Autenticação por par de chaves assimétricas

Bruno Follmann

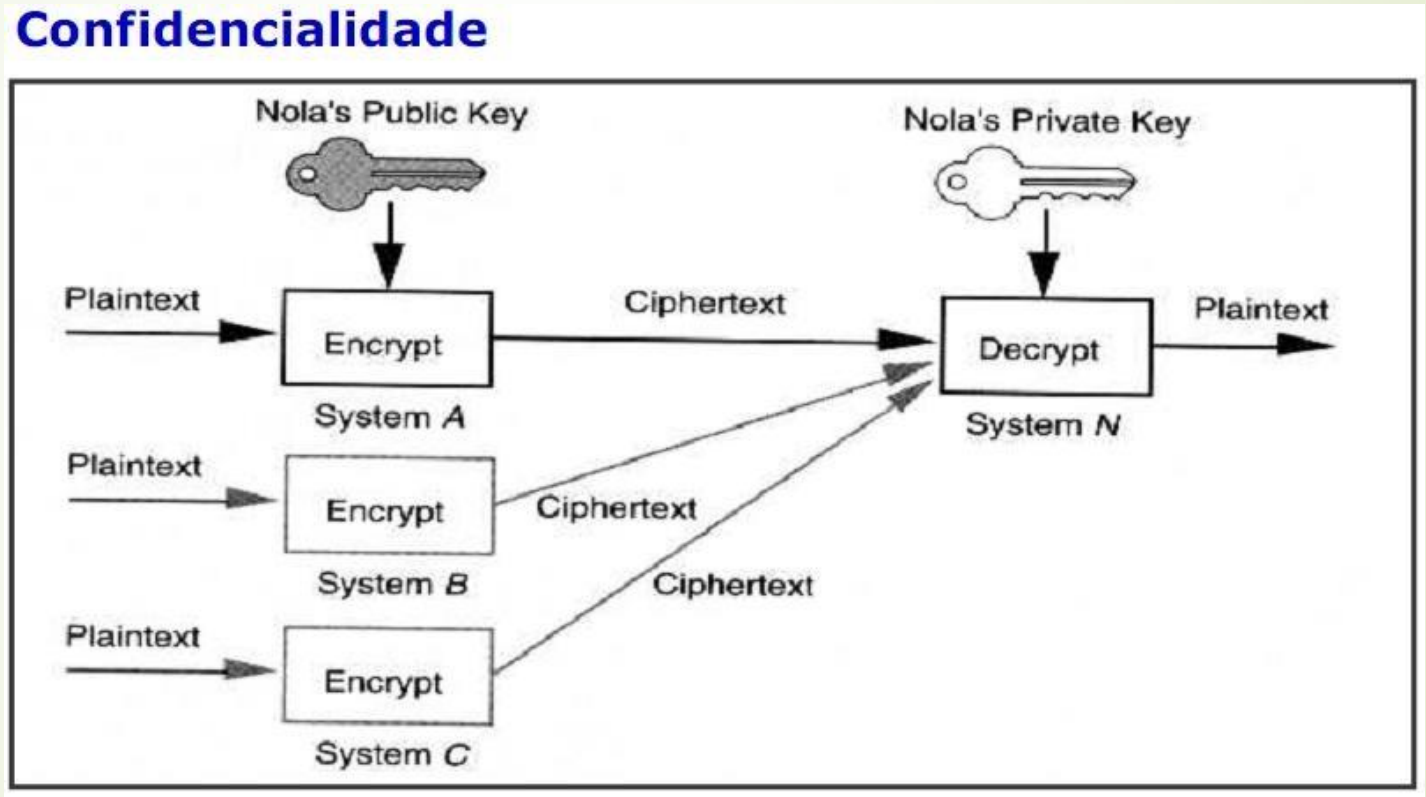
Criptografia assimétrica

- Criada em 1976 por Diffie e Hellman;
- Também chamada de criptografia de chave pública;
- Sistema para cifrar e decifrar uma mensagem com duas chaves distintas;
- A chave pública pode ser divulgada e a privada deve ser mantida em segredo;
- Se uma mensagem for cifrada com uma das chaves, só pode ser decifrada pela outra.

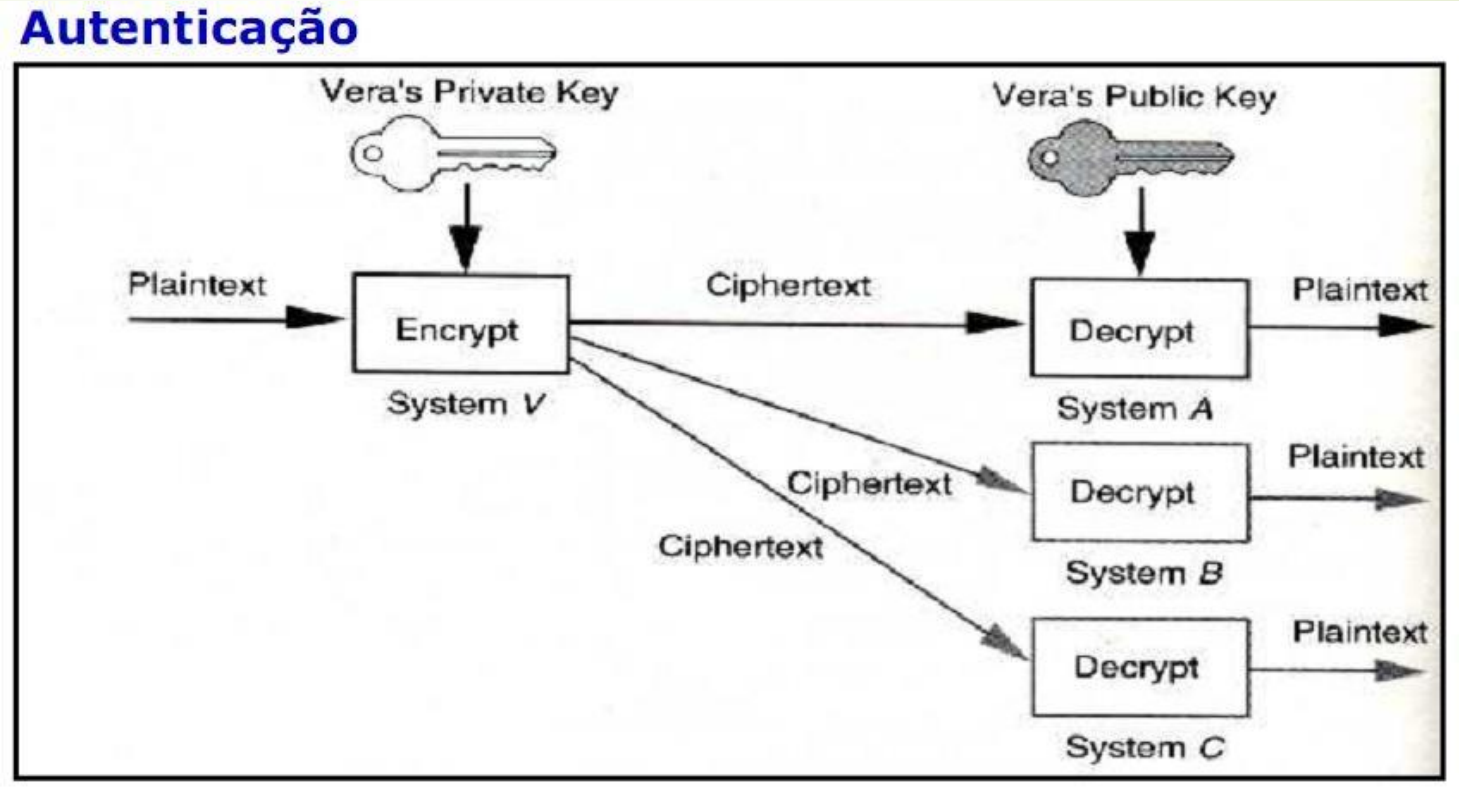
Criptografia assimétrica

- Não substitui a criptografia simétrica;
- É uma técnica lenta e vulnerável a alguns ataques;
- Geralmente, criptografia assimétrica é usada para distribuir chaves simétricas;
- O originador gera uma chave simétrica e cifra a mesma usando a chave pública (assimétrica) do receptor;
- Só poderá decifrar a mensagem quem tiver a chave assimétrica do receptor;
- Assim, obtém-se a chave simétrica e ela pode ser usada para comunicação.

Criptografia assimétrica



Criptografia assimétrica



Geração de um par de chaves

- Geradas por um par de números aleatórios;
- Essa criptografia é possível pois há um relacionamento matemático entre as chaves;
- Há diversas técnicas possíveis;
- Como já mencionado, a primeira foi o protrocolo de Diffie-Hellman.

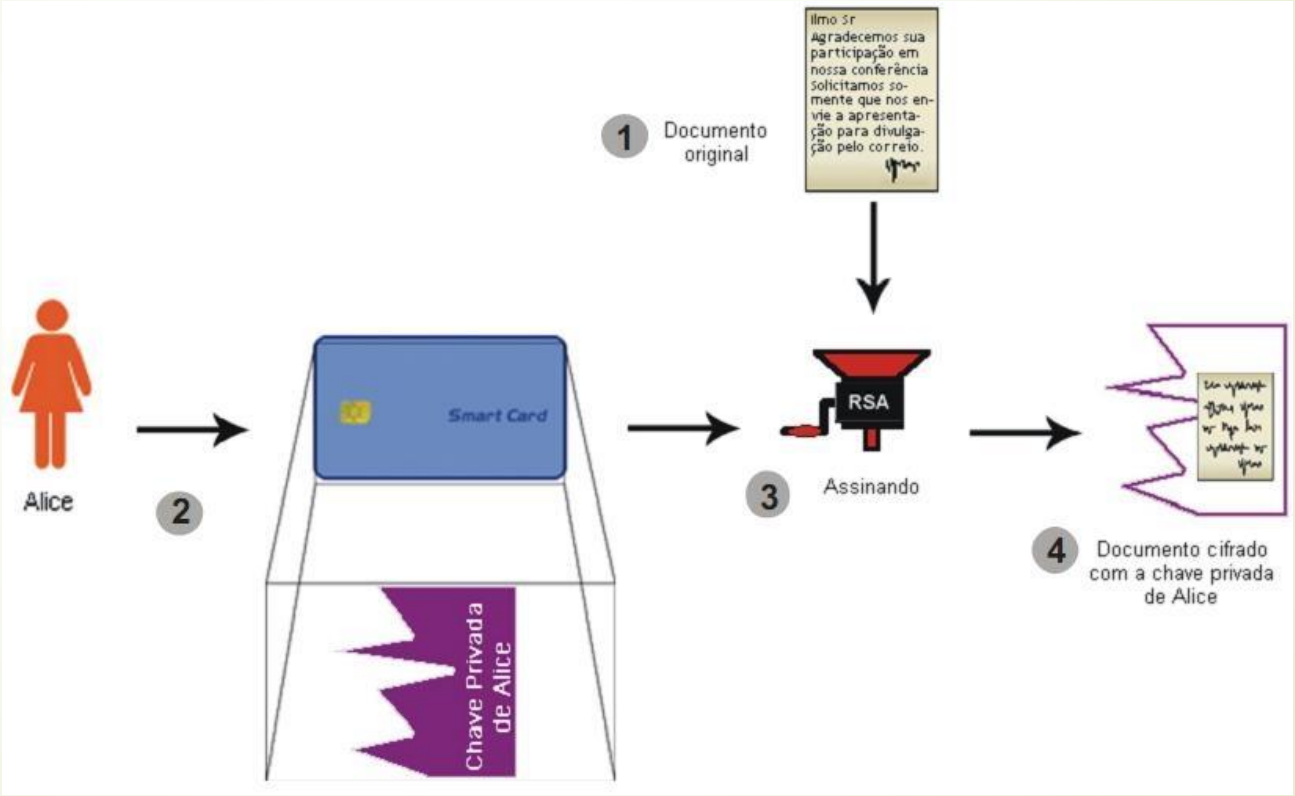
- Alice e Beto entram em acordo para usar um número primo p=23 e como base g=5 (que é raíz primitiva módulo 23).
- Alice escolhe um inteiro secreto ***a*=6**, e então envia a Beto A = g^a mod p
  - A = 5^{6} mod 23
  - A = **15.625** mod 23
  - A = 8
- Beto escolhe um inteiro secreto ***b*=15**, e então envia a Alice B = g^b mod p
  - B = 5^{15} mod 23
  - B = **30.517.578.125** mod 23
  - B = 19
- Alice calcula **s** = B^a mod p
  - **s** = 19^{6} mod 23
  - **s** = **47.045.881** mod 23
  - **s** = **2**

- Beto computa **s** = A^{b} mod p
  - **s** = 8^{15} mod 23
  - **s** = **35.184.372.088.832** mod 23
  - **s** = **2**
- Alice e Beto compartilham agora uma chave secreta: **s** = **2**. Isto é possível porque 6*15 é o mesmo que 15*6. Alguém que tenha descoberto estes dois inteiros privados também será capaz de calcular s da seguinte maneira:
  - **s** = 5^{6*15} mod 23
  - **s** = 5^{15*6} mod 23
  - **s** = 5^{90} mod 23
  - **s** = **807.793.566.946.316.088.741.610.050.849.573.099.185.363.389.551.639.556.884.765.625** mod 23
  - **s** = **2**

Algoritmo RSA

- É a base da maioria das aplicações que empregam criptografia assimétrica;
  1. Escolha dois números primos extensos, p e q, de ordem mínima 10^{100};
  2. Calcule n = p x q;
  3. z = (p – 1) x (q –1);
  4. Escolha um número relativamente primo em relação a “z” e chame-o de “e”;
  5. Encontre “d” de forma que d = e^{-1} mod z. (“mod” é o resto inteiro da divisão).
- Portando, a chave pública (KU) consiste em KU = {e, n} e a chave privada (KR) consiste em KR = {d, n}.

Cifrando com a chave privada



Cifrando com a chave privada

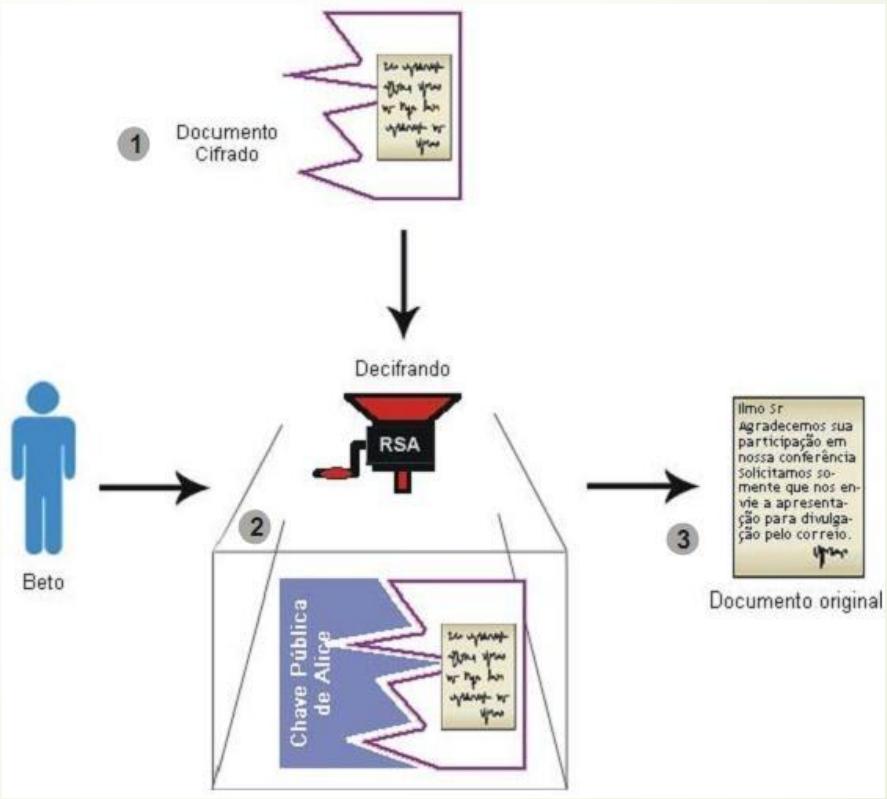
A função RSA para cifrar, utilizando a chave privada, é a seguinte:

$C = M^d \pmod{n}$

Onde:

- C = texto cifrado;
- M = texto plano;
- “d” e “n” são a chave privada KR = {d,n}.

Decifrando com a chave pública



Decifrando com a chave pública

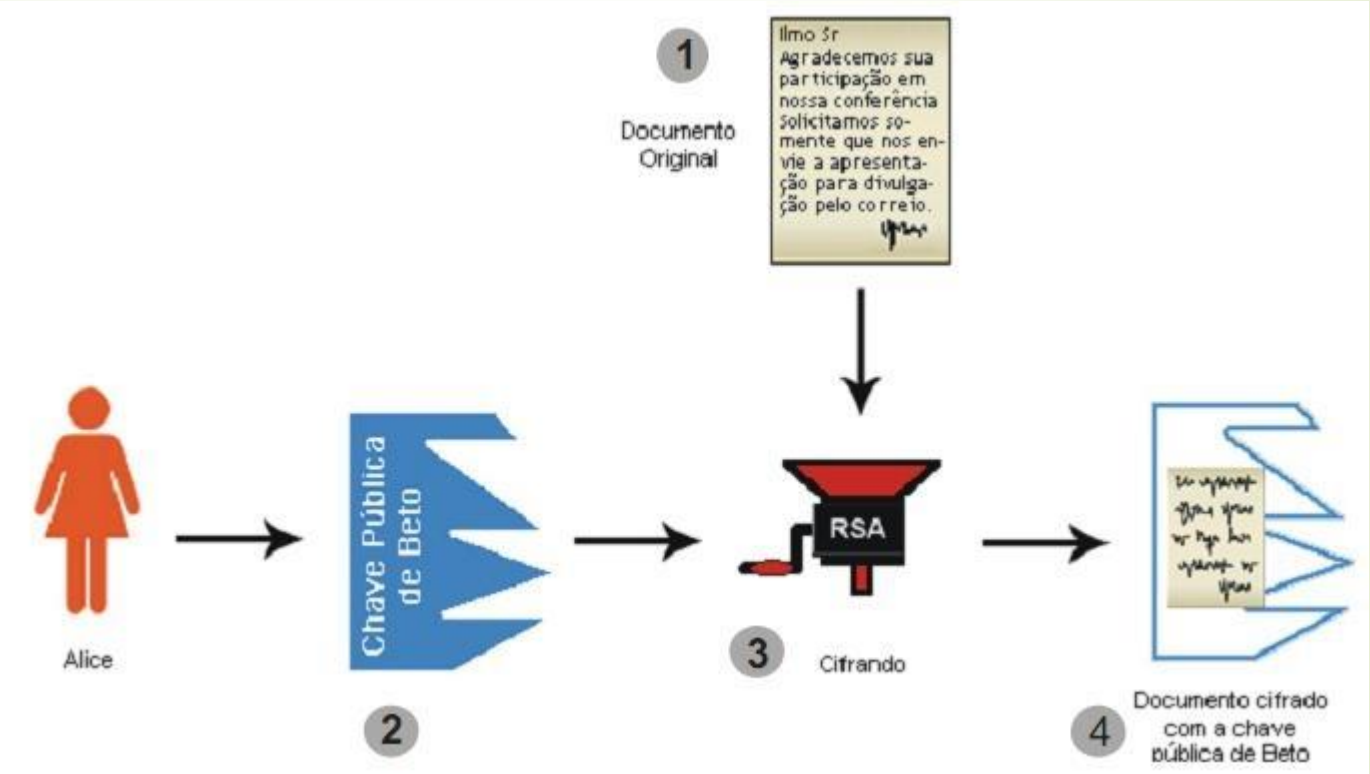
A função RSA para decifrar, utilizando a chave pública, é a seguinte:

$M = C^e \pmod n$

Onde:

- M = texto plano
- C = texto cifrado
- “e” e “n” são a chave pública KU = {e,n}.

Cifrando com a chave pública



Cifrando com a chave pública

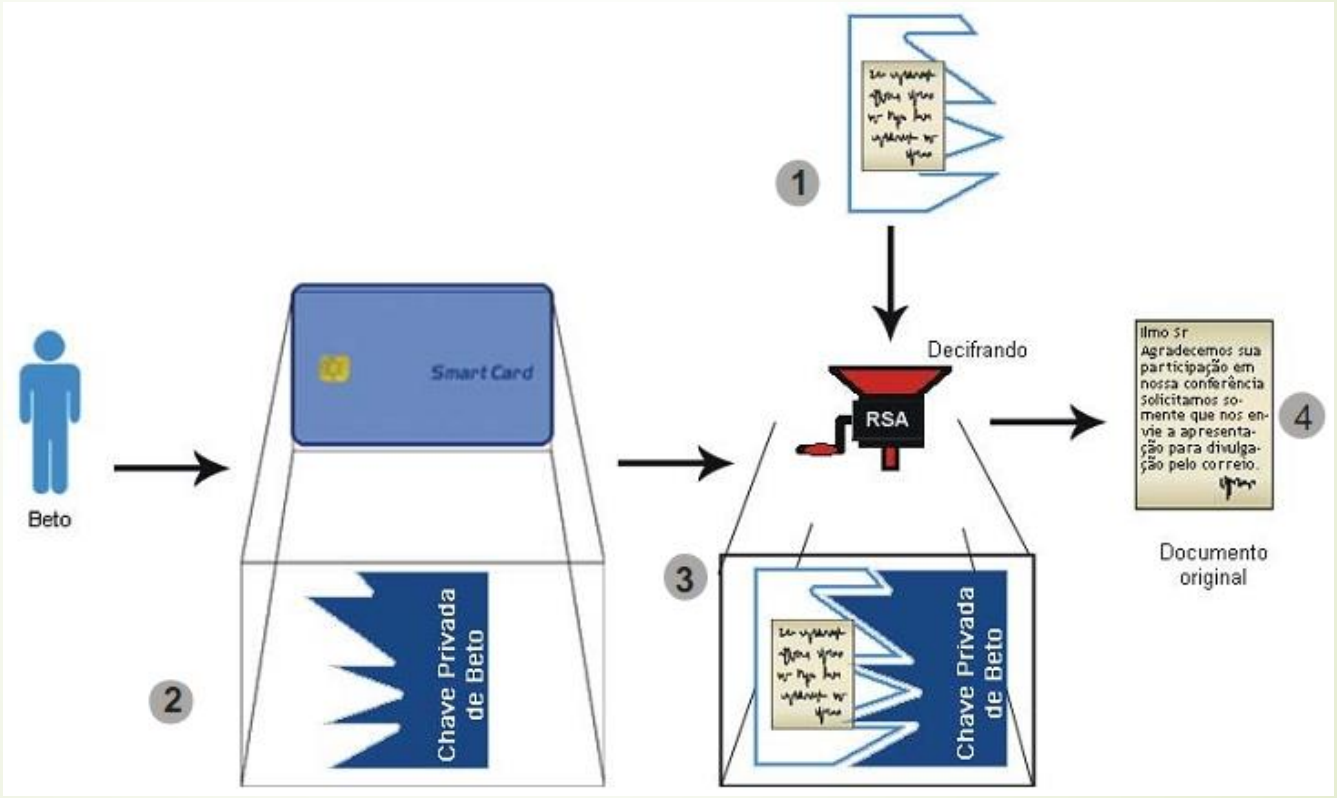
A função RSA para cifrar, utilizando a chave pública, é a seguinte:

$C = M^e \pmod{n}$

Onde:

- C = texto cifrado
- M = texto plano
- “e” e “n” são a chave pública KU = {e,n} do destinatário.

Decifrando com a chave privada



Decifrando com a chave privada

A função RSA para decifrar, utilizando a chave privada, é a seguinte:

$M = C^d \pmod n$

Onde:

- M = texto plano
- C = texto cifrado
- “d” e “n” são a chave privada KR = {d,n}.

- Números primos: p = 61 e q = 53;
- n = 61 x 53 = 3233;
- z = (61 - 1)(53 - 1) = 3120;
- Escolhe-se e = 17, pois é coprimo de 3120;
- $d = e^{-1} \mod z = 2753$;
- Chave pública: (n = 3233, e = 17);
  - Para uma mensagem em texto simples m, a encripção: $c(m) = m^{17} \mod 3233$;
- Chave privada: (d = 2753);
  - Para uma mensagem em texto cifrado c, a decripção: $m(c) = m^{2753} \mod 3233$;
- Assim, se o objetivo fosse encriptar e decriptar m = 65:
  - $c(65) = 65^{17} \mod 3233 = 2790$;
  - $m(2790) = 2790^{2753} \mod 3233 = 65$.

Criptografia assimétrica

- O texto cifrado é do mesmo tamanho que o texto plano;
- Utiliza funções exponenciais para cifrar e decifrar, o que a torna lenta;
- Ela possibilita as tarefas de autenticação e sigilo;
- Pode tornar a troca de chaves simétricas segura.

Criptoanálise

Decifração de uma mensagem cifrada, sem o códigos ou algoritmos empregados.

Um documento é dito seguro se:

- O custo para quebrar o texto cifrado excede ao valor da informação cifrada;
- O tempo requerido para quebrar o texto cifrado excede o tempo de vida útil da informação.

Várias técnicas são empregadas para tentar quebrar chaves, sendo a mais comum a de força bruta.

Segurança

- O RSA baseia-se da grande dificuldade dos computadores de fatorarem números grandes;
- Mesmo que se tenha o produto dos números primos (que faz parte da chave pública), é normalmente inviável fatorá-lo;
- Supondo um ataque de força bruta por computadores operando a 1 bilhão de instruções por segundo por 1 ano:
- Uma chave assimétrica de 512 bits necessitaria de 30 computadores;
- Uma chave assimétrica de 768 bits demandaria 200 mil desses computadores;
- Uma chave assimétrica de 1024 bits demandaria 300 milhões;
- Uma chave de 2048 bits exigiria 300 quadrilhões para ser quebrada.

Hash

- Significa "picar, misturar, confundir“;
- É usada em conjunto com a criptografia assimétrica;
- Tem como finalidade computar um resumo de mensagem ao criar uma assinatura digital;
- É utilizada para garantir a integridade de um documento digital;
- Resumo da cadeia de bits da entrada;
- Unicamente identificável com aquela entrada;
- Tem a função parecida com a do digito verificador do CPF.

Hash

Algumas das propriedades desta função são:

- Deve ser computacionalmente inviável fazer a operação inversa, ou seja, dado um resumo, deve ser inviável obter uma mensagem original;
- Duas mensagens semelhantes devem produzir um resumo completamente diferente;
- Deve ser fácil e rápido produzir o resumo.

Hash

- A função resumo pode ser utilizada para garantir a integridade de uma mensagem;
- Envia-se uma mensagem e o resumo da mensagem cifrada com a chave privada;
- O receptor decifra o resumo com a chave pública do remetente, depois calcula um novo resumo com base na mensagem recebida e compara os dois valores;
- Se forem iguais, a mensagem não foi alterada, garantindo-se dessa forma a sua integridade.

Certificados digitais

- Cenário: em uma transação bancária o banco lhe divulga a chave pública dele para que você passe para ele a sua chave simétrica (chave usada na comunicação, ou chave de seção);
- A chave simétrica é criptografada pela chave pública (assimétrica) do banco;
- Assim, somente ele possuidor da chave privada poderá decifrá-la e a partir daí pode-se comunicar seguramente;
- Agora quem garante que aquela chave pública divulgada como se fosse a de um banco seja realmente dele?
- Para resolver isso entra os certificados digitais;
- É um documento eletrônico assinado digitalmente por uma autoridade certificadora, e que contém diversos dados sobre o emissor e o seu titular;
- A função do certificado digital é a de vincular uma pessoa ou uma entidade a uma chave pública.