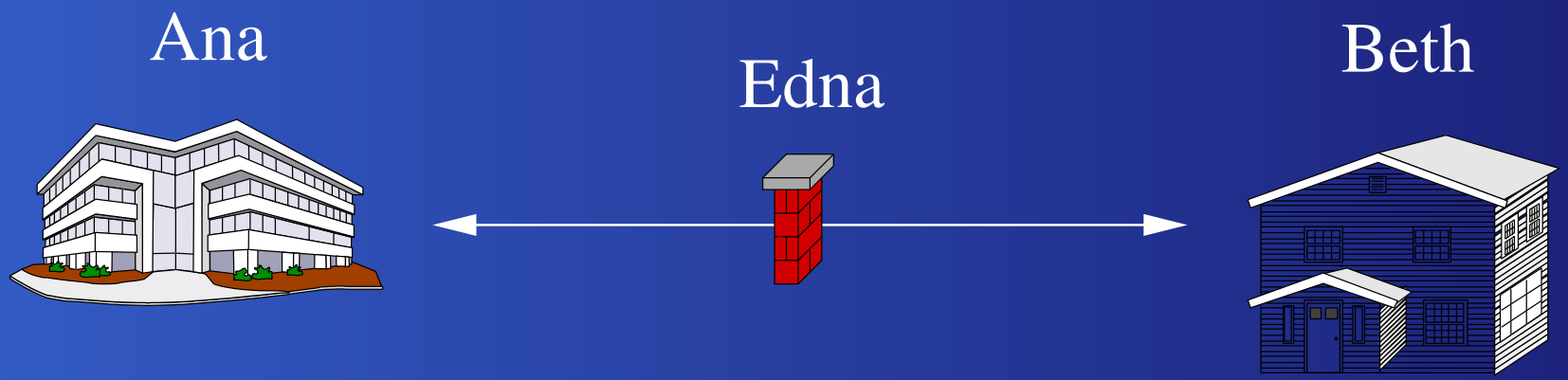
Troca de Chaves

maio/2006

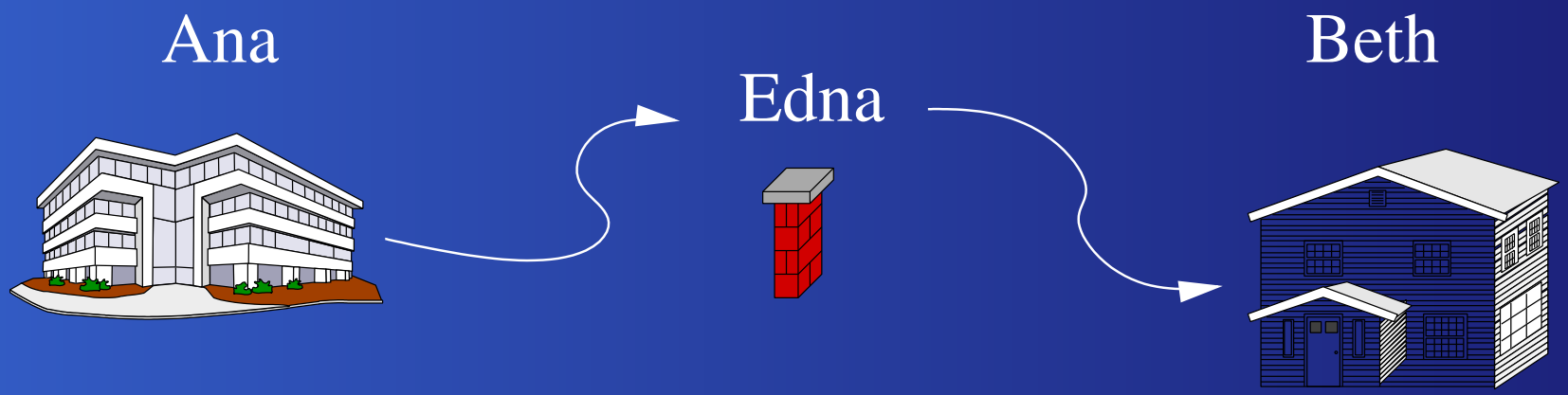
Fábio Borges

Fluxo Normal

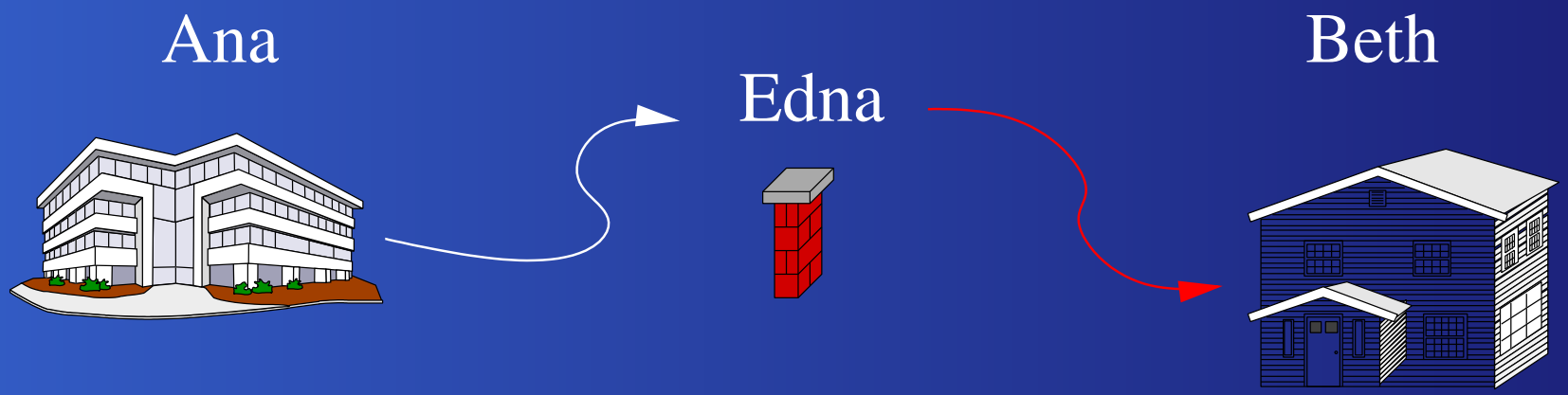


Ameaças eminentes.

Interceptação



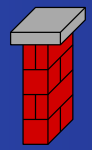
Alteração



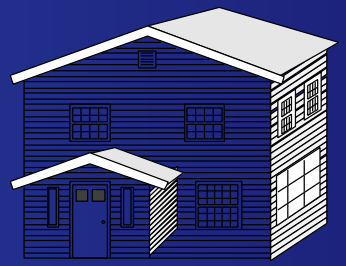
Fabricação

Ana

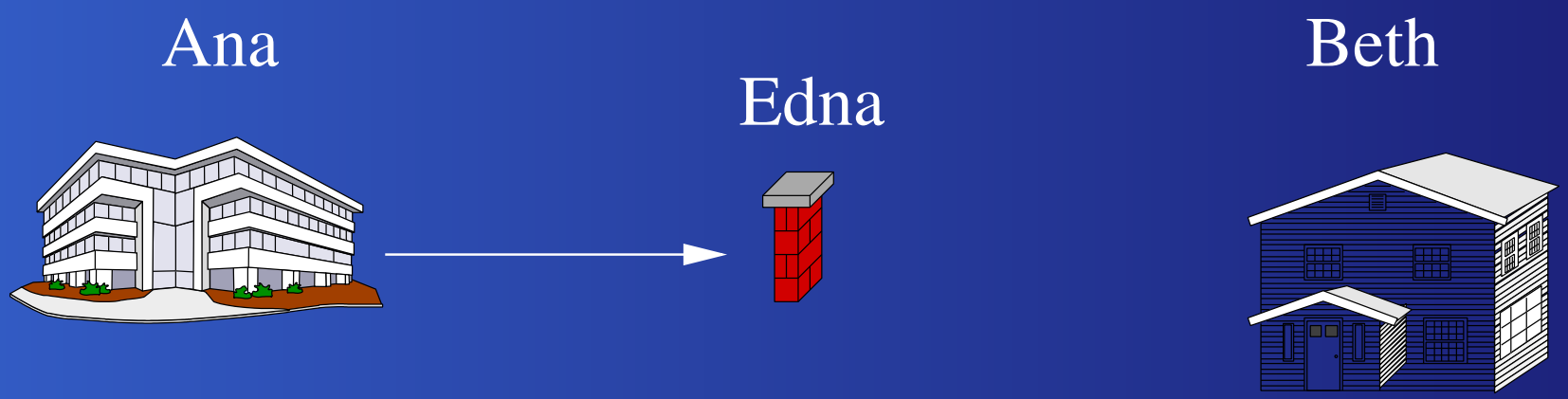
Edna



Beth



Interrupção



Grupo Abeliano

Fechado	Se $a, b \in G$ então $a \oplus b \in G$
Associativa	$a \oplus (b \oplus c) = (a \oplus b) \oplus c$
Identidade	$\exists 0 \in G : a + 0 = a \quad \forall a \in G$
Inversa	$\forall a \in G \quad \exists b \in G : a \oplus b = 0$
Comutatividade	$a \oplus b = b \oplus a \quad a, b \in G$

Contra Exemplo

- Matrizes M com dimensão $n \times n$ e $\det(M) \neq 0$

Contra Exemplo

- Matrizes M com dimensão $n \times n$ e $\det(M) \neq 0$
-

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 8 & 5 \\ 20 & 13 \end{bmatrix}$$

Contra Exemplo

- Matrizes M com dimensão $n \times n$ e $\det(M) \neq 0$
-
$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 8 & 5 \\ 20 & 13 \end{bmatrix}$$
-
$$\begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 13 & 20 \\ 5 & 8 \end{bmatrix}$$

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 × 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

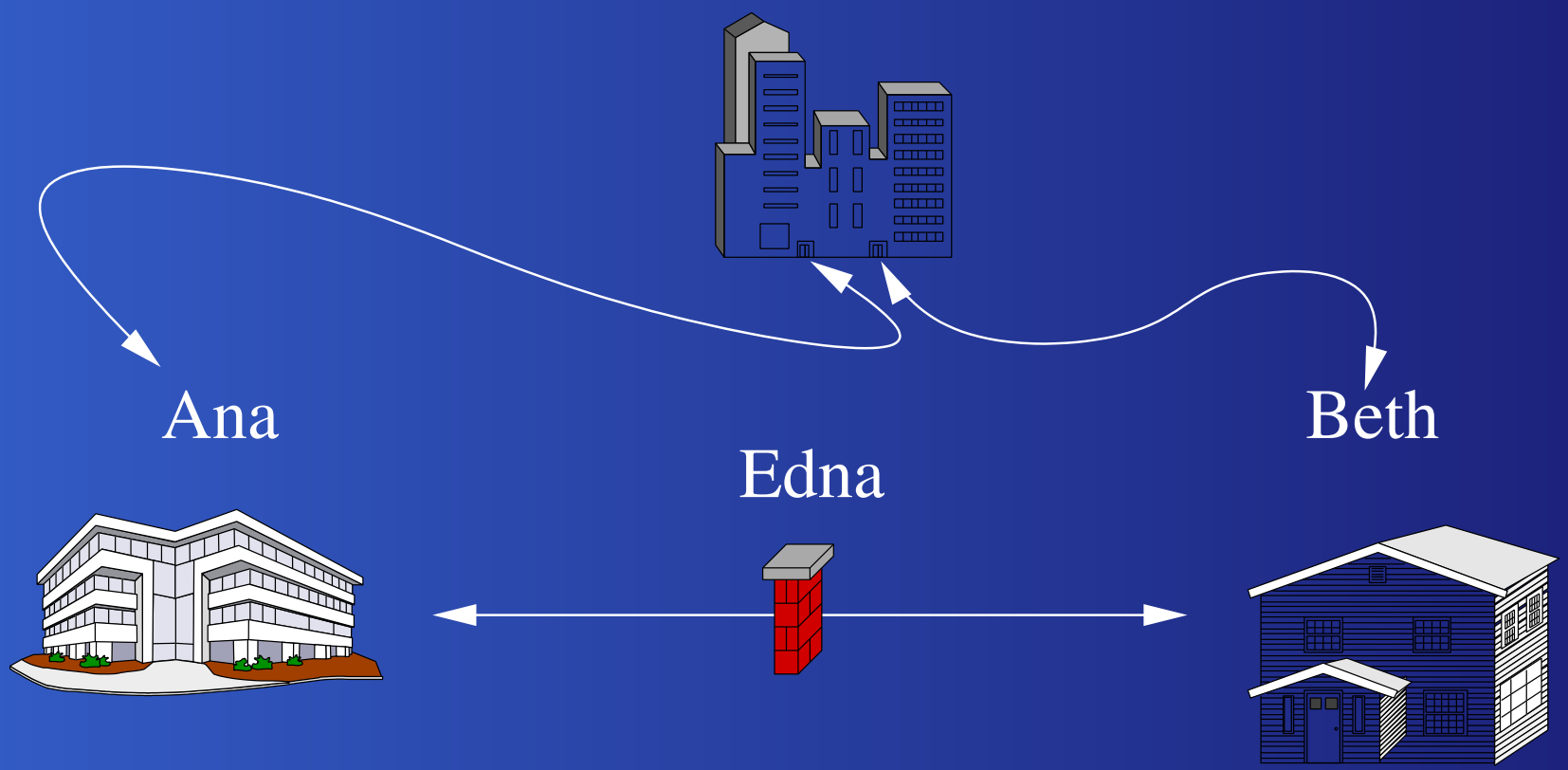
- Quantas chaves são necessárias?
  - Simétrica $\longrightarrow \frac{n(n-1)}{2}$
  - Assimétrica $\longrightarrow 2n$
- Criptografia Simétrica
  - Como distribuir e armazenar as chaves?
- Criptografia Assimétrica

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



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 $256^{109} = 1438$
- $s = 109$
- $b_A = (k^r)^s = 5835^{109} = 3439$

ElGamal (1985)

- Ana quer mandar uma mensagem para Beth

ElGamal (1985)

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $(G, \oplus)$, $a \in G$ e $n \in \mathbb{N}^*$

ElGamal (1985)

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $(G, \oplus)$, $a \in G$ e $n \in \mathbb{N}^*$
- calcula $b = a^n$ e envia a e b

ElGamal (1985)

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $(G, \oplus)$, $a \in G$ e $n \in \mathbb{N}^*$
- calcula $b = a^n$ e envia a e b
- Ana $\alpha : \mathrm{msg} \rightarrow w \in G$ escolhe $k \in \mathbb{N}^*$ e calcula $y = a^k$ e $z = wb^k \in G$ e envia y e z

ElGamal (1985)

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $(G, \oplus)$, $a \in G$ e $n \in \mathbb{N}^*$
- calcula $b = a^n$ e envia a e b
- Ana $\alpha : \mathrm{msg} \rightarrow w \in G$ escolhe $k \in \mathbb{N}^*$ e calcula $y = a^k$ e $z = wb^k \in G$ e envia y e z
- Beth calcula
  $zy^{-n} = wb^k(a^k)^{-n} = w(ba^{-n})^k = w(1)^k = w$

ElGamal (1985)

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $(G, \oplus)$, $a \in G$ e $n \in \mathbb{N}^*$
- calcula $b = a^n$ e envia a e b
- Ana $\alpha : \mathrm{msg} \to w \in G$ escolhe $k \in \mathbb{N}^*$ e calcula $y = a^k$ e $z = wb^k \in G$ e envia y e z
- Beth calcula $zy^{-n} = wb^k(a^k)^{-n} = w(ba^{-n})^k = w(1)^k = w$
- Se $|a| = m$ ou $|G| = m$ então $y^{-n} = y^{m-n}$

Exemplo ElGamal

- Ana quer mandar uma mensagem para Beth

Exemplo ElGamal

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $p = 1000000007$, $a = 419666093$, $n = 110691024$ e calcula $b = a^n \mod p = 215094385$ e envia $p,\ a$ e b

Exemplo ElGamal

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $p = 1000000007$, $a = 419666093$, $n = 110691024$ e calcula $b = a^n \mod p = 215094385$ e envia $p,\ a$ e b
- Ana: $\alpha : \text{msg} \rightarrow w = 12140303$ escolhe $k = 633071297$ e calcula $y = a^k \mod p = 295903670$ e $z = wb^k \mod p = 763646857$

Exemplo ElGamal

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $p = 1000000007$, $a = 419666093$, $n = 110691024$ e calcula $b = a^n \mod p = 215094385$ e envia $p,\ a$ e b
- Ana: $\alpha : \text{msg} \rightarrow w = 12140303$ escolhe $k = 633071297$ e calcula $y = a^k \mod p = 295903670$ e $z = wb^k \mod p = 763646857$
- Beth lê calculando $zy^{-n} \mod p = 12140303$

Exemplo II - ElGamal

- Ana quer mandar uma mensagem para Beth

Exemplo II - ElGamal

- Ana quer mandar uma mensagem para Beth
- Beth escolhe $a = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $n = 5$ calcula

  $b = a^5 = \begin{bmatrix} 25 & 21 \\ 17 & 13 \end{bmatrix}$, sobre $\mathbb{Z}_{27}$ esconde o n

Exemplo II - ElGamal

- Ana faz $w = \begin{bmatrix} 12 & 14 \\ 3 & 3 \end{bmatrix}$, escolhe $k = 3$ e calcula

$$y = a^k = \begin{bmatrix} 37 & 54 \\ 81 & 118 \end{bmatrix} \text{ e } z = wb^k = \begin{bmatrix} 15 & 4 \\ 22 & 7 \end{bmatrix}$$

Exemplo II - ElGamal

- Ana faz $w = \begin{bmatrix} 12 & 14 \\ 3 & 3 \end{bmatrix}$, escolhe $k = 3$ e calcula

$$y = a^k = \begin{bmatrix} 37 & 54 \\ 81 & 118 \end{bmatrix} \text{ e } z = wb^k = \begin{bmatrix} 15 & 4 \\ 22 & 7 \end{bmatrix}$$

- Ana lê calculando $zy^{-n} = \begin{bmatrix} 12 & 14 \\ 3 & 3 \end{bmatrix}$

Último Slide

- Obrigado.
- Quaisquer sugestões serão bem-vindas.

www.lncc.br/borges