Criptografia com Maple

LNCC - Verão/2005

Fábio Borges & Renato Portugal

Simétrica versus Assimétrica

- Simétrica

Simétrica versus Assimétrica

- Simétrica
  - $E_k(M) = C$

Simétrica versus Assimétrica

- Simétrica
  - $E_k(M) = C$
  - $D_k(C) = M$

Simétrica versus Assimétrica

- Simétrica
  - $E_k(M) = C$
  - $D_k(C) = M$
  - $D_k(E_k(M)) = M$

Simétrica versus Assimétrica

- Simétrica
  - $E_k(M) = C$
  - $D_k(C) = M$
  - $D_k(E_k(M)) = M$
  - $D_r(E_k(M)) = S$

Simétrica versus Assimétrica

- Simétrica
  - $E_k(M) = C$
  - $D_k(C) = M$
  - $D_k(E_k(M)) = M$
  - $D_r(E_k(M)) = S$
- Assimétrica

Simétrica versus Assimétrica

- Simétrica
  - $E_k(M) = C$
  - $D_k(C) = M$
  - $D_k(E_k(M)) = M$
  - $D_r(E_k(M)) = S$
- Assimétrica
  - $E_a(M) = C$

Simétrica versus Assimétrica

- Simétrica
  - $E_k(M) = C$
  - $D_k(C) = M$
  - $D_k(E_k(M)) = M$
  - $D_r(E_k(M)) = S$
- Assimétrica
  - $E_a(M) = C$
  - $D_b(C) = M$

Simétrica versus Assimétrica

- Simétrica
  - $E_k(M) = C$
  - $D_k(C) = M$
  - $D_k(E_k(M)) = M$
  - $D_r(E_k(M)) = S$
- Assimétrica
  - $E_a(M) = C$
  - $D_b(C) = M$
  - $D_a(E_b(M)) = M$

Simétrica versus Assimétrica

- Simétrica
  - $E_k(M) = C$
  - $D_k(C) = M$
  - $D_k(E_k(M)) = M$
  - $D_r(E_k(M)) = S$
- Assimétrica
  - $E_a(M) = C$
  - $D_b(C) = M$
  - $D_a(E_b(M)) = M$
  - $D_r(E_a(M)) = S$

Simétrica $\times$ Assimétrica

- Quantas chaves são necessárias?

Simétrica $\times$ Assimétrica

- Quantas chaves são necessárias?
  - Simétrica $\longrightarrow \frac{n(n-1)}{2}$

Simétrica $\times$ Assimétrica

- Quantas chaves são necessárias?
  - Simétrica $\longrightarrow \frac{n(n-1)}{2}$
  - Assimétrica $\longrightarrow 2n$

Simétrica $\times$ Assimétrica

- Quantas chaves são necessárias?
  - Simétrica $\longrightarrow \frac{n(n-1)}{2}$
  - Assimétrica $\longrightarrow 2n$
- Criptografia Simétrica

Simétrica $\times$ Assimétrica

- Quantas chaves são necessárias?
  - Simétrica $\longrightarrow \frac{n(n-1)}{2}$
  - Assimétrica $\longrightarrow 2n$
- Criptografia Simétrica
  - Como distribuir e armazenar as chaves?

Simétrica $\times$ Assimétrica

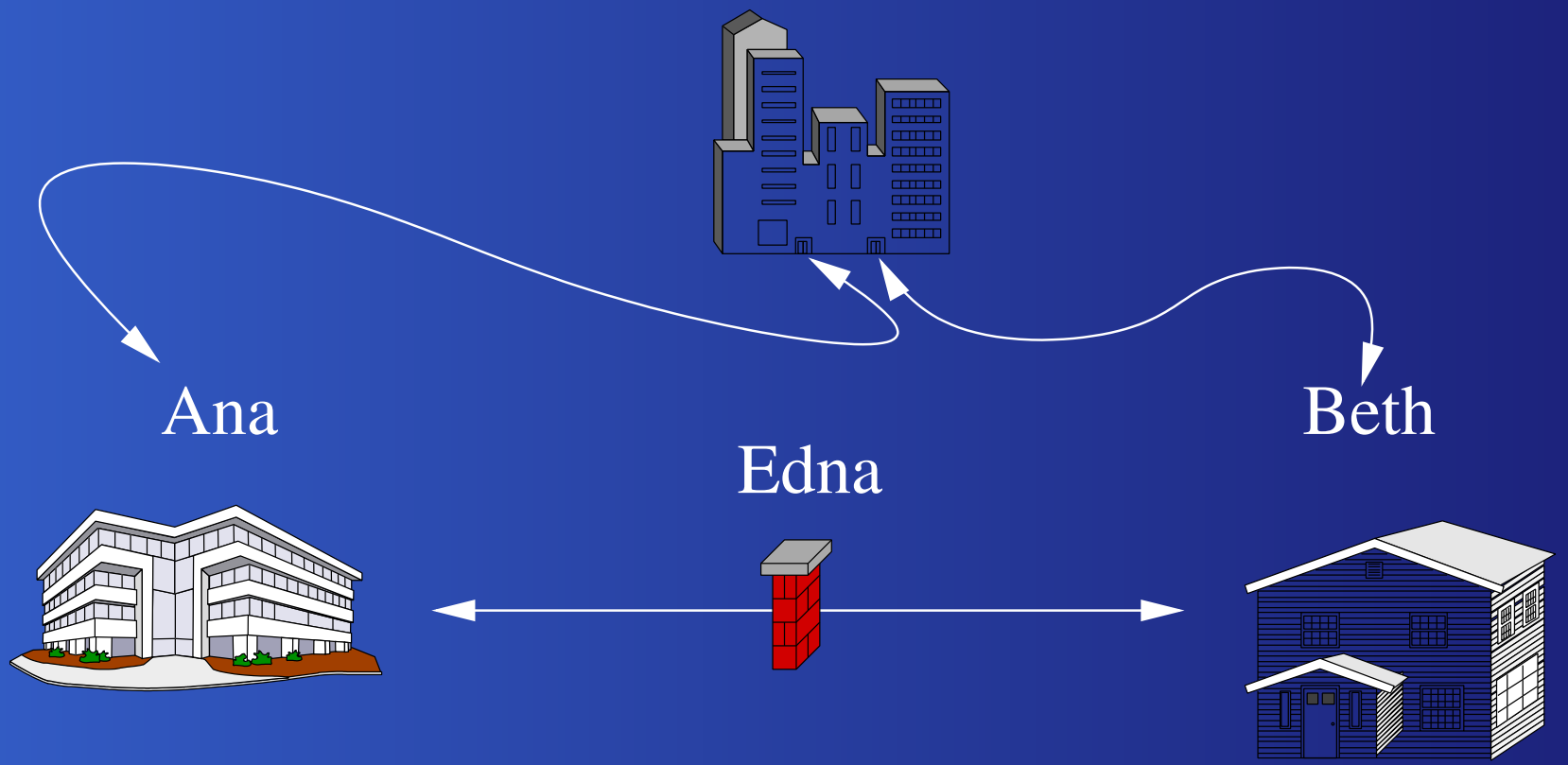
- Quantas chaves são necessárias?
  - Simétrica $\longrightarrow \frac{n(n-1)}{2}$
  - Assimétrica $\longrightarrow 2n$
- Criptografia Simétrica
  - Como distribuir e armazenar as chaves?
- Criptografia Assimétrica

Simétrica $\times$ Assimétrica

- Quantas chaves são necessárias?
  - Simétrica $\longrightarrow \frac{n(n-1)}{2}$
  - Assimétrica $\longrightarrow 2n$
- Criptografia Simétrica
  - Como distribuir e armazenar as chaves?
- Criptografia Assimétrica
  - Como garantir com quem se está comunicando?

Simétrica

Assimétrica



Definição φ de Euler

Seja $m \in \mathbb{N}$ e seja $E(m) = \{x \in \mathbb{N} : x \leqslant m$ e $(x, m) = 1\}$. Usando $\#E$ para denotar o número de elementos. Definimos:

$$\varphi : \mathbb{N} \to \mathbb{N}$$

$$\varphi(m) = \#E(m)$$

Exemplo:

$\varphi(1) = 1,\ \varphi(2) = 1,\ \varphi(3) = 2, \ldots,\ \varphi(27) = 18$

$$\varphi(p) = p - 1$$

Dúvida $\varphi(nm) = \varphi(n)\varphi(m)$?

- $\varphi(3) = 2$

Dúvida $\varphi(nm) = \varphi(n)\varphi(m)$?

- $\varphi(3) = 2$
- $\varphi(4) = 2$

Dúvida $\varphi(nm) = \varphi(n)\varphi(m)$?

- $\varphi(3) = 2$
- $\varphi(4) = 2$
- $\varphi(12) = 4$

Dúvida $\varphi(nm) = \varphi(n)\varphi(m)$?

- $\varphi(3) = 2$
- $\varphi(4) = 2$
- $\varphi(12) = 4$
- $\varphi(9) = 6$

Dúvida $\varphi(nm) = \varphi(n)\varphi(m)$?

- $\varphi(3) = 2$
- $\varphi(4) = 2$
- $\varphi(12) = 4$
- $\varphi(9) = 6$
- $\varphi(3) = 2$

Dúvida $\varphi(nm) = \varphi(n)\varphi(m)$?

- $\varphi(3) = 2$
- $\varphi(4) = 2$
- $\varphi(12) = 4$
- $\varphi(9) = 6$
- $\varphi(3) = 2$
- $\varphi(27) = 18$

RSA - Introdução

$$\varphi = \varphi(pq) = (p-1)(q-1)$$

$$(a, \varphi) = 1$$

$$ab \equiv 1 \mod \varphi$$

$$x^{ab} \equiv x \mod pq \quad \forall x \in \mathbb{Z}$$

RSA - Iniciando

- Ana quer enviar uma mensagem para Beth

RSA - Iniciando

- Ana quer enviar uma mensagem para Beth
- Beth escolhe $p = 71$ e $q = 97$ calcula $pq = 6887$ depois escolhe $a = 27$ e calcula $(27, \varphi) = 3$

RSA - Iniciando

- Ana quer enviar uma mensagem para Beth
- Beth escolhe $p = 71$ e $q = 97$ calcula $pq = 6887$ depois escolhe $a = 27$ e calcula $(27, \varphi) = 3$
- Beth tenta $a = 151$ calcula $(151, \varphi) = 1$, depois calcula $b = 6631$

RSA - Iniciando

- Ana quer enviar uma mensagem para Beth
- Beth escolhe $p = 71$ e $q = 97$ calcula $pq = 6887$ depois escolhe $a = 27$ e calcula $(27, \varphi) = 3$
- Beth tenta $a = 151$ calcula $(151, \varphi) = 1$, depois calcula $b = 6631$
- Esconde a e envia b e pq para Ana criptografar

RSA - Criptografando

- Com $b = 6631$ e $pq = 6887$ Ana calcula:

RSA - Criptografando

- Com $b = 6631$ e $pq = 6887$ Ana calcula:
  - $P_1 = 1214 \leftrightarrow$ "LN"

RSA - Criptografando

- Com $b = 6631$ e $pq = 6887$ Ana calcula:
  - $P_1 = 1214 \leftrightarrow$ "LN"
  - $P_2 = 0303 \leftrightarrow$ "CC"

RSA - Criptografando

- Com $b = 6631$ e $pq = 6887$ Ana calcula:
  - $P_1 = 1214 \leftrightarrow$ "LN"
  - $P_2 = 0303 \leftrightarrow$ "CC"
  - $C_1 = P_1^b \mod pq = 6726$

RSA - Criptografando

- Com $b = 6631$ e $pq = 6887$ Ana calcula:
  - $P_1 = 1214 \leftrightarrow$ "LN"
  - $P_2 = 0303 \leftrightarrow$ "CC"
  - $C_1 = P_1^b \mod pq = 6726$
  - $C_2 = P_2^b \mod pq = 3306$

RSA - Criptografando

- Com $b = 6631$ e $pq = 6887$ Ana calcula:
  - $P_1 = 1214 \leftrightarrow$ "LN"
  - $P_2 = 0303 \leftrightarrow$ "CC"
  - $C_1 = P_1^b \mod pq = 6726$
  - $C_2 = P_2^b \mod pq = 3306$
  - $f : [1214, 303] \mapsto [6726, 3306]$

RSA - Decifrando

- Só Beth conhece a = 151

RSA - Decifrando

- Só Beth conhece a = 151
- $C_1^a \mod pq = 6726^a \mod 6887 = 1214$

RSA - Decifrando

- Só Beth conhece a = 151
- $C_1^a \mod pq = 6726^a \mod 6887 = 1214$
- $C_1^a \mod pq = 3306^a \mod 6887 = 303$

RSA - Decifrando

- Só Beth conhece a = 151
- $C_1^a \mod pq = 6726^a \mod 6887 = 1214$
- $C_1^a \mod pq = 3306^a \mod 6887 = 303$
- $\alpha^{-1} : [12, 14, 3, 3] \mapsto$ "LNCC"

RSA - Cifrando

- Ana quer enviar uma mensagem para Beth

RSA - Cifrando

- Ana quer enviar uma mensagem para Beth
- Ana tem $pq = 5353$ e $b = 4591$

RSA - Cifrando

- Ana quer enviar uma mensagem para Beth
- Ana tem $pq = 5353$ e $b = 4591$
- $P_1 = 1214 \leftrightarrow$ "LN"

RSA - Cifrando

- Ana quer enviar uma mensagem para Beth
- Ana tem $pq = 5353$ e $b = 4591$
- $P_1 = 1214 \leftrightarrow$ "LN"
- $P_2 = 0303 \leftrightarrow$ "CC"

RSA - Cifrando

- Ana quer enviar uma mensagem para Beth
- Ana tem $pq = 5353$ e $b = 4591$
- $P_1 = 1214 \leftrightarrow$ "LN"
- $P_2 = 0303 \leftrightarrow$ "CC"
- $C_1 = P_1^b \mod pq = 3665$

RSA - Cifrando

- Ana quer enviar uma mensagem para Beth
- Ana tem $pq = 5353$ e $b = 4591$
- $P_1 = 1214 \leftrightarrow$ "LN"
- $P_2 = 0303 \leftrightarrow$ "CC"
- $C_1 = P_1^b \mod pq = 3665$
- $C_2 = P_2^b \mod pq = 4545$

RSA - Cifrando

- Ana quer enviar uma mensagem para Beth
- Ana tem $pq = 5353$ e $b = 4591$
- $P_1 = 1214 \leftrightarrow$ "LN"
- $P_2 = 0303 \leftrightarrow$ "CC"
- $C_1 = P_1^b \mod pq = 3665$
- $C_2 = P_2^b \mod pq = 4545$
- $f : [1214, 303] \mapsto [3665, 4545]$

RSA - Cifrando

- Ana quer enviar uma mensagem para Beth
- Ana tem $pq = 5353$ e $b = 4591$
- $P_1 = 1214 \leftrightarrow$ "LN"
- $P_2 = 0303 \leftrightarrow$ "CC"
- $C_1 = P_1^b \mod pq = 3665$
- $C_2 = P_2^b \mod pq = 4545$
- $f : [1214, 303] \mapsto [3665, 4545]$
- Ana envia $[3665, 4545]$

RSA - Decifrando

- Só Beth conhece a = 111

RSA - Decifrando

- Só Beth conhece a = 111
- $C_1^a \mod pq = 3665^a \mod 5353 = 1214$

RSA - Decifrando

- Só Beth conhece a = 111
- $C_1^a \mod pq = 3665^a \mod 5353 = 1214$
- $C_1^a \mod pq = 4545^a \mod 5353 = 0303$

RSA - Decifrando

- Só Beth conhece a = 111
- $C_1^a \mod pq = 3665^a \mod 5353 = 1214$
- $C_1^a \mod pq = 4545^a \mod 5353 = 0303$
- $\alpha^{-1} : [12, 14, 3, 3] \mapsto$ "LNCC"

Teste de Primalidade

- Se n é primo $t^{n-1} \equiv 1 \mod n$ com $(n, t) = 1$

Teste de Primalidade

- Se n é primo $t^{n-1} \equiv 1 \mod n$ com $(n, t) = 1$
- $2^{340} \equiv 1 \mod 341$ é pseudoprimo na base 2

Teste de Primalidade

- Se n é primo $t^{n-1} \equiv 1 \mod n$ com $(n, t) = 1$
- $2^{340} \equiv 1 \mod 341$ é pseudoprimo na base 2
- $3^{340} \equiv 56 \mod 341$

Teste de Primalidade

- Se n é primo $t^{n-1} \equiv 1 \mod n$ com $(n, t) = 1$
- $2^{340} \equiv 1 \mod 341$ é pseudoprimo na base 2
- $3^{340} \equiv 56 \mod 341$
- Existem 245 pseudoprimos na base 2 menores que um milhão

Teste de Primalidade

- Se n é primo $t^{n-1} \equiv 1 \mod n$ com $(n, t) = 1$
- $2^{340} \equiv 1 \mod 341$ é pseudoprimo na base 2
- $3^{340} \equiv 56 \mod 341$
- Existem 245 pseudoprimos na base 2 menores que um milhão
- A maioria não é pseudoprimo em outra base

Teste de Primalidade

- Se n é primo $t^{n-1} \equiv 1 \mod n$ com $(n, t) = 1$
- $2^{340} \equiv 1 \mod 341$ é pseudoprimo na base 2
- $3^{340} \equiv 56 \mod 341$
- Existem 245 pseudoprimos na base 2 menores que um milhão
- A maioria não é pseudoprimo em outra base
- Existe apenas 2163 Carmichael menores que 2.5×10^{10}

Prêmios

Número	Prêmio($US)	Situação	Data
RSA-576	$10,000	Fatorado	3/Dez/2003
RSA-640	$20,000	Não	
RSA-704	$30,000	Não	
RSA-768	$50,000	Não	
RSA-896	$75,000	Não	
RSA-1024	$100,000	Não	
RSA-1536	$150,000	Não	
RSA-2048	$200,000	Não	

http://www.rsasecurity.com/rsalabs/node.asp?id=20

Escolhendo p e q

- Queremos determinar p e q a partir de $n = pq$

Escolhendo p e q

- Queremos determinar p e q a partir de $n = pq$
- Se os primos forem pertos e grandes

Escolhendo p e q

- Queremos determinar p e q a partir de $n = pq$
- Se os primos forem pertos e grandes
- $x = \frac{p+q}{2}$ e $y = \frac{p-q}{2}$

Escolhendo p e q

- Queremos determinar p e q a partir de $n = pq$
- Se os primos forem pertos e grandes
- $x = \frac{p+q}{2}$ e $y = \frac{p-q}{2}$
- $n = pq = x^2 - y^2 = (x + y)(x - y)$

Escolhendo p e q

- Queremos determinar p e q a partir de $n = pq$
- Se os primos forem pertos e grandes
- $x = \frac{p+q}{2}$ e $y = \frac{p-q}{2}$
- $n = pq = x^2 - y^2 = (x + y)(x - y)$
- para achar x e y escolhemos $x = \lceil \sqrt{n} \rceil$ então $x^2 - n$ deve ser um quadrado perfeito y^2 senão procuramos na vizinhança de x

Exemplo de Ataque

- Queremos determinar p e q a partir de $n = 1520273$

Exemplo de Ataque

- Queremos determinar p e q a partir de $n = 1520273$
- para achar x e y escolhemos $x = \lceil \sqrt{1520273} \rceil = 1233$

Exemplo de Ataque

- Queremos determinar p e q a partir de $n = 1520273$
- para achar x e y escolhemos $x = \lceil \sqrt{1520273} \rceil = 1233$
- Então $x^2 - n = 16 = y^2$

Exemplo de Ataque

- Queremos determinar p e q a partir de $n = 1520273$
- para achar x e y escolhemos $x = \lceil \sqrt{1520273} \rceil = 1233$
- Então $x^2 - n = 16 = y^2$
- Portanto $p = 1233 - 4$ e $q = 1233 + 4$

Custo Computacional

bits	Máquina	Memória
430	1	trivial
760	215,000	4 Gb
1020	342,000,000	170 Gb
1620	1.6 x 1015	120 Tb

Máquina Pentium de 500 MHz.
A coluna memória é a requerida em cada máquina.

http://www.rsasecurity.com/rsalabs/node.asp?id=20

Assinatura Digital

- a_A é a chave secreta de Ana

Assinatura Digital

- a_A é a chave secreta de Ana
- a_B é a chave secreta de Beth

Assinatura Digital

- a_A é a chave secreta de Ana
- a_B é a chave secreta de Beth
- b_x e $n_x = pq$ suas respectivas chaves públicas

Assinatura Digital

- a_A é a chave secreta de Ana
- a_B é a chave secreta de Beth
- b_x e $n_x = pq$ suas respectivas chaves públicas
- $E_{a_A}(M)$

Assinatura Digital

- a_A é a chave secreta de Ana
- a_B é a chave secreta de Beth
- b_x e $n_x = pq$ suas respectivas chaves públicas
- $E_{a_A}(M)$
- $E_{b_A}(M)$

Assinatura Digital

- a_A é a chave secreta de Ana
- a_B é a chave secreta de Beth
- b_x e $n_x = pq$ suas respectivas chaves públicas
- $E_{a_A}(M)$
- $E_{b_A}(M)$
- $E_{a_A}(E_{b_B}(M))$ se $n_A > n_B$

Assinatura Digital

- a_A é a chave secreta de Ana
- a_B é a chave secreta de Beth
- b_x e $n_x = pq$ suas respectivas chaves públicas
- $E_{a_A}(M)$
- $E_{b_A}(M)$
- $E_{a_A}(E_{b_B}(M))$ se $n_A > n_B$
- $E_{b_B}(E_{a_A}(M))$ se $n_A < n_B$

Assinatura Digital

- a_A é a chave secreta de Ana
- a_B é a chave secreta de Beth
- b_x e $n_x = pq$ suas respectivas chaves públicas
- $E_{a_A}(M)$
- $E_{b_A}(M)$
- $E_{a_A}(E_{b_B}(M))$ se $n_A > n_B$
- $E_{b_B}(E_{a_A}(M))$ se $n_A < n_B$
- $E_{b_A}(E_{a_B}(M))$ se $n_A > n_B$

Assinatura Digital

- a_A é a chave secreta de Ana
- a_B é a chave secreta de Beth
- b_x e $n_x = pq$ suas respectivas chaves públicas
- $E_{a_A}(M)$
- $E_{b_A}(M)$
- $E_{a_A}(E_{b_B}(M))$ se $n_A > n_B$
- $E_{b_B}(E_{a_A}(M))$ se $n_A < n_B$
- $E_{b_A}(E_{a_B}(M))$ se $n_A > n_B$
- $E_{a_B}(E_{b_A}(M))$ se $n_A < n_B$

Randômico

$$x^s \equiv y \mod z$$

Randômico

- $$x^s \equiv y \mod z$$
- Dado x, s e z temos y é pseudo-randômico

Randômico

- $$x^s \equiv y \mod z$$
- Dado x, s e z temos y é pseudo-randômico
- Dado x, y e z temos s secreto

A Troca de Chaves de Diffie-Hellman

- Ana escolhe p, q e $0 < k \in R$ t.q. $(k, pq) = 1$ e envia k e pq para Beth

A Troca de Chaves de Diffie-Hellman

- Ana escolhe p, q e $0 < k \in R$ t.q. $(k, pq) = 1$ e envia k e pq para Beth
- depois escolhe $0 < r \in R$, calcula k^r e envia o resultado para Beth mantendo r em segredo

A Troca de Chaves de Diffie-Hellman

- Ana escolhe p, q e $0 < k \in R$ t.q. $(k, pq) = 1$ e envia k e pq para Beth
- depois escolhe $0 < r \in R$, calcula k^r e envia o resultado para Beth mantendo r em segredo
- Beth escolhe $0 < s \in R$, calcula k^s e envia o resultado para Ana mantendo s em segredo

A Troca de Chaves de Diffie-Hellman

- Ana escolhe p, q e $0 < k \in R$ t.q. $(k, pq) = 1$ e envia k e pq para Beth
- depois escolhe $0 < r \in R$, calcula k^r e envia o resultado para Beth mantendo r em segredo
- Beth escolhe $0 < s \in R$, calcula k^s e envia o resultado para Ana mantendo s em segredo
- Ambas tem $b_A = (k^r)^s = (k^s)^r$, mas Ana verifica se b_A é um expoente válido (b_A, φ), se não for inicia novamente o processo

Exemplo de Diffie-Hellman

- Ana escolhe $83, 101$ e $k = 256$ calcula $(8383, 256) = 1$ e envia k e pq para Beth

Exemplo de Diffie-Hellman

- Ana escolhe $83, 101$ e $k = 256$ calcula $(8383, 256) = 1$ e envia k e pq para Beth
- depois escolhe $r = 91$, calcula $k^r = 2908$ e envia o resultado para Beth mantendo r em segredo

Exemplo de Diffie-Hellman

- Ana escolhe $83, 101$ e $k = 256$ calcula $(8383, 256) = 1$ e envia k e pq para Beth
- depois escolhe $r = 91$, calcula $k^r = 2908$ e envia o resultado para Beth mantendo r em segredo
- Beth escolhe $s = 4882$, calcula $k^s = 1754$ e envia o resultado para Ana mantendo s em segredo

Exemplo de Diffie-Hellman

- Ana escolhe $83, 101$ e $k = 256$ calcula $(8383, 256) = 1$ e envia k e pq para Beth
- depois escolhe $r = 91$, calcula $k^r = 2908$ e envia o resultado para Beth mantendo r em segredo
- Beth escolhe $s = 4882$, calcula $k^s = 1754$ e envia o resultado para Ana mantendo s em segredo
- Ambas tem $b_A = 2908^s = 1754^r = 6584$, mas Ana verifica que b_A não é um expoente válido $(6584, 8200) = 8$

Cont. Exemplo de Diffie-Hellman

- Suponha que Ana mantém $83, 101$ e $k = 256$

Cont. Exemplo de Diffie-Hellman

- Suponha que Ana mantém $83, 101$ e $k = 256$
- depois escolhe $r = 17$, calcula $k^r = 5835$ e envia o resultado para Beth mantendo r em segredo

Cont. Exemplo de Diffie-Hellman

- Suponha que Ana mantém $83, 101$ e $k = 256$
- depois escolhe $r = 17$, calcula $k^r = 5835$ e envia o resultado para Beth mantendo r em segredo
- Beth escolhe $s = 109$, calcula $k^s = 1438$ e envia o resultado para Ana mantendo s em segredo

Cont. Exemplo de Diffie-Hellman

- Suponha que Ana mantém $83, 101$ e $k = 256$
- depois escolhe $r = 17$, calcula $k^r = 5835$ e envia o resultado para Beth mantendo r em segredo
- Beth escolhe $s = 109$, calcula $k^s = 1438$ e envia o resultado para Ana mantendo s em segredo
- Ambas tem $b_A = 5835^s = 1438^r = 3439$, e Ana verifica que b_A é um expoente válido $(3439, 8200) = 1$.

Problema do Logaritmo Discreto

- Com k, pq, k^r e k^s

Problema do Logaritmo Discreto

- Com k, pq, k^r e k^s
- Poderia calcular s ou r e depois b_A

Intruso e o Logaritmo Discreto

- Com $k = 256$, $pq = 8383$, $k^r = 5835$ e $k^s = 1438$

Intruso e o Logaritmo Discreto

- Com $k = 256$, $pq = 8383$, $k^r = 5835$ e $k^s = 1438$
- o intruso calcula $256^{109} = 1438$

Intruso e o Logaritmo Discreto

- Com $k = 256$, $pq = 8383$, $k^r = 5835$ e $k^s = 1438$
- o intruso calcula $256^{109} = 1438$
- $s = 109$

Intruso e o Logaritmo Discreto

- Com $k = 256$, $pq = 8383$, $k^r = 5835$ e $k^s = 1438$
- o intruso calcula $256^{109} = 1438$
- $s = 109$
- $b_A = (k^r)^s = 5835^{109} = 3439$

Último Slide

- Obrigado.
- Quaisquer sugestões serão bem-vindas.

www.lncc.br/borges

Teorema $\varphi(nm) = \varphi(n)\varphi(m)$

Sejam $m, n \in \mathbb{N}$ tais que $(m, n) = 1$. Então $\varphi(nm) = \varphi(n)\varphi(m)$.
Prova: Sejam $x_1, \ldots, x_{\varphi(n)}$ e $x_1, \ldots, x_{\varphi(m)}$ sistemas de resíduo módulo n e m resp. Mostraremos que o conjunto $\mathcal{B}$ da combinações lineares

$$b_{ij} = x_i m + y_j n$$

forma um sistema resíduo módulo mn.

Precisamos

1. $(b_{ij}, mn) = 1$
2. $b_{ij} \not\equiv b_{kl} \mod mn$ se $i \neq k$ ou $j \neq l$
3. Se $(a, mn) = 1$ então existe $b_{ij} \in \mathcal{B} : a \equiv b_{ij} \mod mn$

1)

$$b_{ij} = x_i m + y_j n$$

Precisamos: item 2

2) Assumindo que

$$mx_i + ny_j \equiv mx_k + ny_l \mod mn$$

então

$$m(x_i - x_k) \equiv n(y_l - y_j) \mod mn$$

Como $m|mn$

$$n(y_l - y_j) \equiv 0 \mod n$$

como

$$y_l \equiv y_j \mod m$$

Implica que $j = l$. Da mesma forma $i = k$

Precisamos: item 3

3) Como $a = xm + yn$ e $(a, mn) = 1$ temos que $(a, m) = (a, n) = 1$, concluímos que $(m, y) = (n, x) = 1$
Portanto existe índices i e j tais que

$$y \equiv y_i \mod m \quad \text{e} \quad x \equiv x_i \mod n$$

$$ny \equiv ny_i \mod nm \quad \text{e} \quad mx \equiv mx_i \mod mn$$

Portanto

$$a = mx + ny \equiv mx_i + ny_j = b_{ij} \mod mn$$

Teorema de Euler

Sejam $a \in \mathbb{Z}$ e $m \in \mathbb{N}$, tais que $(a, m) = 1$. Então

$$a^{\varphi(m)} \equiv 1 \mod m$$

Prova: Seja $\{r_1, \ldots, r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m. Como $(a, m) = 1$ temos $\{ar_1, \ldots, ar_{\varphi(m)}\}$, assim para um dado i existe um j tal que $ar_i \equiv r_j \mod m$

$$ar_1 \ldots, ar_{\varphi(m)} \equiv r_1 \ldots r_{\varphi(m)} \mod m$$

$$a^{\varphi(m)} r_1 \ldots, r_{\varphi(m)} \equiv r_1 \ldots r_{\varphi(m)} \mod m$$

QED

Teorema da Inversa do RSA

Sejam $p, q \in \mathbb{P} : p \neq q$ e $\varphi = \varphi(pq)$. Se $a, b \in \mathbb{Z}$ t.q. $ab \equiv 1 \mod \varphi \Rightarrow x^{ab} \equiv x \mod pq \; \forall \, x \in \mathbb{Z}$
Prova: Se $ab \equiv 1 \mod \varphi$ então $ab = 1 + k\varphi$ com $k \in \mathbb{Z}$, logo

$$x^{ab} = x^{1+k\varphi} = x(x^{k\varphi}) = x(x^{p-1})^{k(q-1)}$$

Se $(x, p) = 1$ então $x^{p-1} \equiv 1 \mod p$. Portanto $x^{ab} \equiv x(1)^{k(q-1)} \equiv x \mod p$. Idem para $x^{ab} \equiv x \mod q$. Portanto $pq|(x^{ab} - x) \Leftrightarrow x^{ab} \equiv x \mod pq$
QED