Criptografia de chave pública e RSA

Objetivos de aprendizagem

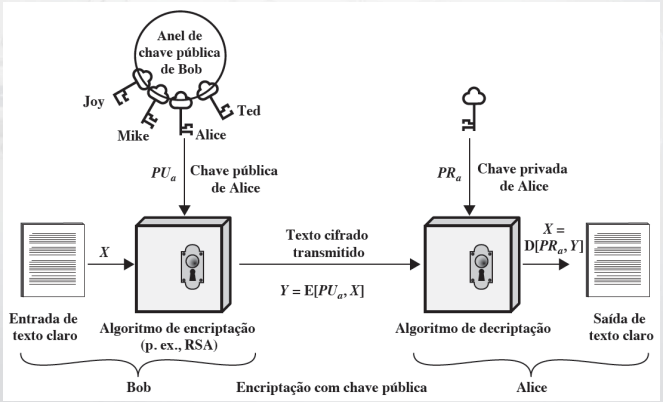
- Apresentar uma visão geral dos princípios básicos dos criptossistemas de chave pública.
- Explicar os dois usos distintos dos criptossistemas de chave pública.
- Listar e explicar os requisitos para um criptossistema de chave pública.
- Apresentar uma visão geral do algoritmo RSA.
- Entender o ataque de temporização.
- Resumir os aspectos relevantes relacionados à complexidade dos algoritmos.

Princípios de criptossistemas de chave pública

- Os algoritmos assimétricos contam com uma chave para encriptação e uma chave diferente, porém relacionada, para a decriptação.
- Eles têm a seguinte característica importante:
- É computacionalmente inviável determinar a chave de decriptação dado apenas o conhecimento do algoritmo de criptografia e da chave de encriptação.
- Qualquer uma das duas chaves relacionadas pode ser usada para encriptação, com a outra para a decriptação.

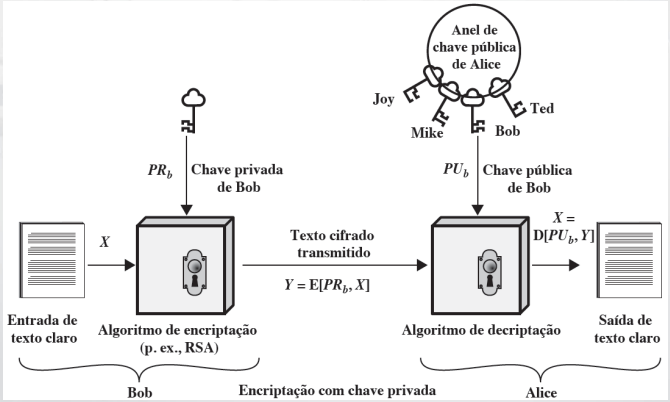
Princípios de criptossistemas de chave pública

- Um esquema de encriptação de chave pública possui cinco elementos:



Princípios de criptossistemas de chave pública

- Um esquema de encriptação de chave pública possui cinco elementos:



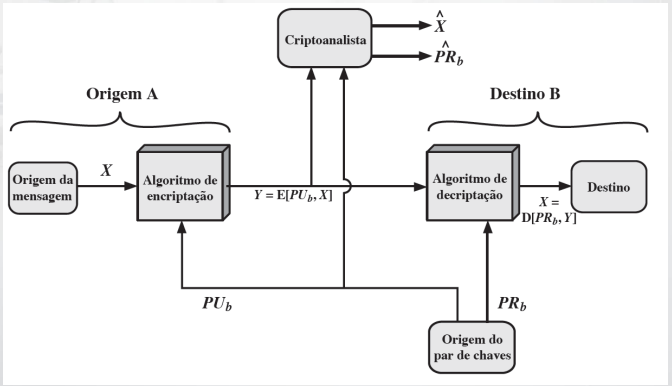
Princípios de criptossistemas de chave pública

- Encriptação convencional e de chave pública:

ENCRIPTAÇÃO CONVENCIONAL	ENCRIPTAÇÃO DE CHAVE PÚBLICA
Necessário para funcionar:	*Necessário para funcionar:*
1. O mesmo algoritmo com a mesma chave é usado para encriptação e decriptação.	1. Um algoritmo é usado para encriptação, e um relacionado, para decriptação com um par de chaves, uma para encriptação e outra para decriptação.
2. O emissor e o receptor precisam compartilhar o algoritmo e a chave.	2. O emissor e o receptor precisam ter, cada um, uma chave do par (não a mesma).
Necessário para a segurança:	*Necessário para a segurança:*
1. A chave precisa permanecer secreta.	1. Uma das duas chaves precisa permanecer secreta.
2. Deverá ser impossível, ou pelo menos impraticável, decifrar uma mensagem se a chave for mantida secreta.	2. Deverá ser impossível, ou pelo menos impraticável, decifrar uma mensagem se uma das chaves for mantida secreta.
3. O conhecimento do algoritmo mais amostras do texto cifrado precisam ser insuficientes para determinar a chave.	3. O conhecimento do algoritmo mais uma das chaves mais amostras do texto cifrado precisam ser insuficientes para determinar a outra chave.

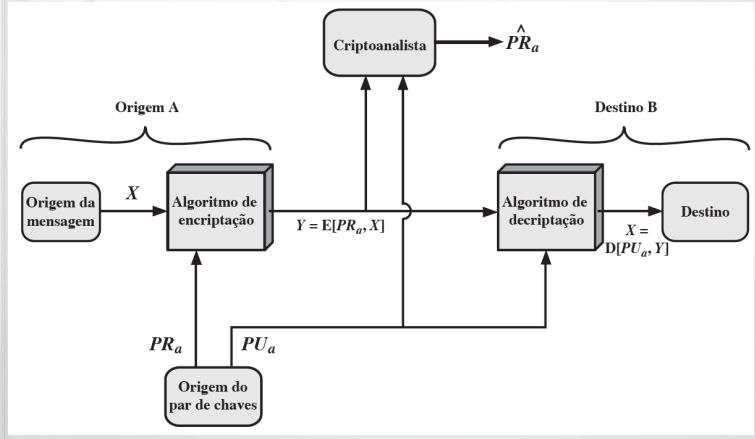
Princípios de criptossistemas de chave pública

- Criptossistema de chave pública – sigilo:



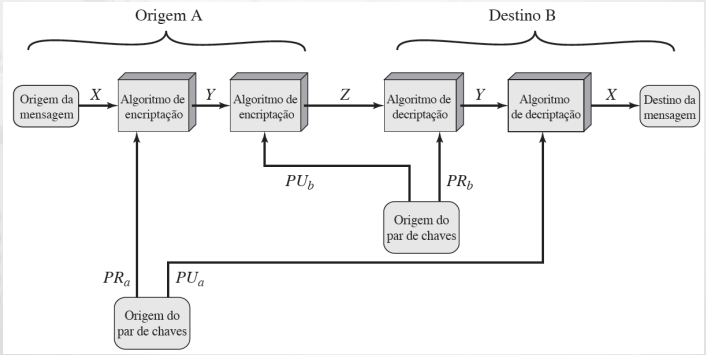
Princípios de criptossistemas de chave pública

- Criptossistema de chave pública – autenticação:



Princípios de criptossistemas de chave pública

- Criptossistema de chave pública – autenticação e sigilo:



Aplicações para criptossistemas de chave pública

ALGORITMO	ENCRIPTAÇÃO/ DECRIPTAÇÃO	ASSINATURA DIGITAL	TROCA DE CHAVE
RSA	Sim	Sim	Sim
Curva elíptica	Sim	Sim	Sim
Diffie-Hellman	Não	Não	Sim
DSS	Não	Sim	Não

Algoritmo RSA *(Rivest-Sharmir-Adleman)*

- O esquema RSA é uma cifra de bloco em que o texto claro e o cifrado são inteiros entre 0 e $n - 1$, para algum n.
- Um tamanho típico para n é 1024 bits, ou 309 dígitos decimais.
- RSA utiliza uma expressão com exponenciais.
- O texto claro é encriptado em blocos, com cada um tendo um valor binário menor que algum número n.

Algoritmo RSA

- O algoritmo RSA:

Geração de chave por Alice	
Selecione p, q	p e q são primos, $p \neq q$
Calcule $n = p \times q$	
Calcule $\phi(n) = (p-1)(q-1)$	
Selecione o inteiro e	$\text{mdc}(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calcule d	$d \equiv e^{-1} \pmod{\phi(n)}$
Chave pública	$PU = \{e, n\}$
Chave privada	$PR = \{d, n\}$
Encriptação por Bob com chave pública de Alice	
Texto claro:	$M < n$
Texto cifrado:	$C = M^e \bmod n$
Decriptação por Alice com a chave privada de Alice	
Texto cifrado:	C
Texto claro:	$M = C^d \bmod n$

RSA: Exemplo

Bob escolhe $p = 5$, $q = 7$. Depois, $n = 35$, $\varphi(n) = 24$.

$e = 5$ "mdc(e, φ(n))=1; 1 < e < φ(n)"

$d = 29$ "$d*e = 1 \pmod{\varphi(n)}$".

Criptografando mensagens de 8 bits.

	padrão de bits	m	m^e	$c = m^e \bmod n$
criptografia:	0000l000	12	24832	17

	c	c^d	$m = c^d \bmod n$
decriptação:	17	481968572106750915091411825223071697	12

Algoritmo RSA

- Tanto encriptação quanto decriptação no RSA envolvem elevar um inteiro a uma potência inteira, mod *n*.
- Se a exponenciação fosse feita sobre os inteiros e depois reduzida módulo *n*, os valores intermediários seriam gigantescos.
- Felizmente, podemos utilizar uma propriedade da aritmética modular:

$$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$$

Algoritmo RSA

- Algoritmo para calcular $a^b \bmod n$:

```
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
```

A=7, b=560=1000110000 e n =561

i	9	8	7	6	5	4	3	2	1	0
bi	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

Algoritmo RSA

- Para agilizar a operação do algoritmo RSA usando a chave pública, normalmente é feita uma escolha específica de *e*.
- A mais comum é 65537 (2^{16} + 1); duas outras escolhas populares são 3 e 17.
- Cada uma delas tem apenas dois bits 1, e, por isso, o número de multiplicações exigidas para realizar a exponenciação é minimizado.
- Porém, com uma chave pública muito pequena, como $e = 3$, o RSA torna-se vulnerável a um ataque simples.

Algoritmo RSA

- Antes da aplicação do criptossistema de chave pública, cada participante precisa gerar um par de chaves.
- Isso envolve as seguintes tarefas:

1. Determinar dois números primos, *p* e *q*.
2. Selecionar *e* ou *d* e calcular o outro.

- Resumindo, o procedimento para escolher um número primo é o seguinte:

1. Escolha um inteiro ímpar *n* aleatoriamente.

Algoritmo RSA

2. Escolha um inteiro $a < n$ aleatoriamente.
3. Realize o teste probabilístico de números primos, como Miller-Rabin, usando *a* como parâmetro. Se *n* falhar no teste, rejeite o valor dele e vá para a etapa 1.
4. Se *n* tiver passado por um número de testes suficiente, aceite-o; caso contrário, vá para a etapa 2.

- Esse processo é realizado com relativamente pouca frequência: somente quando um novo par (*PU*, *PR*) é necessário.

Segurança do RSA

- Cinco técnicas possíveis para atacar o algoritmo RSA são as seguintes:

1. **Força bruta**: isso envolve tentar todas as chaves privadas possíveis.
2. **Ataques matemáticos**: existem várias técnicas, todas equivalentes em esforço a fatorar o produto de dois primos.
3. **Ataques de temporização**: estes dependem do tempo de execução do algoritmo de decriptação.

Segurança do RSA

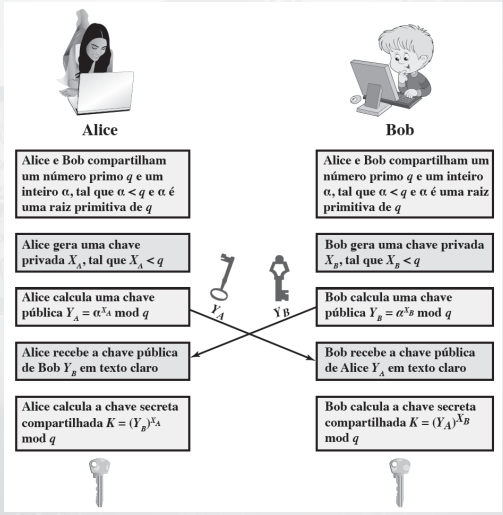
4. **Ataques baseados em falha de hardware**: estes envolvem a indução de falhas de hardware no processador que está gerando as assinaturas digitais.
5. **Ataques de texto cifrado escolhido**: esse tipo de ataque explora as propriedades do algoritmo RSA.

- A defesa contra a técnica de força bruta é a mesma para o RSA e para outros criptossistemas, ou seja, usar um espaço de chave grande.
- Assim, quanto maior o número de bits em *d*, melhor.

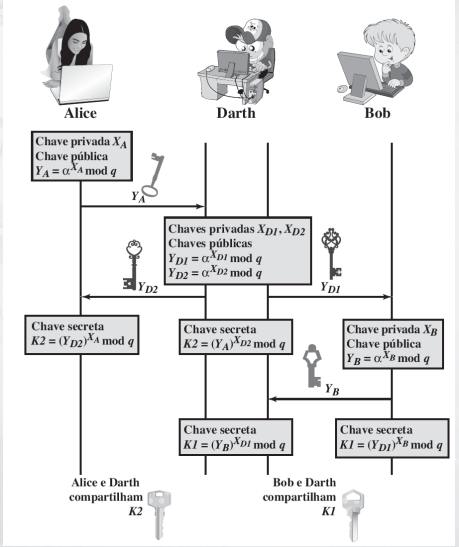
Troca de chaves Diffie-Hellman

- A finalidade do algoritmo é permitir que dois usuários troquem uma chave com segurança, que pode, então, ser usada para a criptografia subsequente das mensagens.
- O próprio algoritmo é limitado à troca de valores secretos.
- O algoritmo Diffie-Hellman depende, para a sua eficácia, da dificuldade de se calcular logaritmos discretos.
- A figura a seguir resume o algoritmo de troca de chaves Diffie-Hellman.

Troca de chaves Diffie-Hellman



Ataque *man-in-the-middle*



Exercício

Geração de chave por Alice	
Selecione p, q	p e q são primos, $p \neq q$
Calcule $n = p \times q$	
Calcule $\phi(n) = (p-1)(q-1)$	
Selecione o inteiro e	$\text{mdc}(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calcule d	$d = e^{-1} \pmod{\phi(n)}$
Chave pública	$PU = \{e, n\}$
Chave privada	$PR = \{d, n\}$
Encriptação por Bob com chave pública de Alice	
Texto claro:	$M < n$
Texto cifrado:	$C = M^e \bmod n$
Decriptação por Alice com a chave privada de Alice	
Texto cifrado:	C
Texto claro:	$M = C^d \bmod n$

Para o algoritmo RSA, adote os valores, *p = 17, q =11* e *e=7*:

a) Determine a chave pública
b) Determine a chave privada
c) Encripte e decripte a mensagem, M = 88