as torna candidatas a funções de mão única.

Suponha a função $\mathbf{y} = 3^{\mathbf{x}} \bmod 7$, qual o valor de $\mathbf{x}$ para $\mathbf{y} = \mathbf{1}$?

Distribuição de Chaves

Suponha a função $\mathbf{y} = 3^{\mathbf{x}} \bmod 7$, qual o valor de $\mathbf{x}$ para $\mathbf{y} = 1$?

1) $x = 1 \rightarrow y = 3^1 \bmod 7 \rightarrow y = 3$

Distribuição de Chaves

Suponha a função $\mathbf{y} = 3^{\mathbf{x}} \bmod 7$, qual o valor de $\mathbf{x}$ para $\mathbf{y} = 1$?

1) $x = 1 \rightarrow y = 3^1 \bmod 7 \rightarrow y = 3$
2) $x = 2 \rightarrow y = 3^2 \bmod 7 \rightarrow y = 2$

Distribuição de Chaves

Suponha a função $\mathbf{y} = 3^{\mathbf{x}} \bmod 7$, qual o valor de $\mathbf{x}$ para $\mathbf{y} = 1$?

1) $x = 1 \rightarrow y = 3^1 \bmod 7 \rightarrow y = 3$
2) $x = 2 \rightarrow y = 3^2 \bmod 7 \rightarrow y = 2$
3) $x = 3 \rightarrow y = 3^3 \bmod 7 \rightarrow y = 6$

Distribuição de Chaves

Suponha a função $\mathbf{y} = 3^{\mathbf{x}} \mod 7$, qual o valor de $\mathbf{x}$ para $\mathbf{y} = 1$?

1) $x = 1 \rightarrow y = 3^1 \mod 7 \rightarrow y = 3$
2) $x = 2 \rightarrow y = 3^2 \mod 7 \rightarrow y = 2$
3) $x = 3 \rightarrow y = 3^3 \mod 7 \rightarrow y = 6$
4) $x = 4 \rightarrow y = 3^4 \mod 7 \rightarrow y = 4$

Distribuição de Chaves

Suponha a função $\mathbf{y} = 3^{\mathbf{x}} \bmod 7$, qual o valor de $\mathbf{x}$ para $\mathbf{y} = 1$?

1) $x = 1 \rightarrow y = 3^1 \bmod 7 \rightarrow y = 3$
2) $x = 2 \rightarrow y = 3^2 \bmod 7 \rightarrow y = 2$
3) $x = 3 \rightarrow y = 3^3 \bmod 7 \rightarrow y = 6$
4) $x = 4 \rightarrow y = 3^4 \bmod 7 \rightarrow y = 4$
5) $x = 5 \rightarrow y = 3^5 \bmod 7 \rightarrow y = 5$

Distribuição de Chaves

Suponha a função $\mathbf{y} = 3^{\mathbf{x}} \bmod 7$, qual o valor de $\mathbf{x}$ para $\mathbf{y} = 1$?

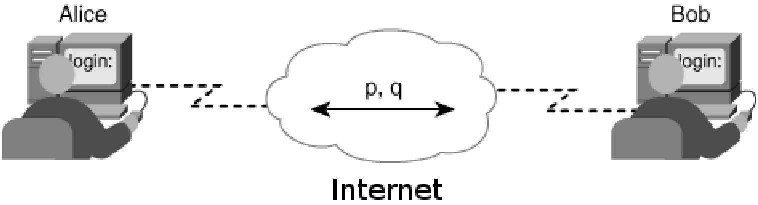
1) $x = 1 \rightarrow y = 3^1 \bmod 7 \rightarrow y = 3$
2) $x = 2 \rightarrow y = 3^2 \bmod 7 \rightarrow y = 2$
3) $x = 3 \rightarrow y = 3^3 \bmod 7 \rightarrow y = 6$
4) $x = 4 \rightarrow y = 3^4 \bmod 7 \rightarrow y = 4$
5) $x = 5 \rightarrow y = 3^5 \bmod 7 \rightarrow y = 5$
6) $x = 6 \rightarrow y = 3^6 \bmod 7 \rightarrow y = 1$

Sumário

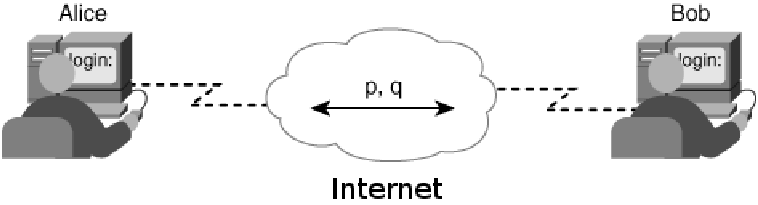
Diffie-Hellman Key Exchange (DHKE)

DHKE - Inicialização

- Escolha um número primo grande p.
- Escolha um inteiro $q \in \{2, 3, \ldots, p-2\}$
- Troque p e q publicamente.



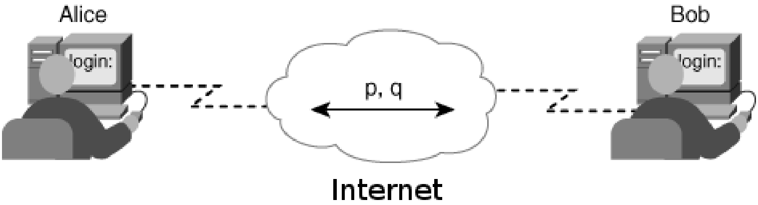
Diffie-Hellman Key Exchange (DHKE)



Alice		**Bob**
Escolhe p e q com Bob	$\leftrightarrow$	Escolhe p e q com Alice
Escolhe chave privada $\mathbf{a}$		Escolhe chave privada $\mathbf{b}$
Calcula $\mathbf{A} = q^{\mathbf{a}} \bmod p$		Calcula $\mathbf{B} = q^{\mathbf{b}} \bmod p$
Envia $\mathbf{A}$ para Bob	$\rightarrow$	Recebe $\mathbf{A}$ de Alice
Recebe $\mathbf{B}$ de Bob	$\leftarrow$	Envia $\mathbf{B}$ para Alice
Chave $= \mathbf{B}^{\mathbf{a}} \bmod p$		Chave $= \mathbf{A}^{\mathbf{b}} \bmod p$

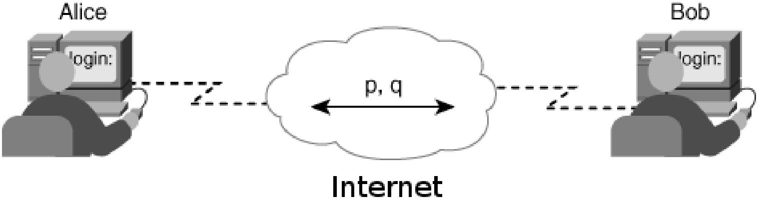
$$\mathbf{a}, \mathbf{b} \in \{2, \ldots, p-2\}$$

Diffie-Hellman Key Exchange (DHKE)



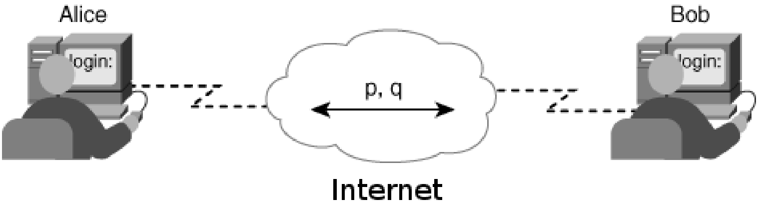
Alice		**Bob**
Escolhe $p = 29$ e $q = 2$	$\rightarrow$	Recebe de Alice p e q
Escolhe chave privada **a**		Escolhe chave privada **b**
Calcula **A** $= q^{\mathbf{a}} \bmod p$		Calcula **B** $= q^{\mathbf{b}} \bmod p$
Envia **A** para Bob	$\rightarrow$	Recebe **A** de Alice
Recebe **B** de Bob	$\leftarrow$	Envia **B** para Alice
Chave $= \mathbf{B}^{\mathbf{a}} \bmod p$		Chave $= \mathbf{A}^{\mathbf{b}} \bmod p$

Diffie-Hellman Key Exchange (DHKE)



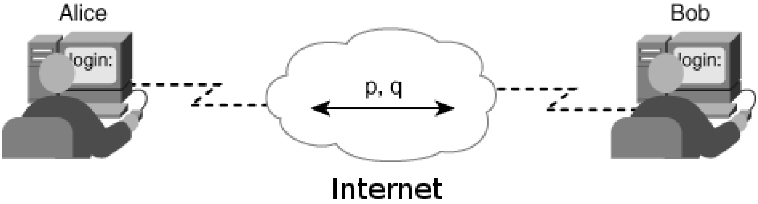
Alice		**Bob**
Escolhe $p = 29$ e $q = 2$	$\rightarrow$	Recebe de Alice p e q
Escolhe chave privada **5**		Escolhe chave privada **12**
Calcula **A** $= q^{\mathbf{a}} \bmod p$		Calcula **B** $= q^{\mathbf{b}} \bmod p$
Envia **A** para Bob	$\rightarrow$	Recebe **A** de Alice
Recebe **B** de Bob	$\leftarrow$	Envia **B** para Alice
Chave $=$ $\mathbf{B}^{\mathbf{a}} \bmod p$		Chave $=$ $\mathbf{A}^{\mathbf{b}} \bmod p$

Diffie-Hellman Key Exchange (DHKE)



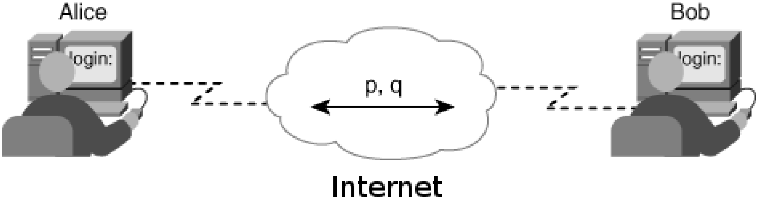
Alice		**Bob**
Escolhe $p = 29$ e $q = 2$	$\rightarrow$	Recebe de Alice p e q
Escolhe chave privada **5**		Escolhe chave privada **12**
Calcula **A** $= 2^{\mathbf{5}}$ mod 29		Calcula **B** $= 2^{\mathbf{12}}$ mod 29
Envia **A** para Bob	$\rightarrow$	Recebe **A** de Alice
Recebe **B** de Bob	$\leftarrow$	Envia **B** para Alice
Chave $=$ **B**$^{\mathbf{a}}$ mod p		Chave $=$ **A**$^{\mathbf{b}}$ mod p

Diffie-Hellman Key Exchange (DHKE)



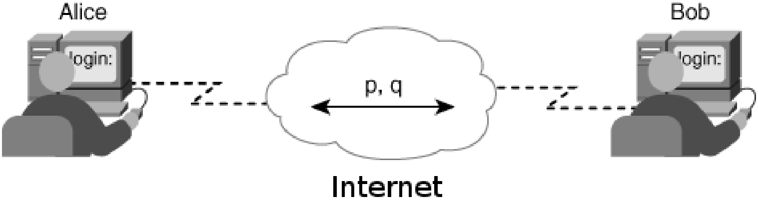
Alice		**Bob**
Escolhe $p = 29$ e $q = 2$	$\rightarrow$	Recebe de Alice p e q
Escolhe chave privada **5**		Escolhe chave privada **12**
Calcula **3** $= 2^{5} \bmod 29$		Calcula **7** $= 2^{12} \bmod 29$
Envia **A** para Bob	$\rightarrow$	Recebe **A** de Alice
Recebe **B** de Bob	$\leftarrow$	Envia **B** para Alice
Chave $=$ $\mathbf{B}^{\mathbf{a}} \bmod p$		Chave $=$ $\mathbf{A}^{\mathbf{b}} \bmod p$

Diffie-Hellman Key Exchange (DHKE)



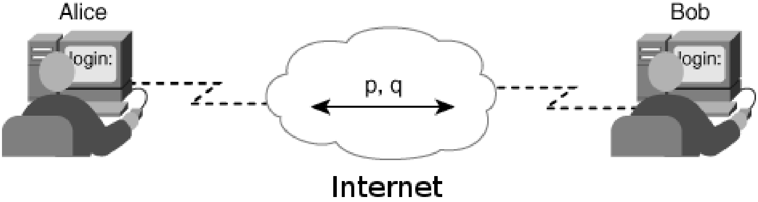
Alice		**Bob**
Escolhe $p = 29$ e $q = 2$	$\rightarrow$	Recebe de Alice p e q
Escolhe chave privada **5**		Escolhe chave privada **12**
Calcula **3** $= 2^{\mathbf{5}} \bmod 29$		Calcula **7** $= 2^{\mathbf{12}} \bmod 29$
Envia **3** para Bob	$\rightarrow$	Recebe **3** de Alice
Recebe **B** de Bob	$\leftarrow$	Envia **B** para Alice
Chave $= \mathbf{B}^{\mathbf{a}} \bmod p$		Chave $= \mathbf{A}^{\mathbf{b}} \bmod p$

Diffie-Hellman Key Exchange (DHKE)



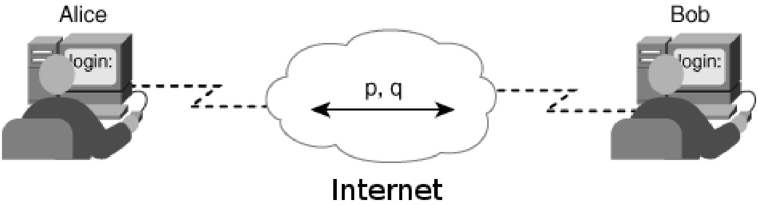
Alice		**Bob**
Escolhe $p = 29$ e $q = 2$	$\rightarrow$	Recebe de Alice p e q
Escolhe chave privada **5**		Escolhe chave privada **12**
Calcula **3** $= 2^{\mathbf{5}} \bmod 29$		Calcula **7** $= 2^{\mathbf{12}} \bmod 29$
Envia **3** para Bob	$\rightarrow$	Recebe **3** de Alice
Recebe **7** de Bob	$\leftarrow$	Envia **7** para Alice
Chave $=$ $\mathbf{B}^{\mathbf{a}} \bmod p$		Chave $=$ $\mathbf{A}^{\mathbf{b}} \bmod p$

Diffie-Hellman Key Exchange (DHKE)



Alice		**Bob**
Escolhe $p = 29$ e $q = 2$	$\rightarrow$	Recebe de Alice p e q
Escolhe chave privada **5**		Escolhe chave privada **12**
Calcula $\mathbf{3} = 2^{\mathbf{5}} \bmod 29$		Calcula $\mathbf{7} = 2^{\mathbf{12}} \bmod 29$
Envia **3** para Bob	$\rightarrow$	Recebe **3** de Alice
Recebe **7** de Bob	$\leftarrow$	Envia **7** para Alice
Chave $= \mathbf{7}^{\mathbf{5}} \bmod 29$		Chave $= \mathbf{3}^{\mathbf{12}} \bmod 29$

Diffie-Hellman Key Exchange (DHKE)



Alice		**Bob**
Escolhe $p = 29$ e $q = 2$	$\rightarrow$	Recebe de Alice p e q
Escolhe chave privada **5**		Escolhe chave privada **12**
Calcula **3** $= 2^{5}$ mod 29		Calcula **7** $= 2^{12}$ mod 29
Envia **3** para Bob	$\rightarrow$	Recebe **3** de Alice
Recebe **7** de Bob	$\leftarrow$	Envia **7** para Alice
Chave = **16**		Chave = **16**

Sumário

Corretude do Algoritmo DHKE

Porque essa troca de chaves de funciona?

Alice

Chave privada **a**

$\mathbf{A} = q^{\mathbf{a}} \bmod p$

Chave $= \mathbf{B}^{\mathbf{a}} \bmod p$

Chave $= q^{\mathbf{b}^{\mathbf{a}}} \bmod p$

Bob

Chave privada **b**

$\mathbf{B} = q^{\mathbf{b}} \bmod p$

Chave $= \mathbf{A}^{\mathbf{b}} \bmod p$

Chave $= q^{\mathbf{a}^{\mathbf{b}}} \bmod p$

A ordem dos expoentes não altera o resultado!

$$(q^a)^b = q^{ab} = (q^b)^a = q^{ba}$$

Sumário

Segurança do Algoritmo DHKE

O algoritmo de Diffie-Hellman é baseado em uma função matemática de mão única conhecida como **problema do logarítimo discreto** (DLP). Considerando a equação

$$\beta = q^{\alpha} \bmod p$$

mesmo conhecendo β, p e q, encontrar α é um problema computacionalmente inviável.

Sumário

Exponenciação Modular

Questão: como calcular $q^{x} \bmod n$?

```
ulong SquareMult (ulong q, ulong x, ulong n){
  ulong r = 1;
  while (x > 0) {
    if ((x % 2) == 1) {
      r = (r * q) % n; /*Multiply (MUL)*/
    }
    x /= 2;
    q = (q * q) % n; /*Square (SQ)*/
  }
  return r;
}
```

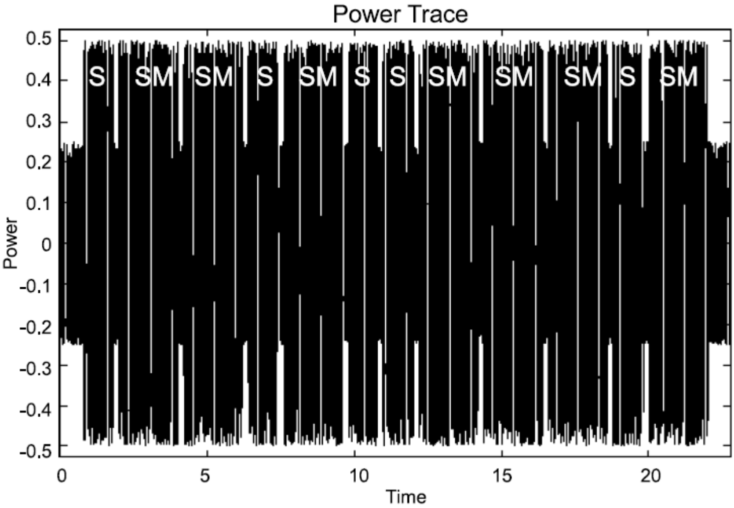
Questão: como calcular $q^x \mod n$?

```
          3^{43}                            101011 (43)
          /
        3^21 * 3^21 * 3  -> SQ and M        (1)
        /
      3^10 * 3^10 * 3  -> SQ and M          (1)
      /
    3^5 * 3^5  -> SQ                        (0)
    /
  3^2 * 3^2 * 3 -> SQ and M                 (1)
  /
 3^1 * 3^1 -> SQ                            (0)
 /
3^0 * 3^0 * 3 -> SQ and M                   (1)
```

Exponenciação Modular

operations: $S\ SM\ SM\ S\ SM\ S\ S\ SM\ SM\ SM\ S\ SM$

private key: 0 1 1 0 1 0 0 1 1 1 0 1



Sumário

Considerações finais

- O protocolo de Diffie-Hellman é para troca de chaves. Não é utilizado para criptografia de dados. Para cifrar dados existe uma extensão do algoritmo de Diffie-Hellman conhecida como **esquema de Elgamal**.

- O tamanho do número primo p para uma segurança de 2^{80} (números de tentativas para um ataque bem sucedido) deve ser de 1024 bits. Paper: Daniel M. Gordon, Discrete Logarithms in GF(p) using the Number Field Sieve, in SIAM Journal on Discrete Mathematics, 6(1):124–138, 1993

Sumário

Demonstração

```
Mostre que a * b mod n = (a mod n * b mod n) mod n
Utilizando a definição, seja
   a mod n = ra -> a = qa * n + ra
   b mod n = rb -> b = qb * n + rb

Logo a * b mod n pode ser rescrito como
((qa*n + ra) * (qb*n + rb)) mod n
(qa*n*qb*n + qa*n*rb + ra*qb*n + ra*rb)mod n

colocando n em evidência temos que
(n * (qa * qb * n + qa * rb + ra * qb) + ra * rb) mod n

Note que podemos eliminar múltiplos de n quando usamos
mod n, logo a expressão acima se reduz a ra * rb mod n.
Assim temos que ra*rb mod n = (a mod n * b mod n) mod n,
mas lembre-se que ra*rb mod n = ra*rb mod n (cqd).
```