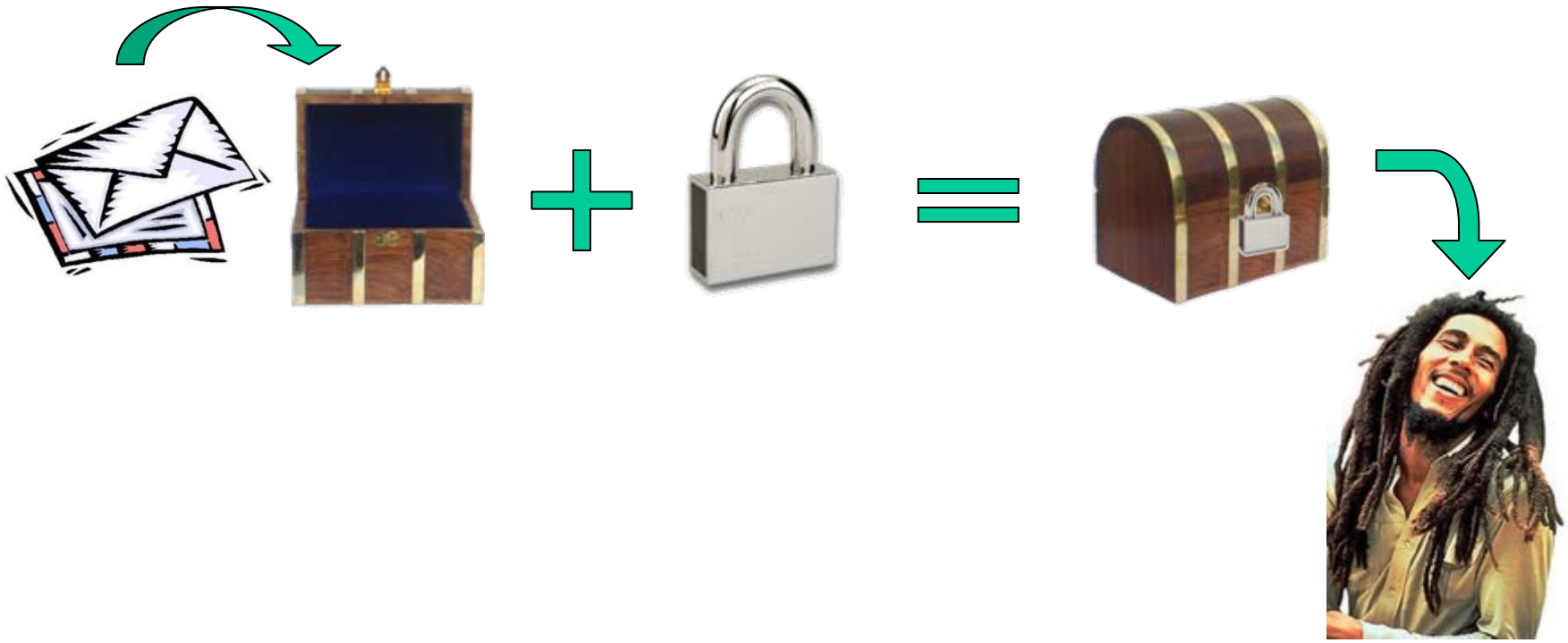
Segurança da Informação

Criptografia Assimétrica
Aritmética Modular

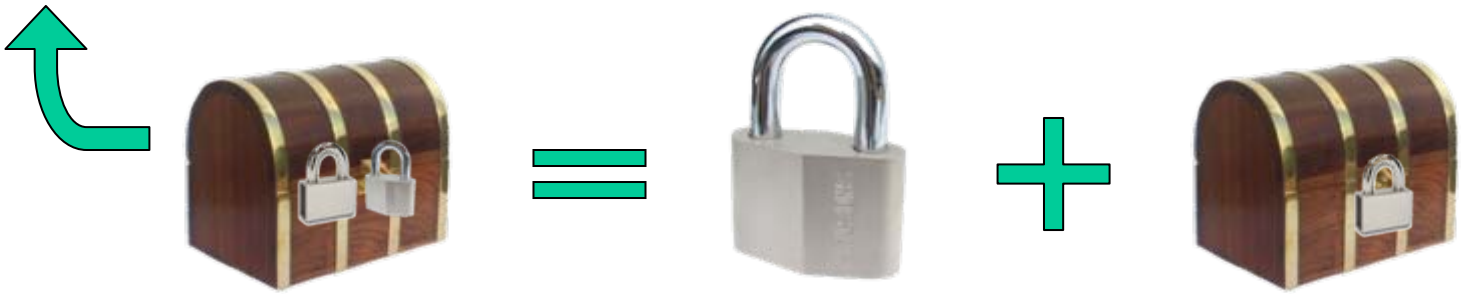
Protocolo Massey-Omura

- Problema: Alice deseja enviar uma carta confidencial para Bob, dispondo apenas de um baú com cadeado.

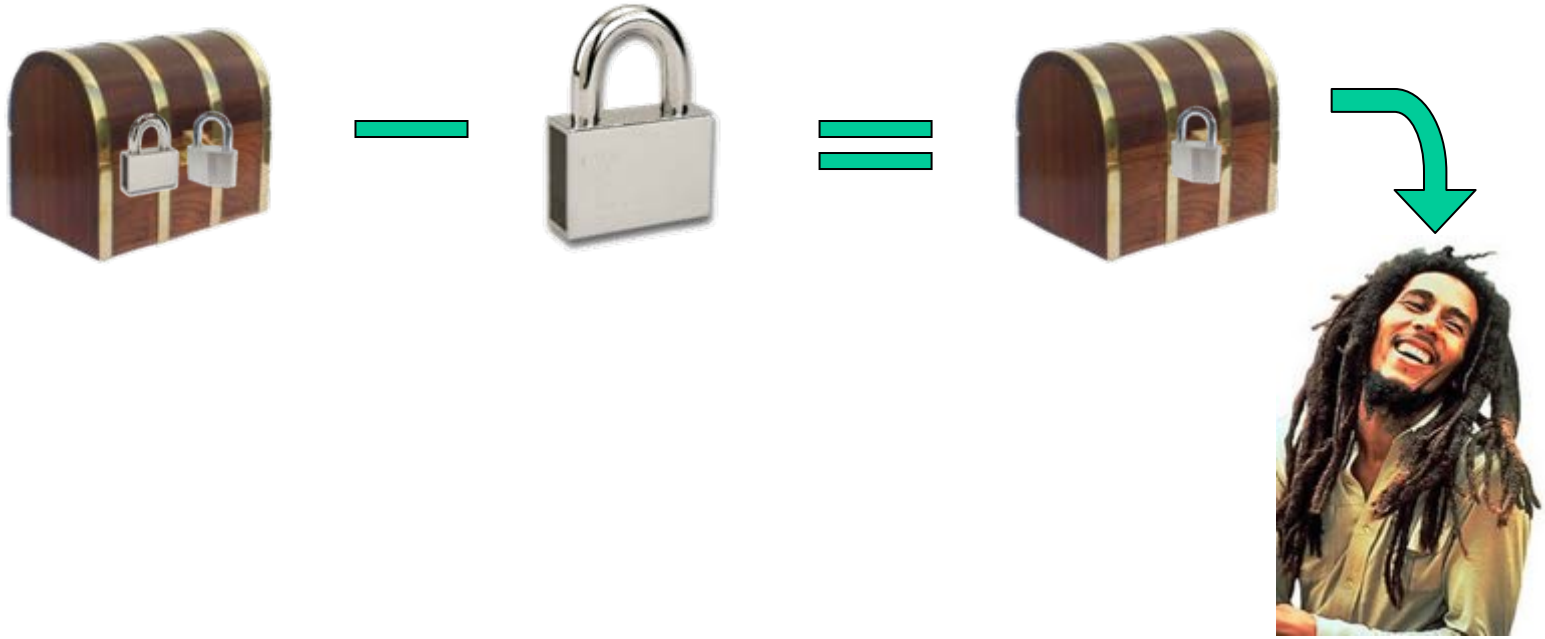
Protocolo Massey-Omura



Protocolo Massey-Omura



Protocolo Massey-Omura



Protocolo Massey-Omura

Protocolo Massey-Omura

- Resumo do protocolo:
  - Alice deposita a carta na caixa, aplica o seu cadeado e envia a caixa para Bob.
  - Bob aplica o seu cadeado e devolve a caixa (com dois cadeados!) para Alice.
  - Alice remove o seu cadeado e envia a caixa de novo para Bob.
  - Bob remove o seu cadeado e recupera a carta.

Protocolo Massey-Omura

- Objetivo geral: transmitir uma mensagem confidencial entre duas entidades que não compartilhem uma informação secreta, dispondo de uma cifra comutativa:

$$E_B(E_A(M)) = E_A(E_B(M)).$$

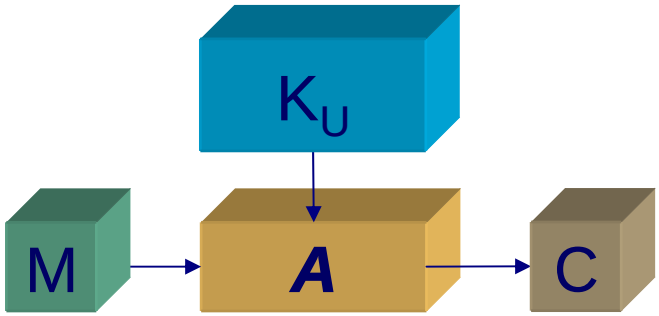
- Importante: cifras de fluxo *não servem*. (Por quê?)
- Defeito geral do protocolo: entidades não são autenticadas.

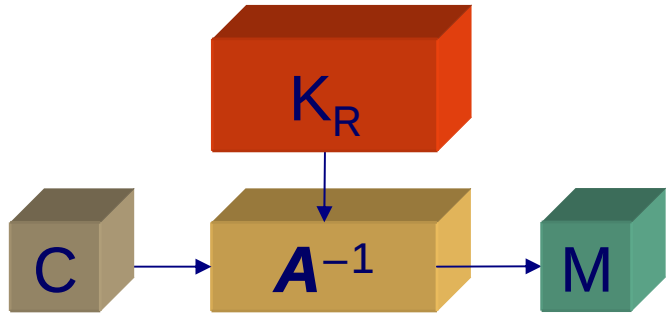
Criptografia Assimétrica

- Duas chaves distintas:
  - Chave privada K_R.
  - Chave pública K_U.
- Inviável calcular a chave privada a partir da chave pública.
- Transformações que dependem de uma das chaves do par somente podem ser invertidas usando a *outra* chave.

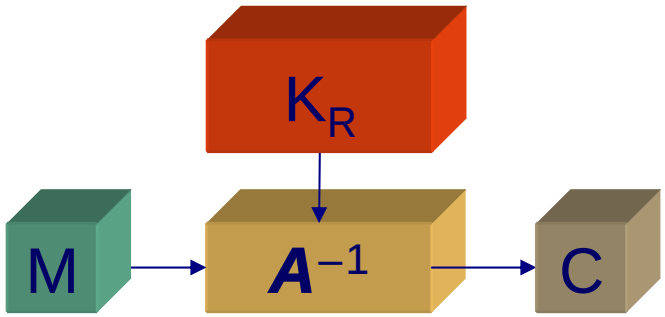
Criptografia Assimétrica

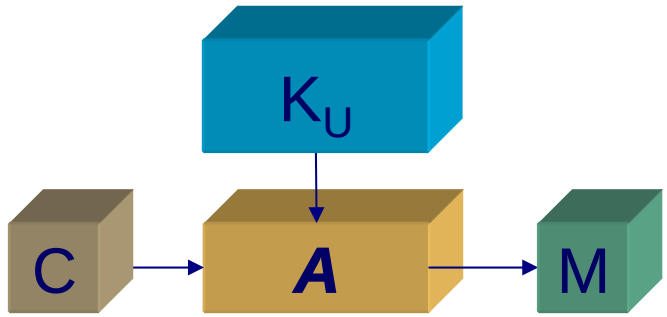
- Cifração:





- Assinatura digital:





Segurança computacional

- Visão clássica: obter informações é *matematicamente impossível*.
- Visão moderna: obter informações é *computacionalmente inviável*.
- Algoritmos assimétricos são baseados em problemas computacionais difíceis de resolver, mas fáceis de verificar (às vezes NP-completos).

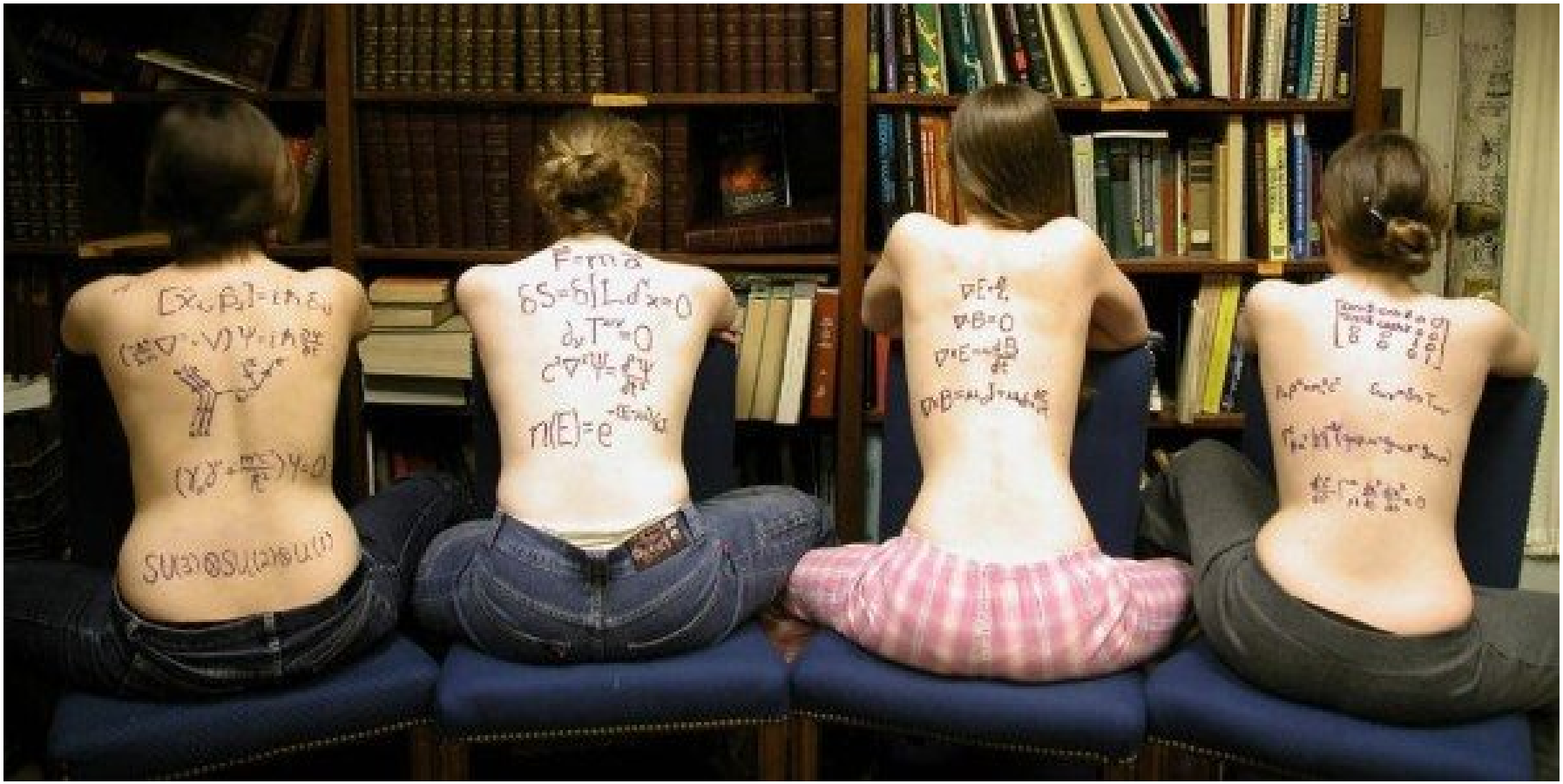
Problemas Matemáticos

- Logaritmo discreto (Diffie-Hellman, DSA) ⇒ algoritmos análogos em curvas elípticas.
- Fatoração inteira (RSA).
- Reticulados (NTRU, LWE).
- Códigos corretores de erro (McEliece, CFS).
- Contra-exemplo: problema da mochila (Hellman-Merkle, Chor-Rivest).

- Teoria dos Números!

Aritmética Modular

Advertência: Equações!



Aritmética modular

- Operações com inteiros são eficientes e livres de erros de arredondamento.
- Por outro lado, em geral não existe inverso multiplicativo.
- Aritmética modular: operações com inteiros, incluindo inversão.

Aritmética modular

- Restrição: valores limitados ao intervalo finito 0, 1, ..., n–1.
- Idéia fundamental: após cada operação aritmética, tomar o resto da divisão por n.
- O resultado está sempre entre 0 e n–1.
- Valores que diferem por múltiplos de n são equivalentes: $a \equiv b \pmod{n}$ sempre que $a–b = kn$ para algum inteiro k.

Exemplo: $n = 11$

- Adição modular:

  $5 + 4 \equiv 9 \pmod{11}$.

  $5 + 8 \equiv 2 \pmod{11} \quad \Rightarrow 13 - 11$

- Subtração modular:

  $5 - 6 \equiv 10 \pmod{11} \quad \Rightarrow -1 + 11$

- Adiciona-se ou subtrai-se livremente qualquer múltiplo de n.

Multiplicação modular

- Mesmo processo das demais operações:

  $3 \cdot 5 \equiv 4 \pmod{11} \Rightarrow 15 - 11$

  $3 \cdot 4 \equiv 1 \pmod{11} \Rightarrow 12 - 11$

- 4 é o inverso de 3 (mod 11) !

- O inverso de a (mod n) é um inteiro x tal que $ax \equiv 1 \pmod{n}$.
- Escreve-se $x \equiv a^{-1} \pmod{n}$:

  $4 = 3^{-1} \pmod{11}$.

Calculando Inversos

- Inverso de 2 (mod 11):

  $2 \cdot x \equiv 1 \pmod{11} \Rightarrow \quad x = 6$

- Inverso de 4 (mod 11)

  $3 \cdot x \equiv 1 \pmod{11} \Rightarrow \quad x = 4$

  $4 \cdot x \equiv 1 \pmod{11} \Rightarrow \quad x = 3$

- Inverso de 11 (mod 11) ?
- Não dividirás por 0...
- ... nem por 11, 22, 33, ...

Inversibilidade Modular

- Se n for primo, todos os inteiros de 1 até $n-1$ possuem inverso (mod n).

- Se n for composto, os números com algum fator em comum com n não possuem inverso (mod n), exceto a unidade.

Exemplo: $n = 10$

- $3 \cdot x \equiv 1 \pmod{10} \Rightarrow \quad x = 7$
- $9 \cdot x \equiv 1 \pmod{10} \Rightarrow \quad x = 9$
- $4 \cdot x \equiv 1 \pmod{10} \Rightarrow \quad x = ?$

- 4 tem um fator comum com 10 (a saber, 2), e por isso não tem inverso (mod 10).

Algoritmo Estendido de Euclides

- Objetivo: calcular $B = A^{-1} \bmod M$ ($\Leftrightarrow \exists\, X: BA + XM = 1$).
- Invariantes: $F = BA + XM$, $G = CA + YM$ para algum X e Y.
- Subtrai-se sucessivamente do maior entre F e G um múltiplo adequado do menor.
- Invariantes preservados com a operação análoga aplicada a B (ou C) e a X (ou Y):
  $F = BA + XM \Rightarrow F - \alpha G = (B - \alpha C)A + (X - \alpha Y)M$, com $G = CA + YM$.

Algoritmo Estendido de Euclides

// invariantes: $F = BA + XM$, $G = CA + YM$
$F \leftarrow A$, $B \leftarrow 1$, $G \leftarrow M$, $C \leftarrow 0$ // $X \leftarrow 0$, $Y \leftarrow 1$
while $F > 1$ {
    if $F < G$ {
        $F \leftrightarrow G$, $B \leftrightarrow C$ // $X \leftrightarrow Y$
    }
    $\alpha \leftarrow \lfloor F/G \rfloor$
    $F \leftarrow F - \alpha G$, $B \leftarrow B - \alpha C$ // $X \leftarrow X - \alpha Y$
}
if $F = 1$ **return** B **else** "não inversível"

Algoritmo Estendido de Euclides

- Exemplo: calcular 4^{-1} mod 11.

passo	*F*	*B*	*G*	*C*	α
init	4	1	11	0	
F < G	11	0	4	1	2
	11–2·4 = 3	0–2·1 = –2	4	1	
F < G	4	1	3	–2	1
	4–1·3 = 1	1–1·(–2) = 3			
stop	1	**3**			

Algoritmo Estendido de Euclides

- Exemplo: calcular $4^{-1} \bmod 10$.

passo	*F*	*B*	*G*	*C*	α
init	4	1	10	0	
F < G	10	0	4	1	2
	10–2·4 = 2	0–2·1 = –2	4	1	
F < G	4	1	2	–2	2
	4–2·2 = 0	1–2· (–2) = 5	2	–2	
stop	**0**		**2**		

gcd(4, 10)

Exponenciação modular

- Multiplicação modular repetida.

  $3^2 \equiv 9 \pmod{11}$.

  $3^{10} \equiv 1 \pmod{11}$.

  $3^{843972} \equiv 9 \pmod{11}$.

- Pequeno Teorema de Fermat:

  $a^{n-1} \equiv 1 \pmod{n}$,

  se n é primo e a não é múltiplo de n.

Exponenciação modular

- Teorema de Euler (restrito):

  $a^x \equiv a^{x \bmod (n-1)} \pmod{n}$,

  se n é primo e a não é múltiplo de n.

- Exponenciações com expoentes grandes:

  $3^{843972} \equiv 3^{843972 \bmod 10} = 3^2 \equiv 9 \pmod{11}$.

- Exercício:

  $14643^{93513} \pmod{11} = ?$

Função tociente (φ) de Euler

- Definição:

  $\varphi(n)$ = número de inteiros positivos menores que n e primos relativos a n.

- Exemplos:

  $\varphi(11) = 10$, pois todos os inteiros de 1 a 10 são primos relativos a 11.

  $\varphi(10) = 4$, pois apenas 1, 3, 7, e 9 são primos relativos a 10.

Função tociente (φ) de Euler

- Se n é primo:

  $\varphi(n) = n - 1$.

  Exemplo: $\varphi(11) = 11 - 1 = 10$.

- Se $n = pq$ onde p e q são primos:

  $\varphi(n) = (p - 1)(q - 1)$.

  Exemplo: $\varphi(10) = (2 - 1)(5 - 1) = 4$.

Exponenciação modular

- Teorema de Euler (geral):

  $a^x \equiv a^{x \bmod \varphi(n)} \pmod{n}$,

  se $\gcd(a, n) = 1$ (a e n primos entre si).

- Exemplo:

  $3^{843972} \equiv 3^{843972 \bmod 4} \pmod{10} = 3^0 = 1$.

- Euler não ajuda a calcular exponenciais modulares quando o módulo é grande.

Algoritmo da Exponenciação

- Objetivo: calcular $a^x \bmod n$.
- Estratégia: aproveitar a representação do expoente numa base b.
- Escrito na base b, o expoente é:
  - $x = x_m\, b^m + x_{m-1}\, b^{m-1} + \ldots + x_1\, b + x_0$,

  onde os x_i são dígitos na base b.
- Exemplo na base $b = 10$:
  - $x = 8\times10^5 + 4\times10^4 + 3\times10^3 + 9\times10^2 + 7\times10 + 2$.

Algoritmo da Exponenciação

- A exponencial é:
  - $a^x = a^{x_m b^m + x_{m-1} b^{m-1} + \ldots + x_1 b + x_0}$

    $= a^{x_m b^m} \cdot a^{x_{m-1} b^{m-1}} \cdot \ldots \cdot a^{x_1 b} \cdot a^{x_0}$
- Exemplo:
  - $3^{843972} = 3^{8\times10^5} \cdot 3^{4\times10^4} \cdot 3^{3\times10^3} \cdot 3^{9\times10^2} \cdot 3^{7\times10} \cdot 3^2$
- Idéia principal:
  - calcular os fatores $a^{x_i b^i}$ e multiplicá-los.
- Observação:
  - $a^{x_i b^i} = (a^{x_i})^{b^i} = (\ldots((a^{x_i})^b)^b\ldots)^b$.

Algoritmo da Exponenciação

- Calcular a^d para cada dígito d da base b.
- Varrer o expoente da esquerda para a direita.
- Manter o produto dos fatores calculados.
- Acumular cada novo fator: elevar o produto parcial à potência b e multiplicar por a^{x_i}.

Algoritmo da Exponenciação

- Exemplo:
  - 3^{843972}

  $= 3^{8\times10^5} \cdot 3^{4\times10^4} \cdot 3^{3\times10^3} \cdot 3^{9\times10^2} \cdot 3^{7\times10} \cdot 3^2$

  $= ((((3^8)^{10} \cdot 3^4)^{10} \cdot 3^3)^{10} \cdot 3^9)^{10} \cdot 3^7)^{10} \cdot 3^2$
- Independe do módulo (basta reduzir mod *n* em cada passo).
- Especialmente simples em base 2:
  - Dígitos 0 e 1: não é necessário calcular a^d.
  - Cálculo de quadrados.

Algoritmo da Exponenciação

// $x = (x_m\ x_{m-1} \ldots x_1\ x_0)_2$, $x_m = 1$.
$v \leftarrow a$
for i = $m-1, \ldots, 0$ {
    $v \leftarrow v^2 \pmod{n}$
    if $x_i = 1$ {
        $v \leftarrow v \cdot a \pmod{n}$
    }
}
return v // $v = a^x \bmod n$

Inversão com Exponenciação

- Teorema de Euler:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

- Dividindo os dois lados por a:

$$a^{\varphi(n)-1} \equiv a^{-1} \pmod{n}$$

- Eficiente quando $\varphi(n)-1$ tiver uma forma simples (poucos bits iguais a 1).

Teorema Chinês do Resto (TCR)

- Conhecendo:

  $q^{-1} \bmod p = u$,

  $a \bmod p = \alpha$,

  $a \bmod q = \beta$,

  é "fácil" calcular $a \bmod pq$:

  $$a \bmod pq = (((\alpha - \beta) \cdot u) \bmod p) \cdot q + \beta$$

- Cálculo de $a^x \bmod pq$: calcular u, $a^x \bmod p$, $a^x \bmod q$, e combinar os resultados.