- **Criptografia**

Código de Chave Pública: está baseado em algoritmos que requerem chaves assimétricas:

- Existem duas chaves distintas, uma pública e outra privada.
- A chave pública fica à disposição de qualquer pessoa e é utilizada para codificar uma mensagem.
- O receptor da mensagem possui a chave privada e será a única pessoa capaz de decodificar a mensagem.

- **Criptografia**

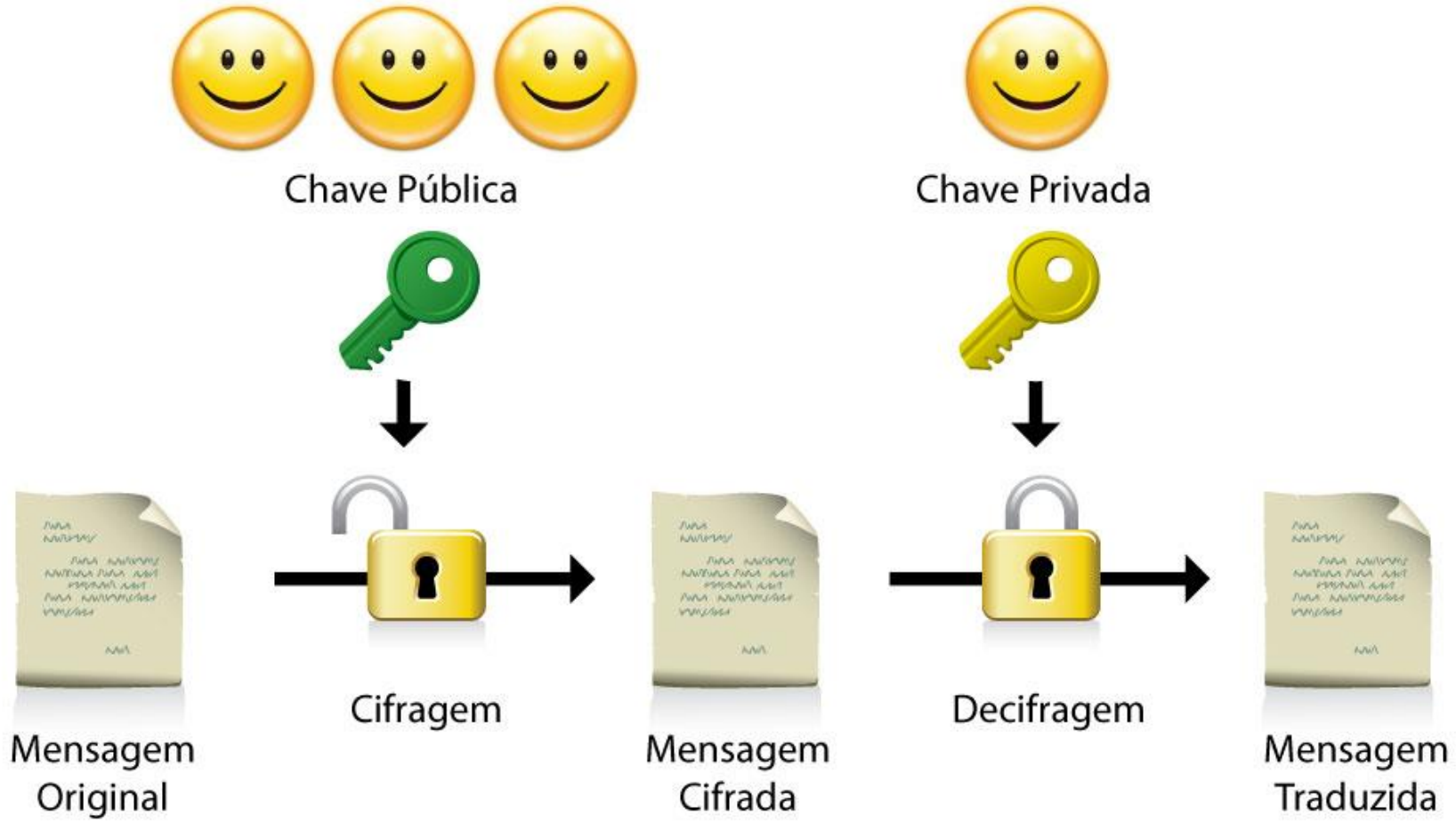
Código de Chave Pública:

❖ O método criptografia mais conhecido de chave pública é o RSA, que foi criado em 1977.

RSA: Iniciais de Rivest, Shamir e Adleman

- **Criptografia RSA**
- Utiliza a teoria dos números para a codificação e decodificação de mensagens.

• Criptografia RSA



Retirado de http://biblioo.info/wp-content/uploads/2012/11/Certifica%C3%A7ao-digital-2.png

- **Criptografia RSA**
- Escolha dois primos distintos muito grandes *p* e *q* (Essa informação é mantida em segredo)
- Calcule $n = p.q$ (*n* é a chave pública)
- Para codificar a mensagem use *n*
- Para decodificar a mensagem use *p* e *q*
- Quebrar o RSA consiste em fatorar *n*, que leva muito tempo se *n* for grande.

- **Criptografia RSA**
- **Exemplo:** Você está implementando ó RSA para uma loja, a loja possui a informação dos números primos *p* e *q*. Quando um cliente compra na loja via web, o computador da loja envia para o computador do cliente a chave *n* para poder codificar os dados do cartão de crédito e enviá-los para o computador da loja.

- **Criptografia RSA: Método**
- Escolha p e q, faça:
  - $n = p.q$
  - $\phi(n) = (p-1)(q-1)$
- Escolha e um número inteiro tal que:
  - $e < \phi(n)$
  - $mdc\big(e, \phi(n)\big) = 1$
  - Então existe $d < \phi(n)$ tal que $1 = k\phi(n) + de$
- A chave de codificação será (e, n) e de decodificação (d, n)

- **Codificação**
- Primeira etapa é a pré-codificação, em que as letras são convertidas em números. Para isso, usaremos a seguinte tabela:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

- **Codificação**

Paraty é linda

25102710293499149921182231310

- **em que 99 significa os espaços entre as palavras.**

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	33	34

- **Codificação**
- Último passo da pré-codificação é separar o número obtido em blocos, os quais devem ter números menores que *n*
- Escolhendo $p = 11$ e $p = 13$, então $n = 11 * 13 = 143$
- Então, **25102710293499149921182313 10** pode ser quebrado em blocos: **25-102-7-102-93-49-91-49-92-118-23-13-10**

❖Existem várias maneiras de quebrar em blocos, o único cuidado deve ser evitar que o bloco comece com *0*

- **Codificação**

- A chave de codificação será (e, n) tal que $mdc\big(e, \phi(n)\big) = 1$

Logo,

$n = 11 * 13 = 143$, $\phi(n) = (10)(12) = 120$. O menor valor para e é *7.*

Cada bloco **b** será codificado da seguinte forma:

- **Codificação**

Cada bloco **b** será codificado da seguinte forma:

C(b)=resto da divisão de b^e por n

Para codificar **25-102-7-102-93-49-91-49-92-118-23-13-10** podemos usar algumas ferramentas computacionais (Matlab, Wolfram)

$$C(25) = mod\,(25^7, 143) = 64$$
$$C(102) = mod\,(102^7, 143) = 119$$
$$C(7) = mod\,(7^7, 143) = 6\ \ldots$$

Obtendo: 64-119-6-119-102-36-130-36-27-79-23-117-10

- **Decodificação**
- 64-119-6-119-102-36-130-36-27-79-23-117-10

$\phi(143) = (10)(12) = 120$ e $e = 7$

- A chave de decodificação será (d, n) tal que $1 = k\phi(n) + de$
- Determinemos quem é *d:* $1 = k.120 + d.7$, dividindo 120 por 7, temos
- $120 = 7 * 17 + 1$, logo $1 = 120 + (-17) * 7$
- Como d é positivo, então fazemos $d = 120 - 17 = 103$
- A chave de decodificação será (103,143)

- **Decodificação**
- Definindo: D(a) = resto da divisão de $a\hat{}d$ por n

$D(64) = mod(64^{103}, 143) = 25$ ...

- Dessa forma, voltaremos a mensagem inicial:

25-102-7-102-93-49-91-49-92-118-23-13-10

- **Decodificação**

25-102-7-102-93-49-91-49-92-118-23-13-10

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	33	34

Paraty é linda