- **Criptografia**

Atualmente, os fatores primos de números monstruosos são usados como chave de criptografia. Esses fatores primos, quando são descobertos, são guardados a ‘’sete chaves’’, pois fazem parte da segurança nacional de muitos países.

- **Criptografia**

Criptografia: do grego *cryptos* que significa secreto, oculto.

Criptografia estuda métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la

- **Criptografia**

Código de César: Consiste em substituir uma letra do alfabeto pela seguinte.

Exemplo: DSJQUPHSBGJB

Um código semelhante a esse foi utilizado pelo ditador romano Júlio César (100-44 a.C.) para se comunicar com as legiões romanas.

- **Criptografia**

Código de César: é fácil de quebrar

❖Qualquer código que envolva substituir cada letra por um outro símbolo sofre do mesmo problema, pois a frequência média com que cada letra aparece em um texto de uma dada língua é mais ou menos constante.

• Criptografia

Tabela de frequência média de cada letra na língua portuguesa:

Letra	%	Letra	%	Letra	%	Letra	%
A	14,64	**G**	1,30	**N**	5,05	**T**	4,34
B	1,04	**H**	1,28	**O**	10,73	**U**	4,34
C	3,88	**I**	6,18	**P**	2,52	**V**	1,70
D	4,1	**J**	0,40	**Q**	1,20	**X**	0,21
E	12,57	**L**	2,78	**R**	6,53	**Z**	0,47
F	1,02	**M**	4,75	**S**	7,81		

- **Criptografia**

❖ **Para quebrar este tipo de código, basta contar o número de vezes que cada símbolo aparece.**

❖ **Entretanto, funciona apenas se a mensagem for longa.**

Exemplo: “Zuza zoou da Zezé”. O Z corresponde a 35% da mensagem.

- **Criptografia**

Códigos em Bloco: Consiste em dividir a mensagem em blocos de várias letras e embaralhamos estes blocos.

Codificar “FUNDAMENTOS DE MATEMATICA” usando o seguinte algoritmo.

- **Criptografia**

Códigos em Bloco:

- Elimine os espaços entre as palavras: FUNDAMENTOSDEMATEMATICA
- Se o número de letras for ímpar, acrescente um A no final: FUNDAMENTOSDEMATEMATICAA
- Divida a mensagem em blocos de duas letras: FU ND AM EM TO SD EM AT EM AT IC AA
- Reflita cada bloco: UF DN MA ME OT DS ME TA ME TA CI AA
- Permute os blocos trocando o primeiro com o último, o terceiro com o antepenúltimo e assim por diante. Os demais mantém

AA ND AT EM AT SD EM TO EM AM IC FU

- **Criptografia**

Códigos em Bloco:

❖ Em transações feitas pela web, esse código não é eficiente. Para o computador receptor saber como a mensagem foi codificada, é necessário que haja uma comunicação entre o computador que envia a mensagem e o que recebe a mensagem.

❖Neste caso a mensagem pode ser interceptada

- **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**

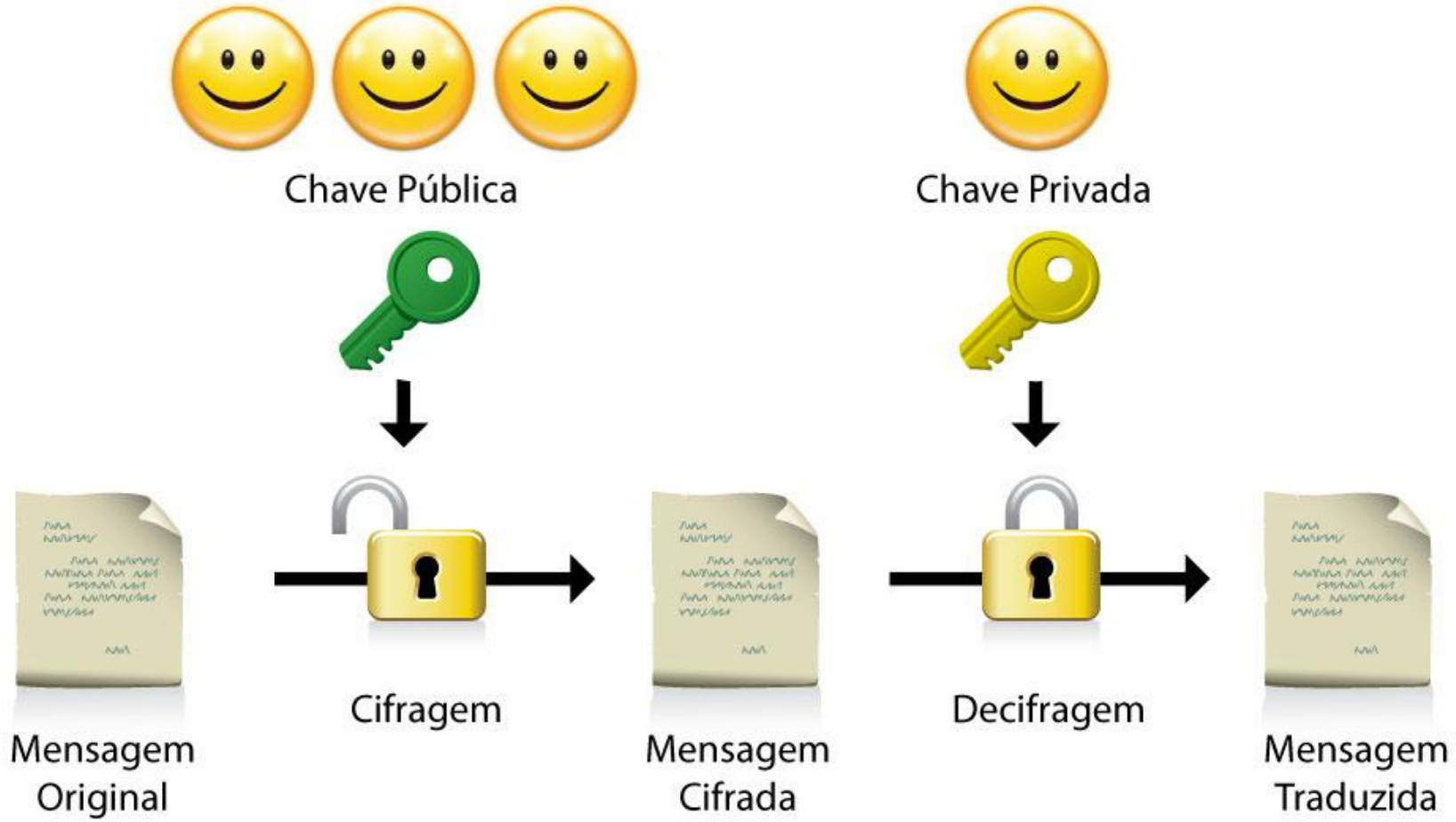
Código de Chave Pública:

❖ 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

• Aplicações de congruência

Sistema de identificação

- Em qualquer texto, um erro de ortografia numa palavra pode ser facilmente percebido, pois ou a palavra não faz parte do idioma ou não faz sentido com o contexto.
- Por exemplo, se digitamos engenheior, logo percebemos que fizemos uma inversão das duas últimas letras. Mas, quando isso ocorre com os algarismos de um número, de um código de identificação qualquer, não teríamos como perceber a troca num simples olhar.
- Para isso e também para minimizar fraudes, foram criados os chamados **dígitos de controle** ou **verificação**. Tais dígitos são normalmente baseados na noção de congruência que mostramos anteriormente.

- **Aplicações de congruência**

Exemplos de dígitos de controle usados como identificadores

1) ISBN

- Um dos exemplos mais antigos é o sistema **International Standard Book Number (ISBN)** de catalogação de livros, CD-Roms e publicações em braile, que foi criado em 1969. A necessidade que as editoras têm de catalogar os seus livros e informatizar o sistema de encomendas serviu de motivação na geração desse código.
- A vantagem é que, por ser um código numérico, ultrapassa as dificuldades geradas pelos diversos idiomas do mundo, bem como a grande diversidade de alfabetos existentes. Dessa forma, poderíamos, por exemplo, identificar através do ISBN um livro japonês.

- **Aplicações de congruência**

1) ISBN

- Em tal sistema, as publicações são identificadas através de 10 algarismos, sendo que o último (dígito de controle) é calculado através da aritmética modular envolvendo operações matemáticas com os outros nove dígitos.
- Esses nove primeiros dígitos são sempre subdivididos em 3 partes, de tamanho variável, separadas por hífen, que transmitem informações sobre o país, editora e sobre o livro em questão.

- **Aplicações de congruência**

1) ISBN

- Vejamos um exemplo:

Na contracapa do livro Temas e Problemas Elementares, da Coleção Professor de Matemática, da SBM, temos o seguinte código do ISBN: 85-85818-29-8. Vejamos o cálculo do dígito de controle que, como estamos observando, é igual a 8.

- **Aplicações de congruência**

1) ISBN

8	5	8	5	8	1	8	2	9
10	9	8	7	6	5	4	3	2

Efetuando as multiplicações correspondentes e somando os produtos obtidos, teremos:

$$8 . 10 + 5 . 9 + 8 . 8 + 5 . 7 + 8 . 6 + 1 . 5 + 8 . 4 + 2 . 3 + 9 . 2 =$$

$$= 80 + 45 + 64 + 35 + 48 + 5 + 32 + 6 + 18 = 333$$

$$333 \equiv 3 (\mathrm{mod}\ 11)$$

- **Aplicações de congruência**

1) ISBN

Para obtermos um múltiplo de 11, ao acrescentarmos o décimo algarismo, o menor valor que atende a tal condição será o número 8, pois 11 – 3 = 8. O que confere o valor apresentado no código dado. Isso significa dizer que 333 + 8 = 341 é um múltiplo de 11, ou ainda, que $341 \equiv 0 \pmod{11}$.

- **Aplicações de congruência**

1) ISBN

Exercício 12: O livro Matemática Aplicada à Administração, Economia e Contabilidade, da Editora Thompson, tem o seguinte código ISBN 85-221-0399-X

Qual o seu dígito de controle X?

- **Aplicações de congruência**

1) ISBN

Exercício 12:

Solução:

8	5	2	2	1	0	3	9	9
10	9	8	7	6	5	4	3	2

Efetuando a soma dos produtos correspondentes, teremos:

80 + 45 + 16 + 14 + 6 + 0 + 12 + 27 + 18 = 218

$$218 \equiv 9 \ (mod\ 11)$$

Dessa forma, o dígito de controle será igual a 2 (11 – 9 = 2).

- **Aplicações de congruência**

1) ISBN

Observação:

Os dois livros que usamos como exemplo tem o prefixo 85, que identifica livros publicados no Brasil.

Vejamos um livro de outro país.

- **Aplicações de congruência**

1) ISBN

Exercício 13: O livro “Hilbert”, de Constance Reid, publicado em alemão (Berlim), tem o seguinte código ISBN: 3-540-04999-Y.

Qual é o valor de Y, isto é, qual é o seu dígito de controle?

- **Aplicações de congruência**

1) ISBN

Exercício 13:

Solução:

3	5	4	0	0	4	9	9	9
10	9	8	7	6	5	4	3	2

Efetuando a soma dos produtos correspondentes, teremos:

30 + 45 + 36 + 0 + 0 + 20 + 36 + 27 + 18 = 208

$$208 \equiv 10 \ (mod \ 11)$$

Dessa forma, o dígito de controle será igual a 1 (11 – 10 = 1).

- **Aplicações de congruência**

1) ISBN

Observação:

- No ISBN, se o dígito for igual a 10 (no caso do resto da divisão por 11 ser igual a 1), é usada a representação do 10 em algarismos romanos, ou seja usa-se um X.
- Desde janeiro de 2007 os códigos do ISBN passaram a ser representados com 13 dígitos. No caso dos livros editados no Brasil há um acréscimo dos dígitos 978 antes do 85.

- **Aplicações de congruência**

2) Código de barra EAN-13

Um dos códigos de barras mais usados no mundo todo é o EAN-13 (EAN - European Article Number), que é constituído de 13 algarismos:

- 3 primeiros dígitos referem-se ao país de registro do produto (produtos brasileiros começam com: 789)
- 4 algarismos seguintes referem-se a empresa fabricante do produto
- 5 algarismos referem-se ao produto do fabricante
- 13º dígito é o código de segurança ou dígito de controle.

- **Aplicações de congruência**

2) Código de barra EAN-13

- O dígito de controle é definido usando a congruência módulo 10 e os fatores que compõem a base de multiplicação são os dígitos 1 e 3, que vão se repetindo da esquerda para a direita.

- **Aplicações de congruência**

2) Código de barra EAN-13

Exemplo:

Numa embalagem de uma garrafa para bebidas, de Portugal, temos o seguinte código de barras: 978294019961

Vamos efetuar os cálculos para a determinação do dígito de controle

- **Aplicações de congruência**

2) Código de barra EAN-13

Exemplo:

9	7	8	2	9	4	0	1	9	9	6	1
1	3	1	3	1	3	1	3	1	3	1	3

(esta é a base de multiplicação)

Efetuando os produtos, temos:

9 + 21 + 8 + 6 + 9 + 12 + 0 + 3 + 9 + 27 + 6 + 3 = 107

$$107 \equiv 7(mod\ 10)$$

Logo, o dígito de controle será igual a 3, pois 10 –7 = 3.

Note que 107 + 3 = 110, que é múltiplo de 10.

- **Aplicações de congruência**

3) CPF: Cadastro de pessoas físicas

Outro exemplo importante, do nosso cotidiano: Verificação dos dois dígitos de controle do CPF de uma pessoa:

- O número de CPF de uma pessoa, no Brasil, é constituído de 11 dígitos, sendo um primeiro bloco com 9 algarismos e um segundo, com mais dois algarismos, que são, como no ISBN e nos códigos de barra, dígitos de controle ou de verificação .
- A determinação desses dois dígitos de controle é mais um caso de aplicação da noção de congruência. No caso do CPF, o décimo dígito (que é o primeiro dígito verificador) é o resultado de uma congruência, módulo 11 de um número obtido por uma operação dos primeiros nove algarismos.

- **Aplicações de congruência**

3) CPF: Cadastro de pessoas físicas

Exemplo

- Considere o CPF de uma pessoa com os seguintes 9 primeiros: 235 343 104, determinemos o primeiro dígito de controle.
- Escrevemos os nove primeiros e, abaixo deles, a base de multiplicação com os dígitos de 1 a 9.

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

- **Aplicações de congruência**

3) CPF: Cadastro de pessoas físicas

Exemplo

- Escrevemos os nove primeiros e, abaixo deles, a base de multiplicação com os dígitos de 1 a 9.

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

Efetuando as multiplicações correspondentes, teremos:

2 x 1 + 3 x 2 + 5 x 3 + 3 x 4 + 4 x 5 + 3 x 6 + 1 x 7 + 0 x 8 + 4 x 9 = 116.

116

$$116 \equiv 6 (\mathrm{mod}\ 11)$$

Portanto o primeiro dígito de controle será **6**.

- **Aplicações de congruência**

3) CPF: Cadastro de pessoas físicas

Exemplo

- Determinemos o segundo dígito de controle. Neste caso usamos uma base de multiplicação de 0 a 9

2 3 5 3 4 3 1 0 4 6

0 1 2 3 4 5 6 7 8 9

Efetuando as multiplicações, teremos:

2 x 0 + 3 x 1 + 5 x 2 + 3 x 3 + 4 x 4 + 3 x 5 + 1 x 6 + 0 x 7 + 4 x 8 + 6 x 9 = 145

$$145 \equiv 2 (\mathrm{mod}\ 11)$$

Logo o segundo dígito de controle é **2**.

- **Aplicações de congruência**

3) CPF: Cadastro de pessoas físicas

Exemplo

Portanto o CPF completo é: **235 343 104 62**

- **Aplicações de congruência**

3) CPF: Cadastro de pessoas físicas

Observação:

- Se o resto da divisão fosse 10, ou seja, se o número obtido fosse congruente ao 10, módulo 11, usaríamos, nesse caso, o dígito zero.