0101010101010101
0101010101010101
0011001010101111
0101010101010100
1010101011010101
0101010101010101
0101010101010101
1111100101010101
0101010101010111
1100101010101001
0101010100101010
1111111010010101
0101010100101010
1010100101011110
1010110101110101
0101010101010100
1011111111010010

A Teoria dos Números e sua Aplicação em Criptografia

Prof. Pablo Furlan
Prof. Mário Lemes

Cifra de César

Letras que queremos Cifra	Valor referente a letra	Valor dado após Cifragem	Letra referente ao valo
A	0	3	D
M	11	14	P
A	0	3	D
T	18	21	X
E	4	7	H
M	11	14	P
A	0	3	D
T	18	21	X
I	8	11	M
C	2	5	F
A	0	3	D
E	4	7	H
S	17	20	V
T	18	21	X
A	0	3	D
E	4	7	H
M	11	14	P
T	18	21	X
U	19	22	Z
D	3	6	G
O	13	16	R

Cifra de César (Linear)

Letras que queremos Cifra	Valor referente a letra	Valor dado após Cifragem	Letra referente ao valor
A	0	1	B
M	11	0	A
A	0	1	B
T	18	14	P
E	4	9	J
M	11	0	A
A	0	1	B
T	18	14	P
I	8	17	S
C	2	5	F
A	0	1	B
E	4	9	J
S	17	12	N
T	18	14	P
A	0	1	B
E	4	9	J
M	11	0	A
T	18	14	P
U	19	16	R
D	3	7	H
O	13	4	E

Criptografia RSA

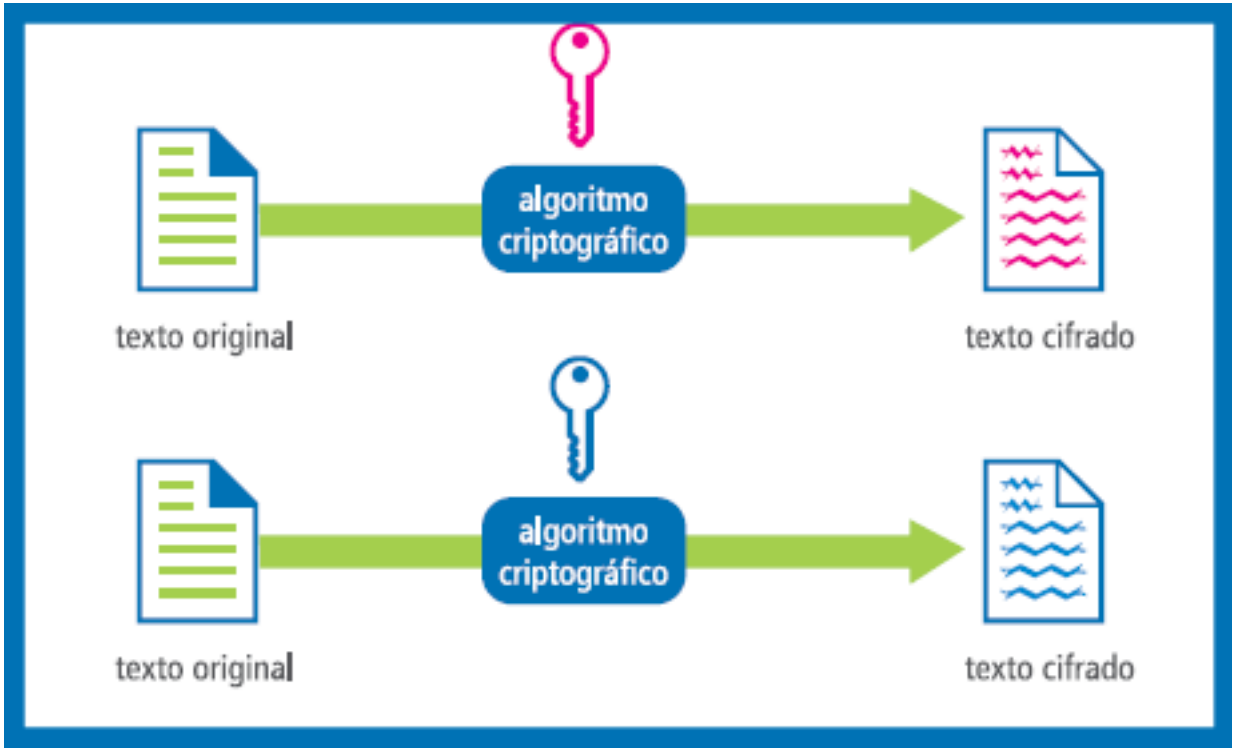
Letras que queremos Cifrar	Valor referente a letra	Valor dado após Cifragem
A	0	0
M	11	33
A	0	0
T	18	83
E	4	49
M	11	33
A	0	0
T	18	83
I	8	112
C	2	84
A	0	0
E	4	49
S	17	140
T	18	83
A	0	0
E	4	49
M	11	33
T	18	83
U	19	2
D	3	9
O	13	117

Decriptografia RSA

Valores que queremos Decifra	Valores decifrados	etras referentes a esses valore
0	0	A
33	11	M
0	0	A
83	18	T
49	4	E
33	11	M
0	0	A
83	18	T
112	8	I
84	2	C
0	0	A
49	4	E
140	17	S
83	18	T
0	0	A
49	4	E
33	11	M
83	18	T
2	19	U
9	3	D
117	13	O

CONCEITOS DE CRIPTOGRAFIA

Chave Privada ou Chave Simétrica



CONCEITOS DE CRIPTOGRAFIA

Chave Pública ou Chave Assimétrica

- Na década de 70 surgiu um novo método criptográfico, o chamado algoritmo assimétrico de criptografia.

- A idéia foi criada por Diffie e Hellman e colocada em prática com o desenvolvimento do RSA.

CONCEITOS DE CRIPTOGRAFIA

Chave Pública ou Chave Assimétrica

- Algoritmos com Chave Assimétrica possuem duas chaves distintas: uma privada (secreta) e uma pública.
- A Chave Pública é livre para ser repassada para qualquer pessoa (ou máquina), independente de participar ou não da comunicação.
- Já a chave privada deve ser secreta e ficar apenas em poder da origem.

CONCEITOS DE CRIPTOGRAFIA

Chave Pública ou Chave Assimétrica

- Aquilo que for encriptado com a chave pública pode ser decriptado apenas com a chave privada e vice-versa.

- Os algoritmos criptográficos de chave pública permitem garantir tanto a confidencialidade quanto a autenticidade das informações por eles protegidas.

CONCEITOS DE CRIPTOGRAFIA

Chave Pública ou Chave Assimétrica

- **Confidencialidade**

CONCEITOS DE CRIPTOGRAFIA

Chave Pública ou Chave Assimétrica

- **Autenticidade**

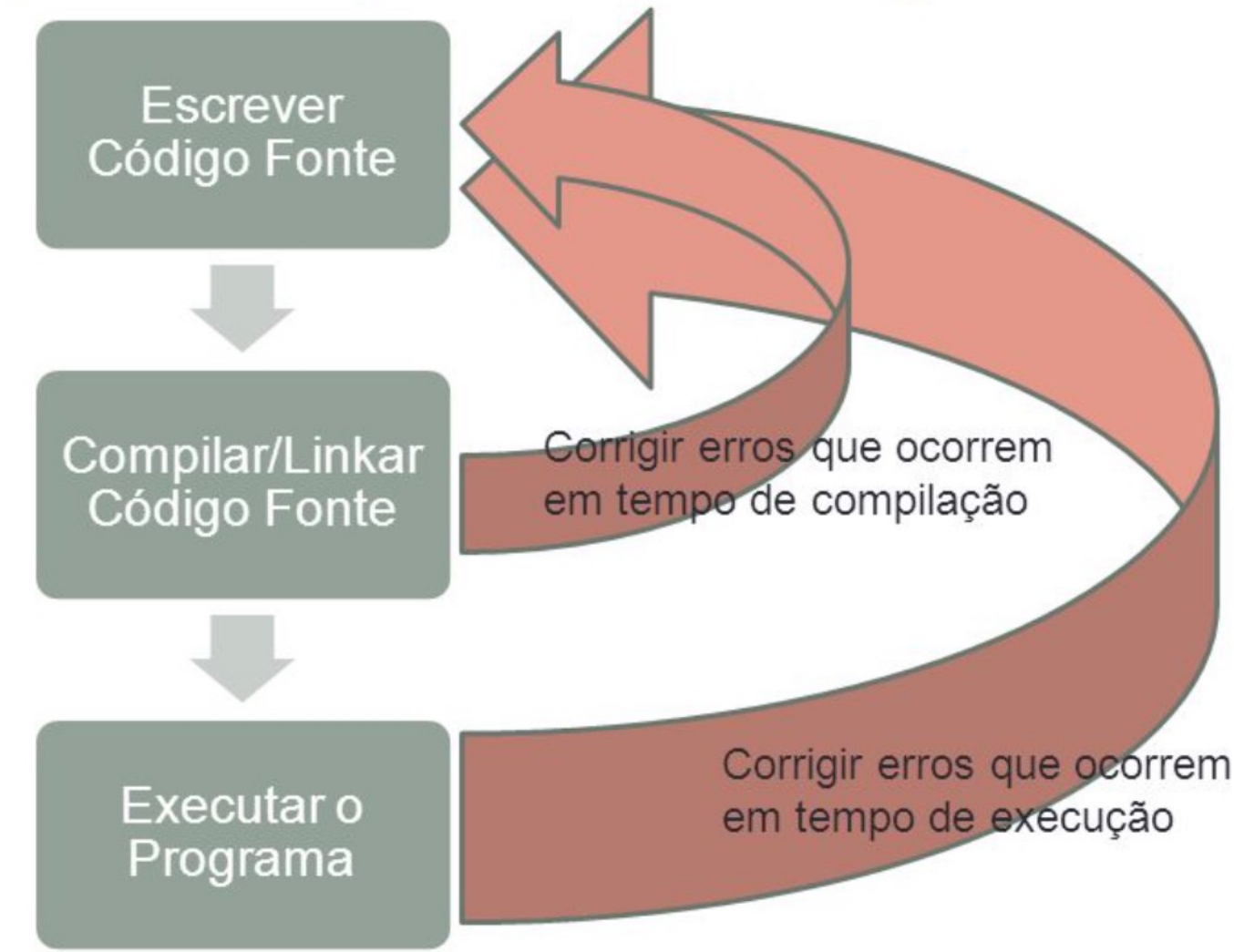
Implementação Computacional da Cifra de César e do RSA

O QUE É LINGUAGEM DE PROGRAMAÇÃO?

Uma linguagem de programação é um método padronizado para comunicar instruções para um computador. É um conjunto de regras sintáticas e semânticas usadas para definir um programa de computador

O QUE É LINGUAGEM DE PROGRAMAÇÃO?

COMPILAR & EXECUTAR



VAMOS DAR UMA OLHADA NO PROGRAMA QUE REALIZA A CIFRA DE CÉSAR?

```
55
56  int main( int argc, char * argv[] )
57  {
58      char original[] = "A matematica esta em tudo";
59
60      char cifrado[100] = {0};
61      char decifrado[100] = {0};
62
63      //cifra o texto original com a chave 3
64      cifrar( cifrado, original, 3 );
65
66      //decifra o texto cifrado com a chave 3
67      decifrar( decifrado, cifrado, 3 );
68
69      printf( "Original: %s\n", original );
70      printf( "Cifrado: %s\n", cifrado );
71      printf( "Decifrado: %s\n", decifrado );
72
73      return 0;
74  }
75
```

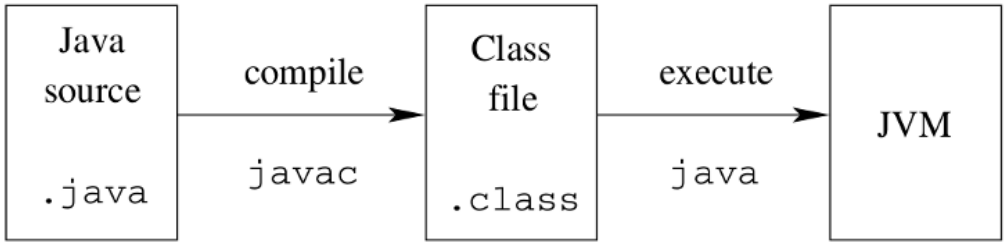
COMO EXECUTAR PROGRAMAS EM C?

(Compilar):
$ gcc nomedoprograma.c –o nomedoprograma

(Executar):
$ ./nomedoprograma

VAMOS DAR UMA OLHADA NO PROGRAMA QUE REALIZA A CRIPTOGRAFIA RSA?

COMO EXECUTAR PROGRAMAS EM JAVA?



(Compilar):
$ javac nomedoprograma.java

(Executar):
$ java nomedoprograma

```java
/**
 * Criptografa o texto puro usando chave pública.
 */
public static byte[] criptografa(String texto, PublicKey chave) {
  byte[] cipherText = null;

  try {
    final Cipher cipher = Cipher.getInstance(ALGORITHM);
    // Criptografa o texto puro usando a chave Púlica
    cipher.init(Cipher.ENCRYPT_MODE, chave);
    cipherText = cipher.doFinal(texto.getBytes());
  } catch (Exception e) {
    e.printStackTrace();
  }

  return cipherText;
}

/**
 * Decriptografa o texto puro usando chave privada.
 */
public static String decriptografa(byte[] texto, PrivateKey chave) {
  byte[] dectyptedText = null;

  try {
    final Cipher cipher = Cipher.getInstance(ALGORITHM);
    // Decriptografa o texto puro usando a chave Privada
    cipher.init(Cipher.DECRYPT_MODE, chave);
    dectyptedText = cipher.doFinal(texto);

  } catch (Exception ex) {
    ex.printStackTrace();
  }

  return new String(dectyptedText);
}
```

```
     */
    public static void main(String[] args) {

      try {

        // Verifica se já existe um par de chaves, caso contrário gera-se as chaves..
        if (!verificaSeExisteChavesNoSO()) {
         // Método responsável por gerar um par de chaves usando o algoritmo RSA e
         // armazena as chaves nos seus respectivos arquivos.
          geraChave();
        }

        final String msgOriginal = "Teste de Mensagem";
        ObjectInputStream inputStream = null;

        // Criptografa a Mensagem usando a Chave Pública
        inputStream = new ObjectInputStream(new FileInputStream(PATH_CHAVE_PUBLICA));
        final PublicKey chavePublica = (PublicKey) inputStream.readObject();
        final byte[] textoCriptografado = criptografa(msgOriginal, chavePublica);

        // Decriptografa a Mensagem usando a Chave Privada
        inputStream = new ObjectInputStream(new FileInputStream(PATH_CHAVE_PRIVADA));
        final PrivateKey chavePrivada = (PrivateKey) inputStream.readObject();
        final String textoPuro = decriptografa(textoCriptografado, chavePrivada);

        // Imprime o texto original, o texto criptografado e
        // o texto decriptografado.
        System.out.println("Mensagem Original: " + msgOriginal);
        System.out.println("Mensagem Criptografada: " +textoCriptografado.toString());
        System.out.println("Mensagem Decriptografada: " + textoPuro);

      } catch (Exception e) {
        e.printStackTrace();
      }
    }
  }
```

FIM