Capítulo 9

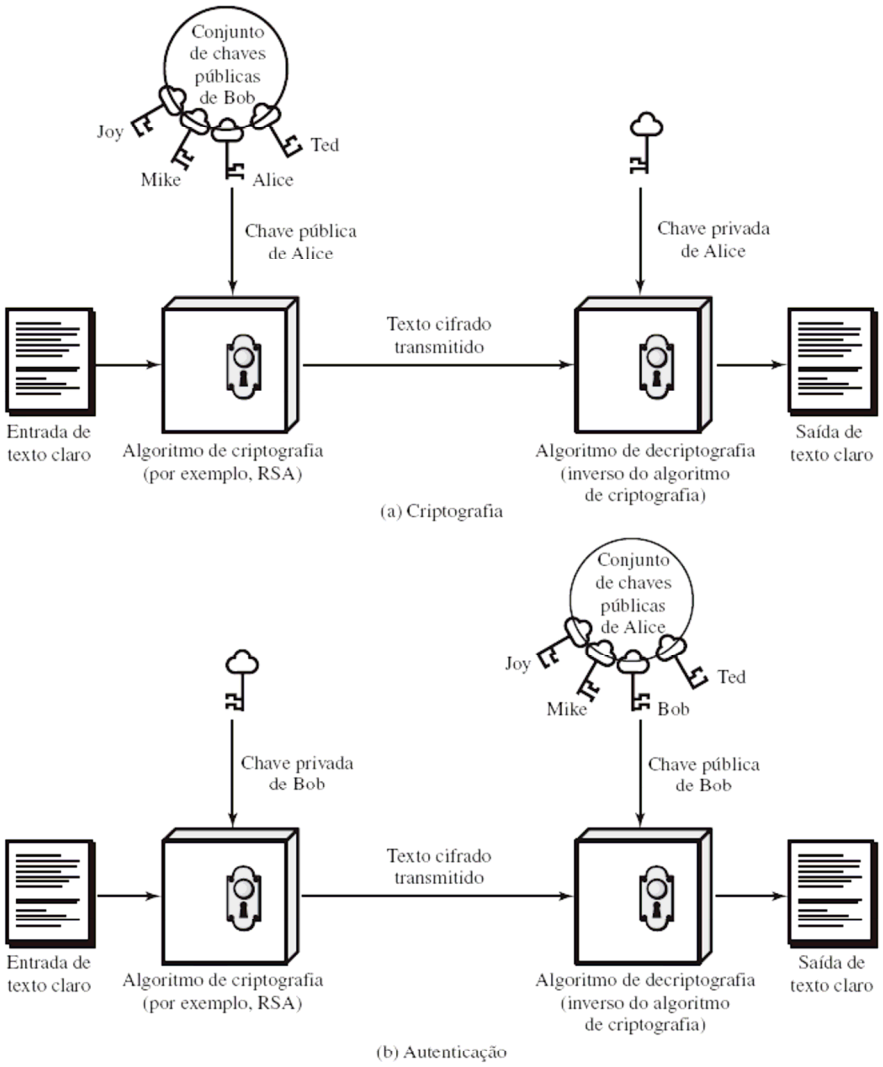


Figura 9.1 Criptografia de chave pública.

Tabela 9.1 Criptografia convencional e de chave pública

Criptografia convencional	Criptografia de chave pública
Necessário para funcionar: 1. O mesmo algoritmo com a mesma chave é usado para criptografia e decriptografia. 2. O emissor e o receptor precisam compartilhar o algoritmo e a chave. **Necessário para a segurança:** 1. A chave precisa permanecer secreta. 2. Deverá ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível. 3. O conhecimento do algoritmo mais amostras do texto cifrado precisam ser insuficientes para determinar a chave.	**Necessário para funcionar:** 1. Um algoritmo é usado para criptografia e decriptografia com um par de chaves, uma para criptografia e outra para decriptografia. 2. O emissor e o receptor precisam ter uma das chaves do par casado de chaves (não a mesma chave). **Necessário para a segurança:** 1. Uma das duas chaves precisa permanecer secreta. 2. Deverá ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível. 3. O conhecimento do algoritmo mais uma das chaves mais amostras do texto cifrado precisam ser insuficientes para determinar a outra chave.

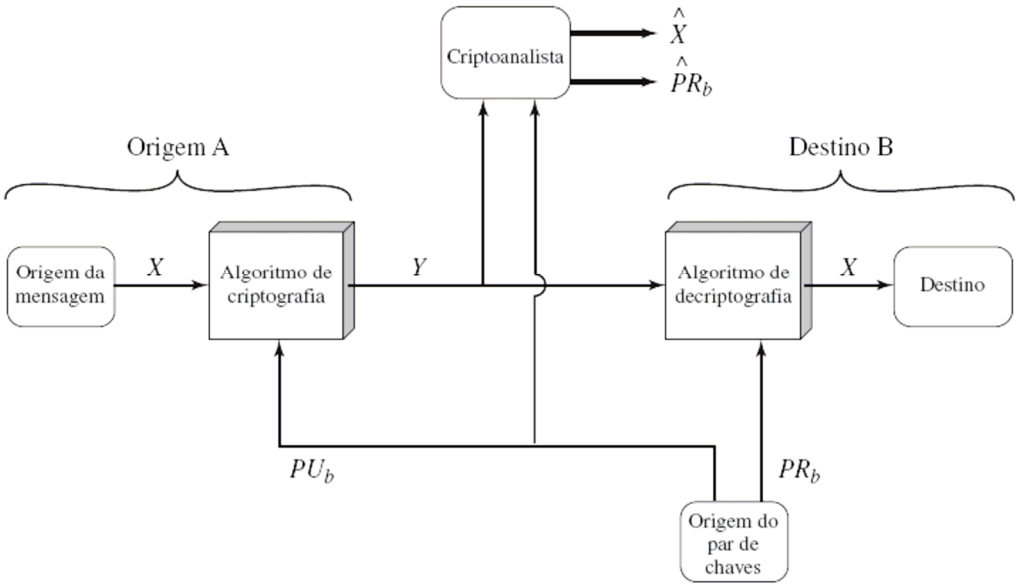


Figura 9.2 Criptossistema de chave pública: sigilo.

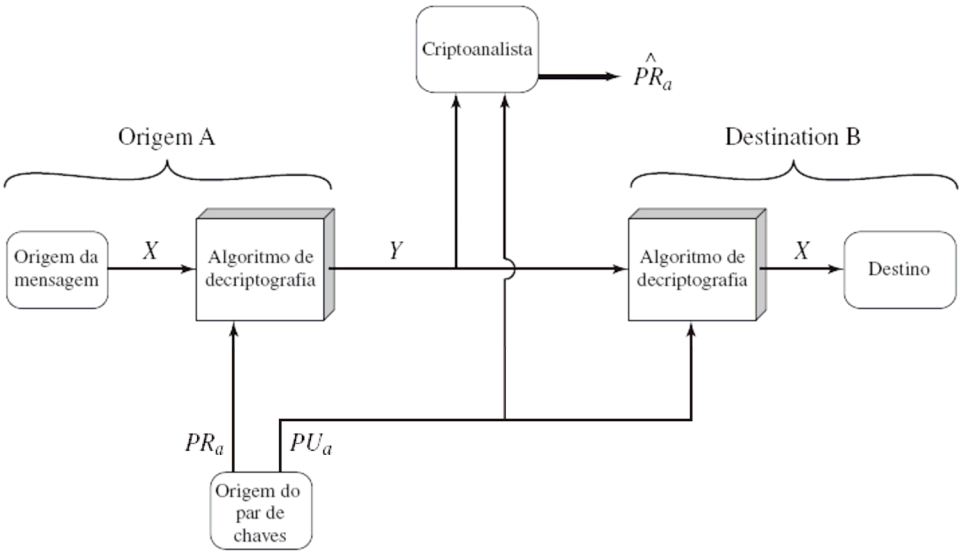


Figura 9.3 Criptossistema de chave pública: autenticação.

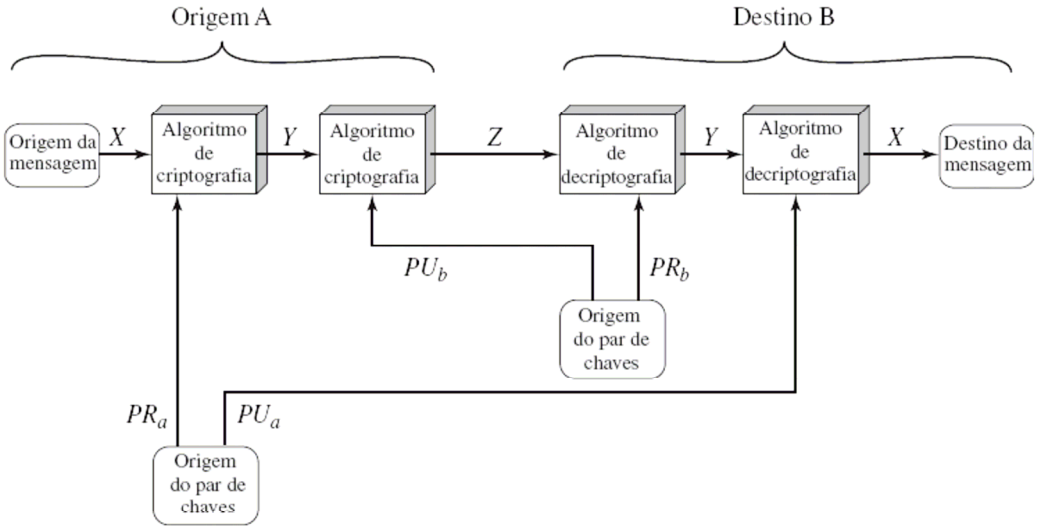


Figura 9.4 Criptossistema de chave pública: autenticação e sigilo.

Tabela 9.2 Aplicações para criptossistemas de chave pública

Algoritmo	Criptografia/decriptografia	Assinatura digital	Troca de chave
RSA	Sim	Sim	Sim
Curva elíptica	Sim	Sim	Sim
Diffie-Hellman	Não	Não	Sim
DSS	Não	Sim	Não

Geração de chaves

Selecione p, q	p eq são primos, $p \neq q$
Calcule $n = p \times q$	
Calcule $\phi(n) = (p - 1)(q - 1)$	
Selecione o inteiro e	mdc $(\phi(n), e) = 1; 1 < e < \phi(n)$
Calcule d	$d \equiv e^{-1} \pmod{\phi(n)}$
Chave pública	$PU = \{e, n\}$
Chave privada	$PR = \{d, n\}$

Criptografia

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

Decriptografia

Texto cifrado:	C
Texto claro:	$M = C^d \bmod n$

Figura 9.5 O algoritmo RSA.

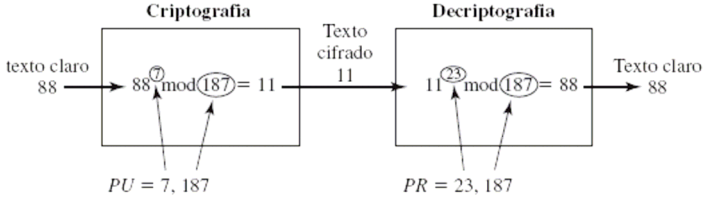


Figura 9.6 Exemplo de algoritmo RSA.

```
c ← 0; f ← 1
for i ← k downto 0
    do  c ← 2 × c
        f ← (f × f) mod n
    if  b_i = 1
        then c ← c + 1
             f ← (f × a) mod n
return f
```

Nota: O inteiro b é expresso como um número binário $b_k b_{k-1} \ldots b_0$

Figura 9.7 Algoritmo para calcular $a^b \bmod n$.

Tabela 9.3 Resultado do algoritmo da exponenciação modular rápida para $a^b \bmod n$, onde $a = 7$, $b = 560 = 1000110000$, $n = 561$

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	0	1	1	0	0	0	0
c	1	2	4	8	17	35	70	140	280	560
f	7	49	157	526	160	241	298	166	67	1

Tabela 9.4 Progresso na fatoração

Número de dígitos decimais	Número aproximado de bits	Data em que foi alcançado	MIPS-anos	Algoritmo
100	332	abril de 1991	7	Crivo quadrático
110	365	abril de 1992	75	Crivo quadrático
120	398	junho de 1993	830	Crivo quadrático
129	428	abril de 1994	5000	Crivo quadrático
130	431	abril de 1996	1000	Crivo de corpo numérico generalizado
140	465	fevereiro de 1999	2000	Crivo de corpo numérico generalizado
155	512	agosto de 1999	8000	Crivo de corpo numérico generalizado
160	530	abril de 2003	—	Crivo de malha (Lattice sieve)
174	576	dezembro de 2003	—	Crivo de malha (Lattice sieve)
200	663	maio de 2005	—	Crivo de malha (Lattice sieve)

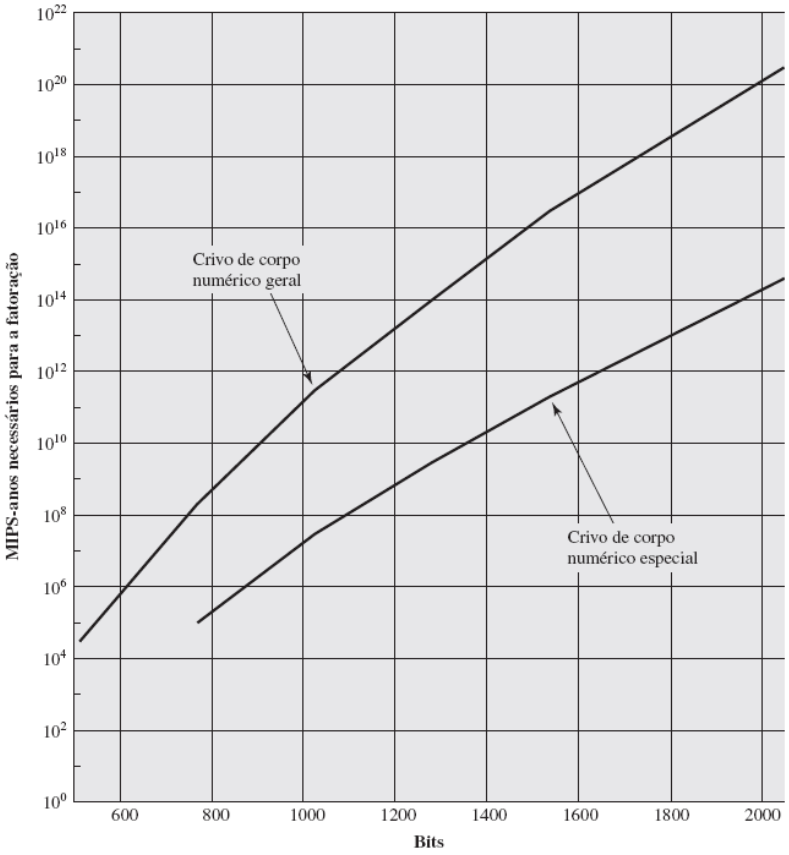
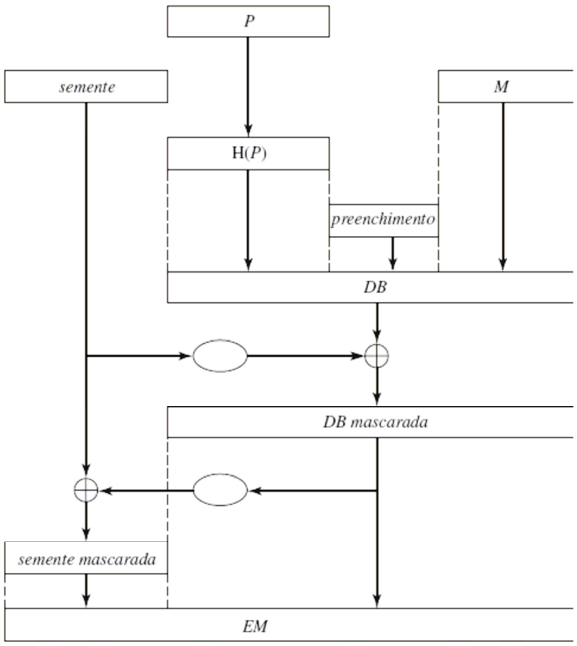


Figura 9.8 MIPS-anos necessários para a fatoração.



P = parâmetros de codificação
M = mensagem a ser codificada
H = função de hash
DB = bloco de dados
MGF = função de geração de máscara
EM = mensagem codificada

Figura 9.9 Criptografia usando preenchimento ideal de criptografia assimétrica (OAEP).

Tabela 9.5 Nível de esforço para vários níveis de complexidade

Complexidade	Tamanho	Operações
$\log_2 n$	$2^{10^{12}} = 10^{3\times10^{11}}$	10^{12}
N	10^{12}	10^{12}
n^2	10^6	10^{12}
n^6	10^2	10^{12}
2^n	39	10^{12}
$n!$	15	10^{12}