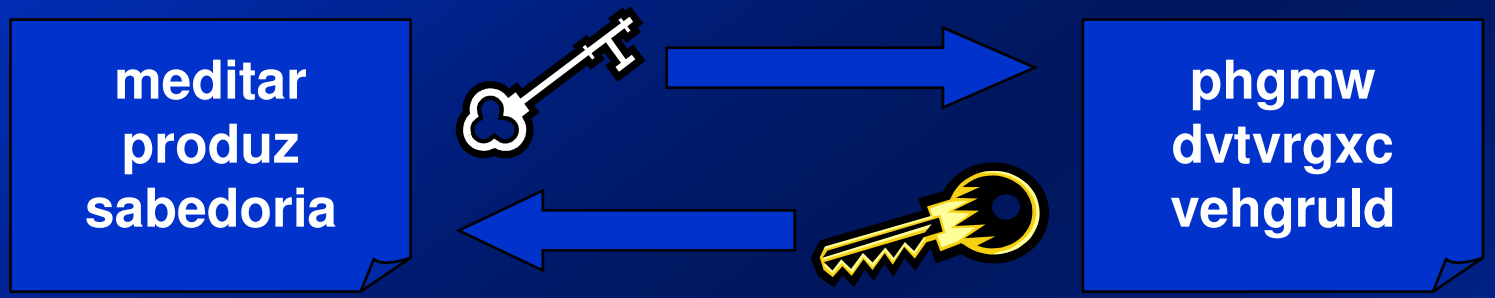
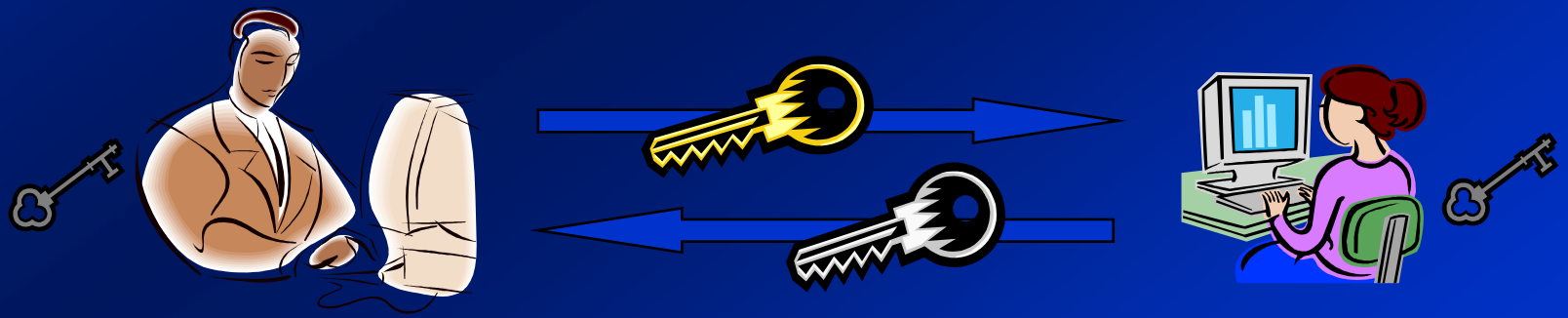
Sistemas criptográficos assimétricos



Segredos (chaves públicas) são trocados



Sistemas criptográficos assimétricos

- Revolucionou a história da criptografia
- Algoritmos baseados em funções matemáticas
- Uso da criptografia assimétrica
  - chave pública e chave privada
- Confidencialidade, autenticação e distribuição de chaves
- Características importantes:
  - impossibilidade computacional de se obter chave privada.
  - possibilidade de uso das duas chaves para criptografia.

Benefícios da Criptografia Assimétrica

- Autenticidade

- Confidencialidade, ou sigilo

Sistemas criptográficos assimétricos

- **Requisitos do Sistema (postulados de Diffie e Hellman)**

- **Fácil para B, gerar o par de chaves (KU_b, KR_b).**
- **Fácil para A, conhecendo a KU_b, gerar texto cifrado $C = E_{KUb} (M)$.**
- **Fácil para B, usando a KU_b, abrir o texto cifrado $M = D_{KUb} (C)$.**
- **Difícil encontrar KR_b, conhecendo KU_b.**
- **Difícil recuperar texto plano, conhecendo KU_b e o texto cifrado.**
- **Função de E / D independente de ordem $M = E_{KUb} \{ D_{KRb} (M) \}$**

Algoritmo RSA (Ron **R**ivest, Adi **S**hamir e Len **A**dleman)

- **Blocos com valores binários menores que n,**
- **Tamanho do bloco é k bits, onde $2^k < n \leq 2^{k+1}$**

Texto cifrado: $C = M^e \bmod n$

Texto Plano: $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

$KU = \{e,n\}$

$KR = \{d,n\}$

Requisitos do Algoritmo

- É possível encontrar **e**, **d**, **n** tal que $M^{ed} = M \bmod n$ para todo $M < n$
- É relativamente fácil calcular M^e e C^d para todos os valores de $M < n$
- É improvável determinar **d** dado **e**, **n**

Algoritmo RSA (Ron **R**ivest, Adi **S**hamir e Len **A**dleman)

Algoritmo Sintetizado

Geração da Chave

Selecione	***p.q***	**p** e **q** primos
Calcular	$n = p \times q$	
Calcular	$\phi(n) = (p-1)(q-1)$	
Selecionar ***e*** inteiro		$\mathbf{gcd}(\phi(n),e) = 1;\ 1 < e < \phi(n)$
Calcular	***d***	$d = e^{-1} \bmod \phi(n)$
Chave Pública		**KU = { *e, n* }**
Chave Privada		**KR = { *d, n* }**

Encriptar

Texto Plano:	$M < n$
Texto Cifrado:	$C = M^e \pmod n$

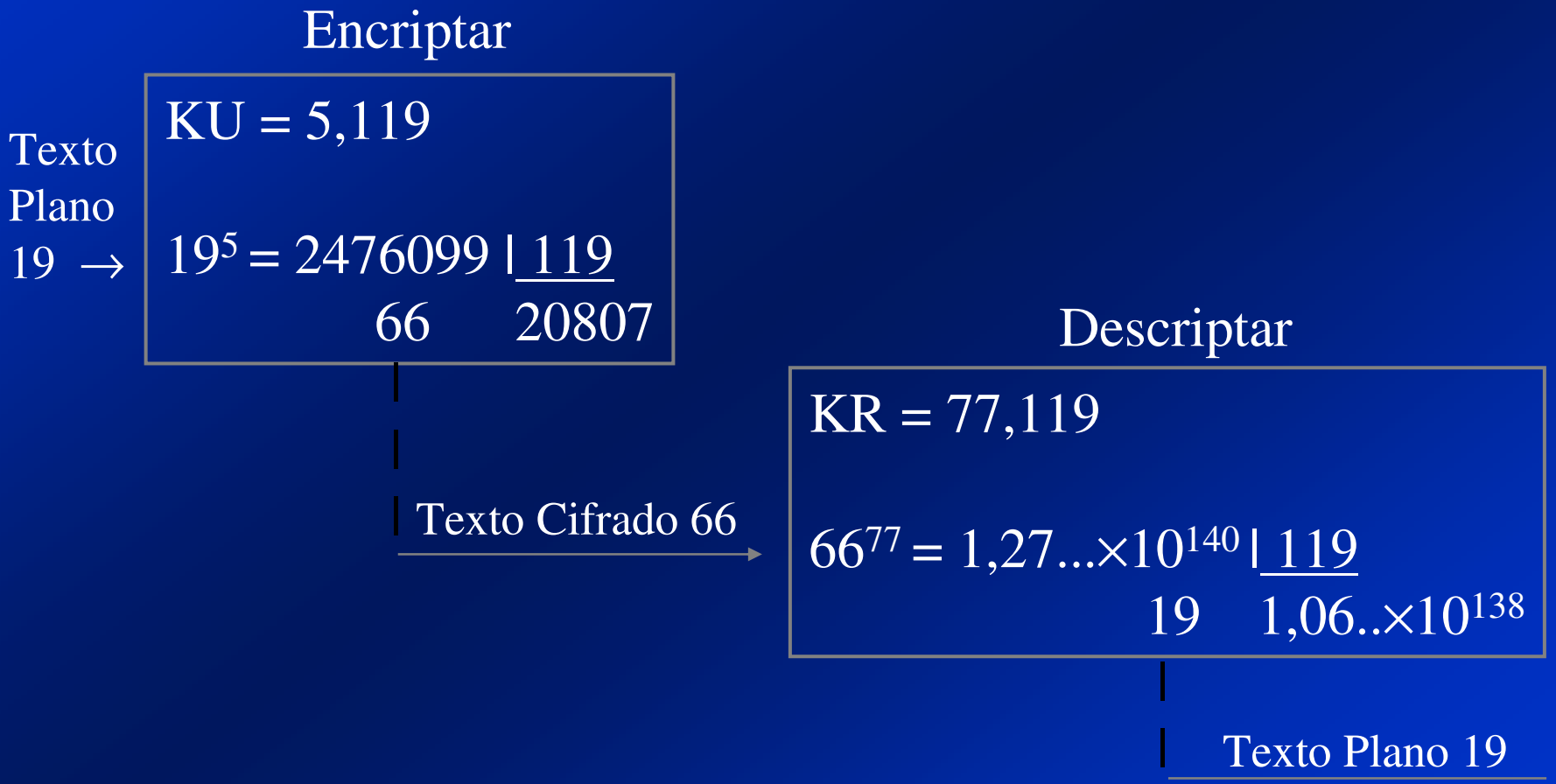
Desencriptar

Texto Cifrado:	C
Texto Plano:	$M = C^d \pmod n$

Algoritmo RSA (Ron **R**ivest, Adi **S**hamir e Len **A**dleman)

- **Exemplo Geração de Chaves**
  - Selecionar dois números primos, $p = 7$ e $q = 17$
  - Calcular $n = pq = 7 \times 17 = 119$
  - Calcular $\phi(n) = (p - 1)(q - 1) = 96$.
  - Selecionar e tal que e é relativamente primo à $\phi(n) = 96$ e menor que $\phi(n)$; neste caso, $e = 5$
  - Determinar d tal que $de = 1 \pmod{96}$ e $d < 96$; logo $d = 77$, visto que $77 \times 5 = 385 = 4 \times 96 + 1$
  - Assim: KU = { 5, 119 } e KR = { 77, 119 }

Algoritmo RSA (Ron **R**ivest, Adi **S**hamir e Len **A**dleman)



Sistemas criptográficos

- Chave Secreta

- **Para Usar**
  - Um algoritmo e uma chave
  - A e B compartilham o algoritmo e a chave

- **Para a segurança**
  - Chave secreta
  - Impossibilidade de descifrar a mensagem
  - Algoritmo + amostra do texto cifrado não é suficientes para determinar a chave

X Chave Pública

- **Para Usar**
  - Um algoritmo e duas chave
  - A e B compartilham um par de chaves

- **Para a segurança**
  - Uma chave pública
  - Impossibilidade de descifrar a mensagem
  - Algoritmo + amostra do texto cifrado + chave pública não determina a chave privada

Uso de Sistemas Criptográficos para Sigilo