Modelo simplificado do cifrador IDEA

Henrique Tomasi Pires
Paulo Fernando da Silva

FURB

Roteiro

- Introdução
- Objetivos
- Fundamentação teórica
- Desenvolvimento
- Conclusões

FURB

Introdução

- Segurança da informação
  - Dados locais
  - Transmissão de dados
- Criptografia
  - Avanço computacional
- Cifradores
  - DES
  - Substituto do DES
  - IDEA

FURB

Objetivos

- Especificar um modelo simplificado do cifrador IDEA
- Implementar um modelo simplificado do cifrador IDEA
- Facilitar a compreensão do IDEA

Objetivos específicos

- Propor um protótipo sem descaracterizar as propriedades matemáticas
- Expor os mecanismos do IDEA
- Identificar pontos de redução
- Disponibilizar versão didática do protótipo
- Servir como referência

FURB

Segurança da informação

FURB

Criptografia

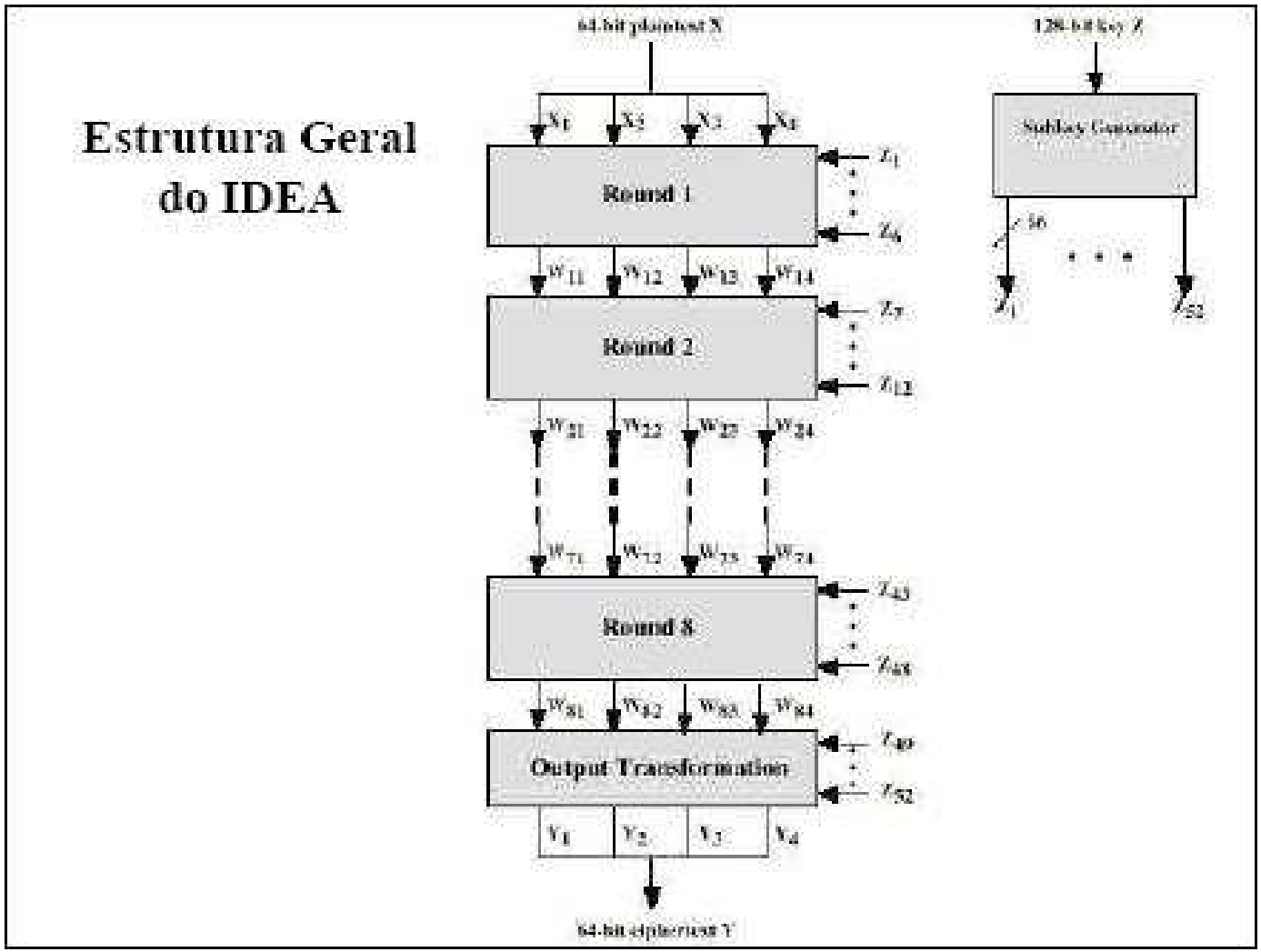
- Simétrica
  - Cifrador de streaming
  - Cifrador de bloco
- Assimétrica
  - Autenticidade
  - Confidencialidade

Cifrador de bloco

- Substituição
- Permutação
- Cifrador de Feistel
  - Difusão
  - Confusão
- DES
- S-DES

FURB

Cifrador IDEA



Trabalhos correlatos

FURB

Trabalhos correlatos

- Schaefer (1996)
  - DES – S-DES
- Mendes (2001)
  - RC6 – SRC6
- Miers (2002)
  - AES – SAES

Desenvolvimento

FURB

Requisitos

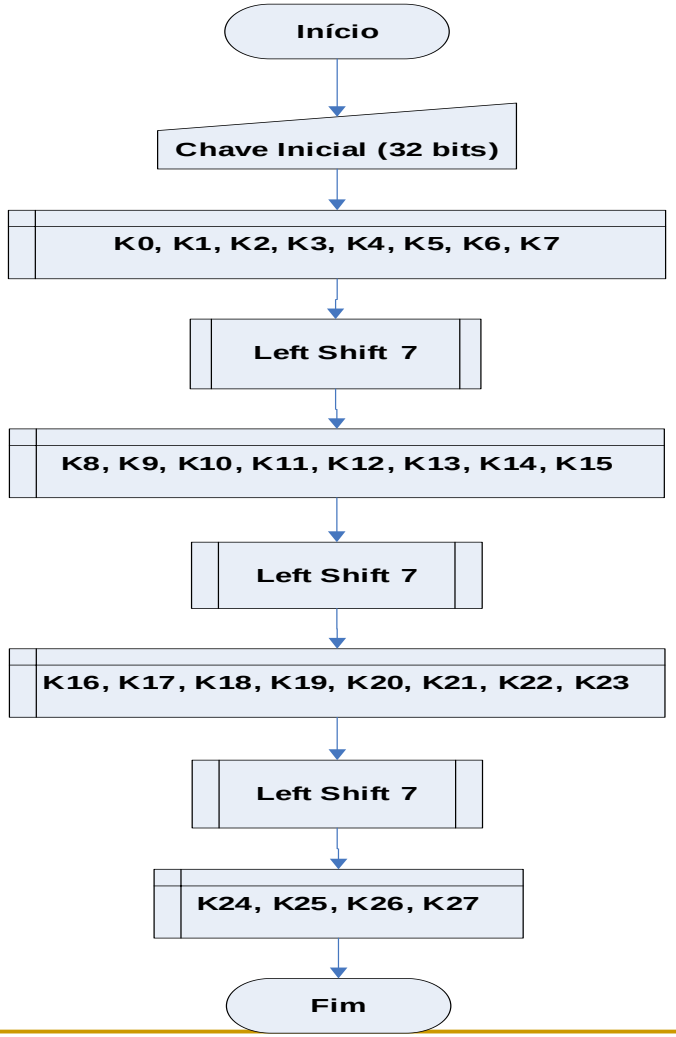
- Funcionais
  - Permitir a implementação manual
  - Cifrar e decifrar textos e dados
- Não Funcionais
  - Requerer baixo requisito de *hardware*
  - Utilizar a linguagem de programação C
  - Utilizar ferramentas e bibliotecas gratuitas
  - Ser de domínio público e estar exposto para estudos

FURB

Especificação

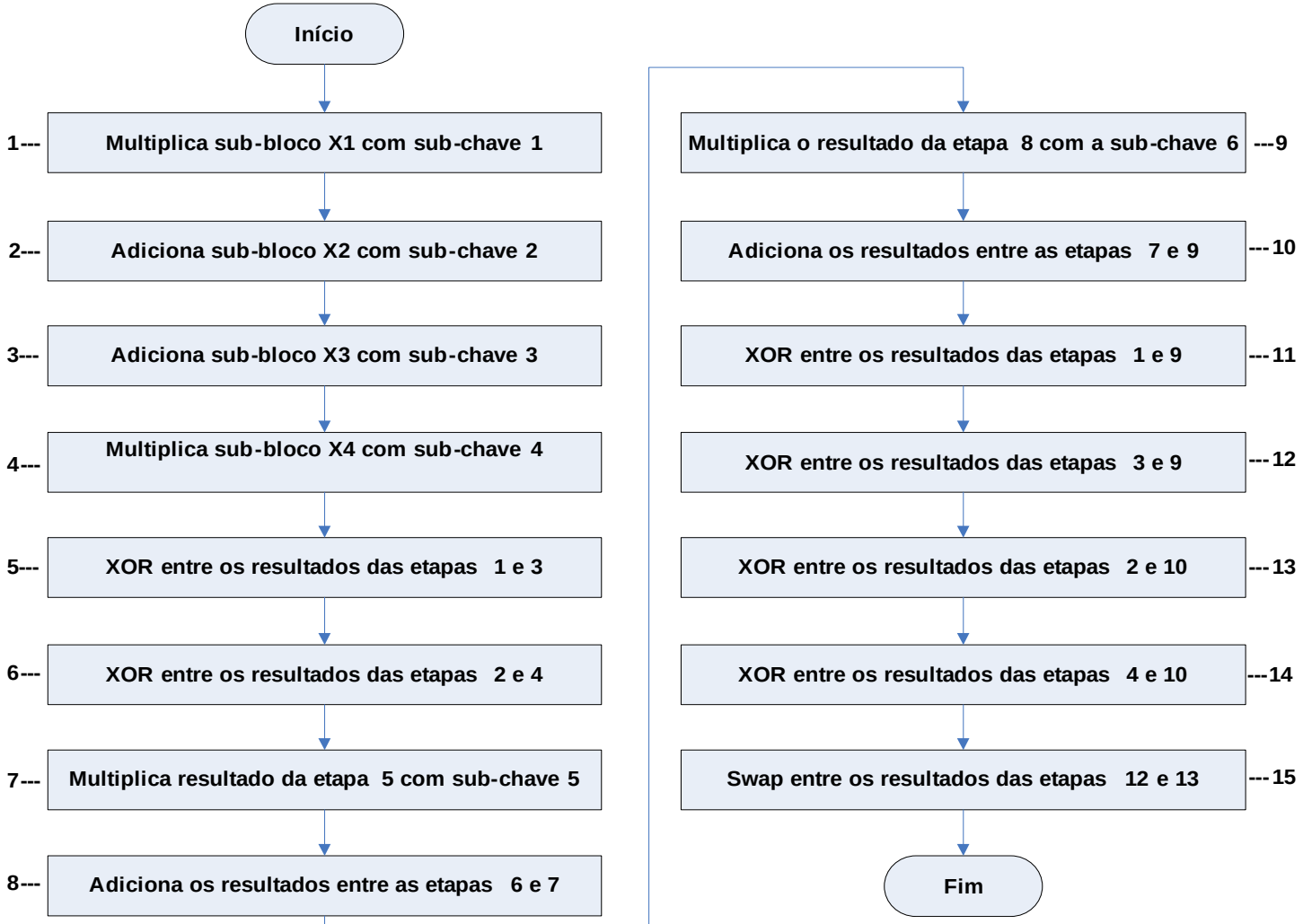
- Metodologia de redução
  - Correlação
- Redução da chave
- Redução do bloco
- Operações matemáticas
  - *Nibbles*

Sub-chaves de encriptação

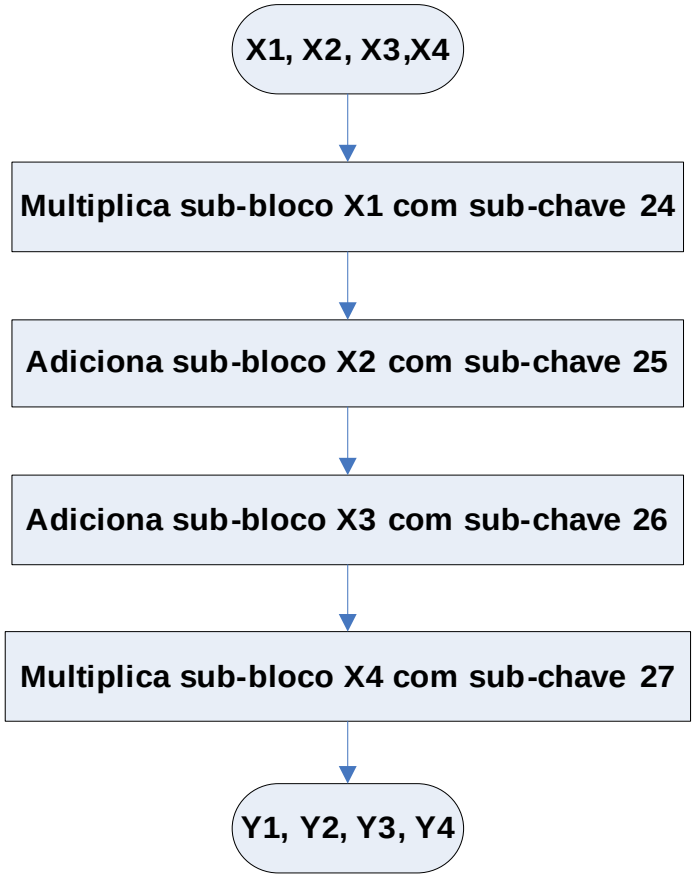


Sub-chaves de decriptação

Rodada


Início
1--- Multiplica sub-bloco X1 com sub-chave 1
2--- Adiciona sub-bloco X2 com sub-chave 2
3--- Adiciona sub-bloco X3 com sub-chave 3
4--- Multiplica sub-bloco X4 com sub-chave 4
5--- XOR entre os resultados das etapas 1 e 3
6--- XOR entre os resultados das etapas 2 e 4
7--- Multiplica resultado da etapa 5 com sub-chave 5
8--- Adiciona os resultados entre as etapas 6 e 7
Multiplica o resultado da etapa 8 com a sub-chave 6 ---9
Adiciona os resultados entre as etapas 7 e 9 ---10
XOR entre os resultados das etapas 1 e 9 ---11
XOR entre os resultados das etapas 3 e 9 ---12
XOR entre os resultados das etapas 2 e 10 ---13
XOR entre os resultados das etapas 4 e 10 ---14
Swap entre os resultados das etapas 12 e 13 ---15
Fim

Transformação final



FURB

Características

Características	IDEA	SIDEA
XOR/Adição/ Multiplicação	SIM	SIM
15 Etapas por rodada	SIM	SIM
Sub-chaves não repetidas	SIM	SIM
Multipl. c/ número primo	SIM	SIM
Divisão s-chave/s-bloco	SIM	SIM
Transformação final	SIM	SIM

FURB

Números

CIFRADORES				
	S-DES	**DES**	**SIDEA**	**IDEA**
Bloco	8 bits	64 bits	16 bits	64 bits
Chave	10 bits	56 bits	32 bits	128 bits
Sub-Chave	8 bits	48 bits	4 bits	16 bits
Rodadas	2	16	4	8

FURB

Implementação

- Ambiente: MS-Windows XP
- Ferramenta: Bloodshed Dev C++ 4.9.8.0
- Linguagem: C-ANSI
- Bibliotecas: Stdio.h, Stdlib.h

Função Cifrar/Decifrar

- *Sidea_cifra*
- Cifra
  - Chave inicial
  - Bloco de entrada (plano)
- Decifra
  - Chave inicial
  - Bloco de entrada (cifrado)

Geração de chaves

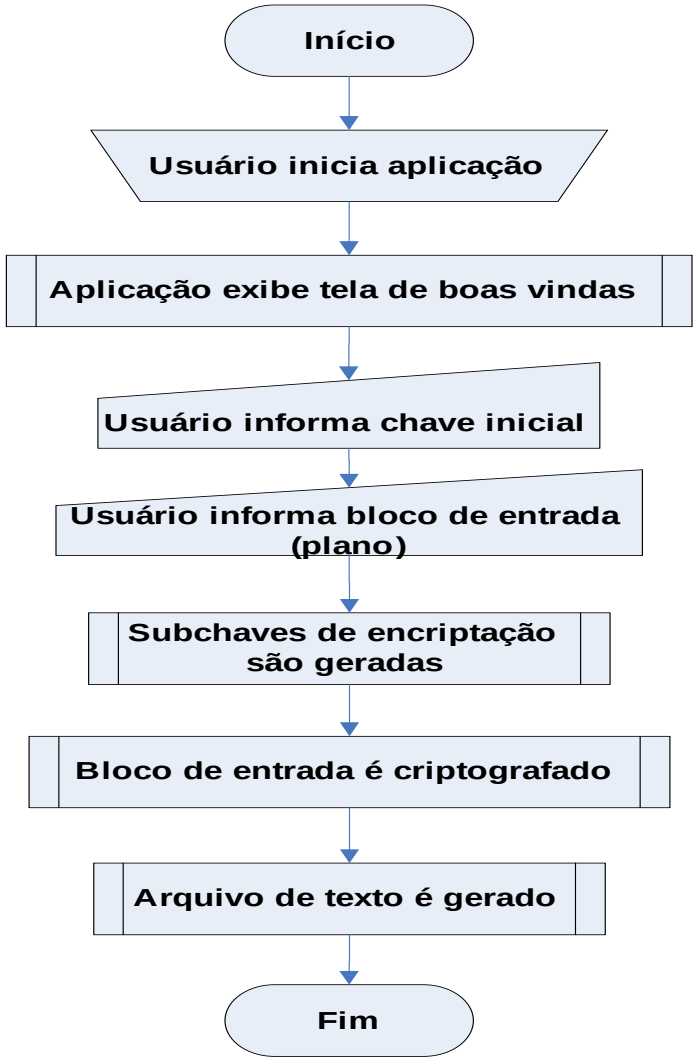
```
void gera_chaves_cifra(){

for (i=0;i<8;i++)
        // Divide a chave inicial de 32 bits em 8 blocos de 4 bits
        key32 = ((chave_entrada[i] & 0x0f) << (4*i)) | key32;

for (i;i<SIDEA_SUBCHAVES;i++) {
        // Deslocamento a esquerda de 7 posicoes
        key32 = i % 8 ? key32 : (key32 << 7) | (key32  >> 25);
        chave_entrada[i] = (key32 << (7-(i%8))*4) >> 28;
   }
printf("\nChaves de encriptacao\n");
for (i=0;i<SIDEA_SUBCHAVES;i++) {
    i % 8 ? printf("\t") : printf("\n");
    printf("0x%x",chave_entrada[i]);
}
printf("\n");
}
```

Operacionalidade

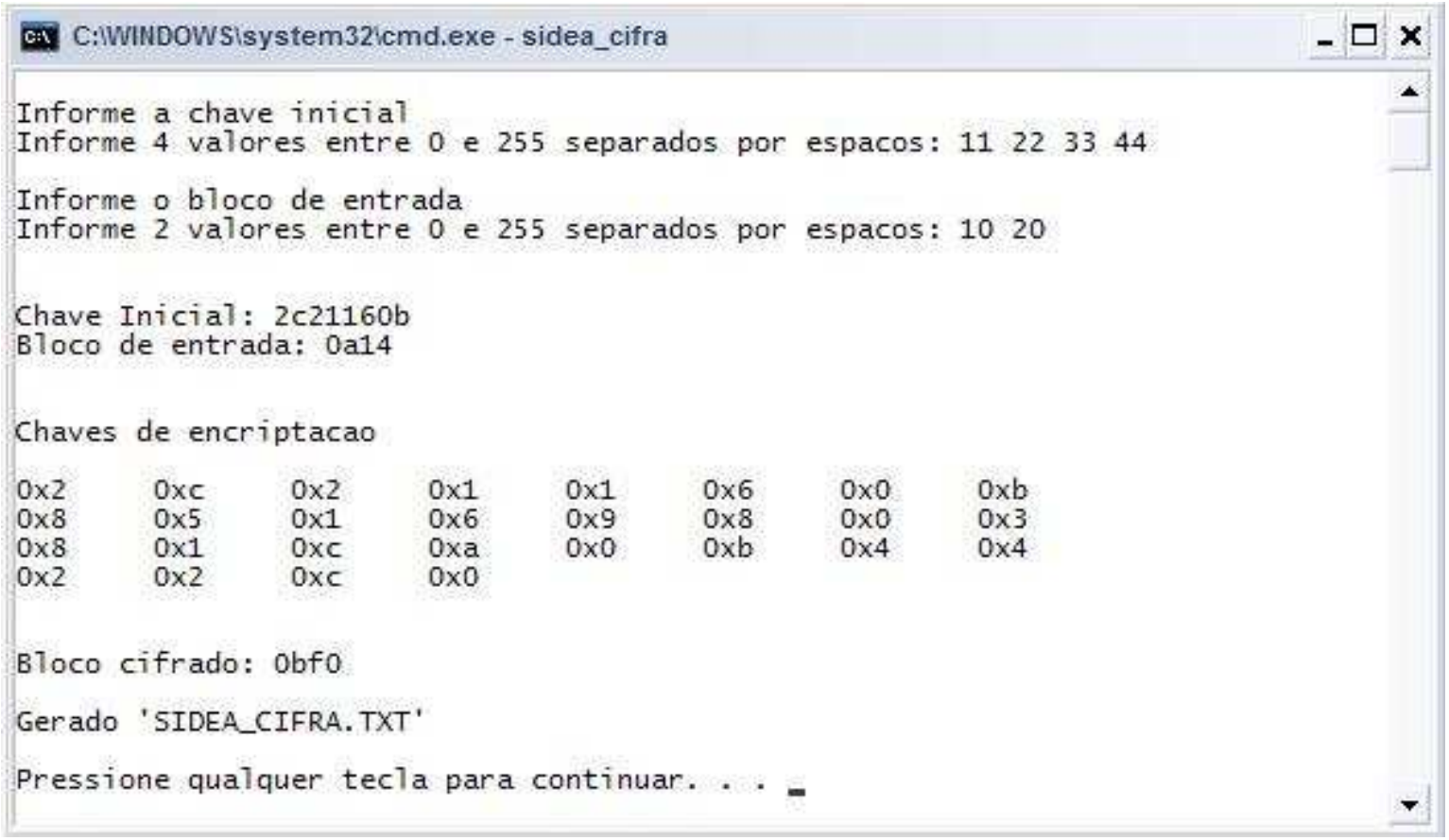
- Sidea_cifra
- Sidea_decifra
- Modo iterativo
- Chave inicial {11, 22, 33, 44}
- Bloco de entrada {10, 20}

FURB

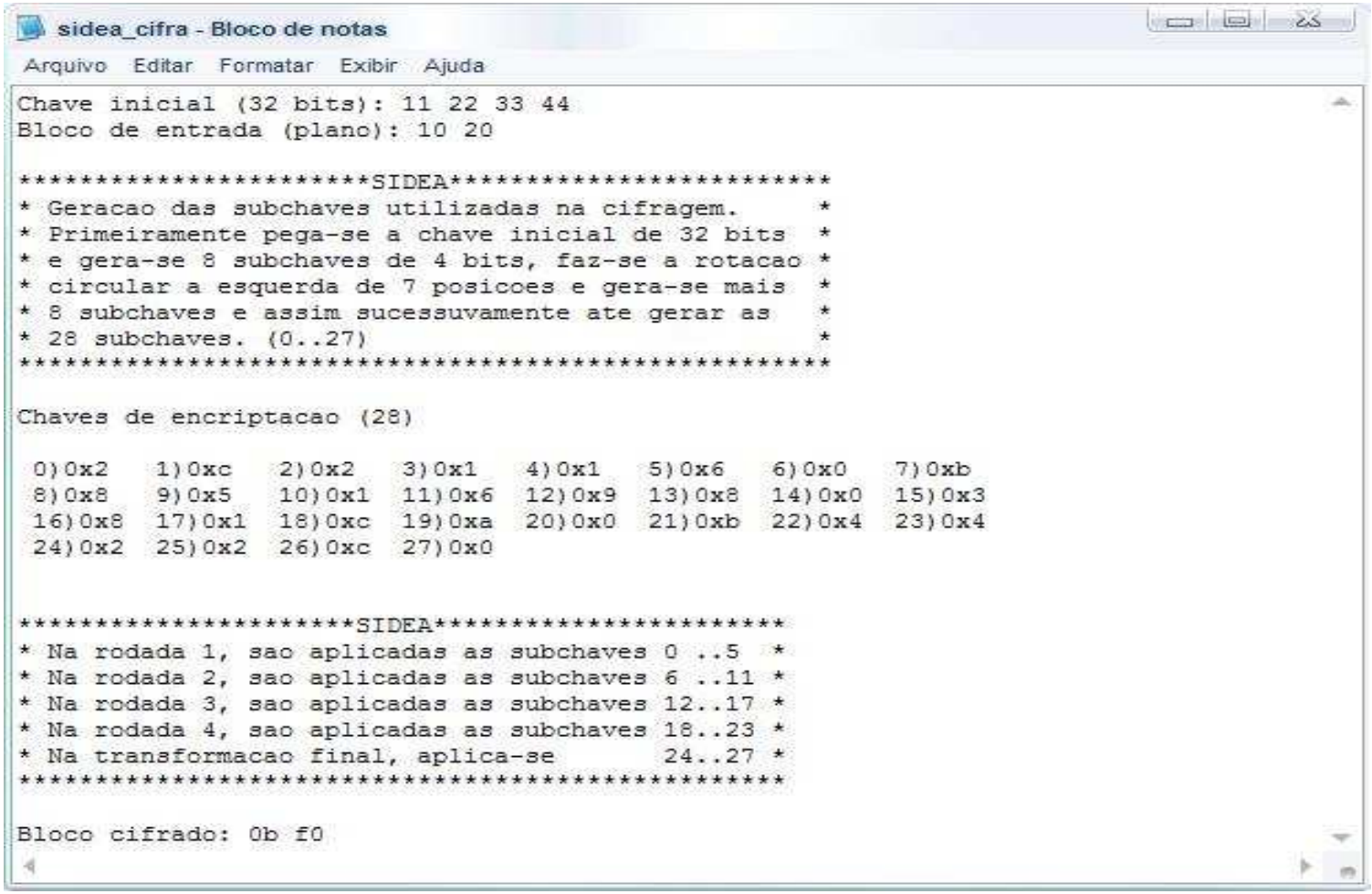
SIDEA - Cifra


Início
Usuário inicia aplicação
Aplicação exibe tela de boas vindas
Usuário informa chave inicial
Usuário informa bloco de entrada (plano)
Subchaves de encriptação são geradas
Bloco de entrada é criptografado
Arquivo de texto é gerado
Fim

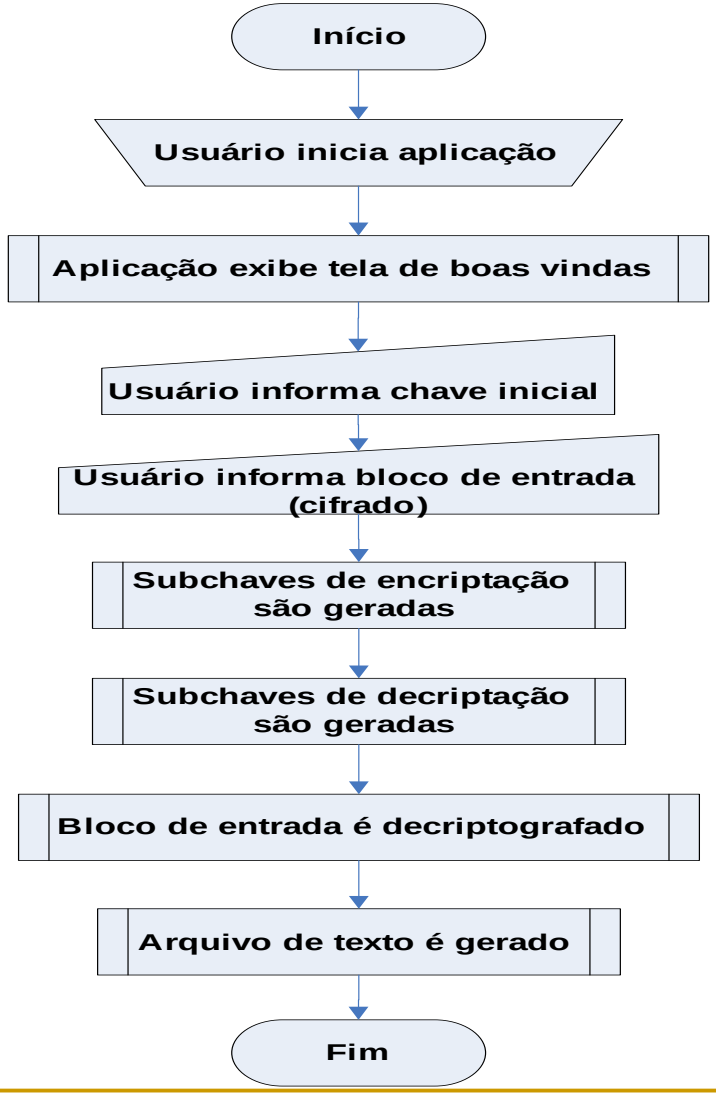
SIDEA - Cifra


C:\WINDOWS\system32\cmd.exe - sidea_cifra
Informe a chave inicial
Informe 4 valores entre 0 e 255 separados por espacos: 11 22 33 44
Informe o bloco de entrada
Informe 2 valores entre 0 e 255 separados por espacos: 10 20
Chave Inicial: 2c21160b
Bloco de entrada: 0a14
Chaves de encriptacao
0x2 0xc 0x2 0x1 0x1 0x6 0x0 0xb
0x8 0x5 0x1 0x6 0x9 0x8 0x0 0x3
0x8 0x1 0xc 0xa 0x0 0xb 0x4 0x4
0x2 0x2 0xc 0x0
Bloco cifrado: 0bf0
Gerado 'SIDEA_CIFRA.TXT'
Pressione qualquer tecla para continuar. . .

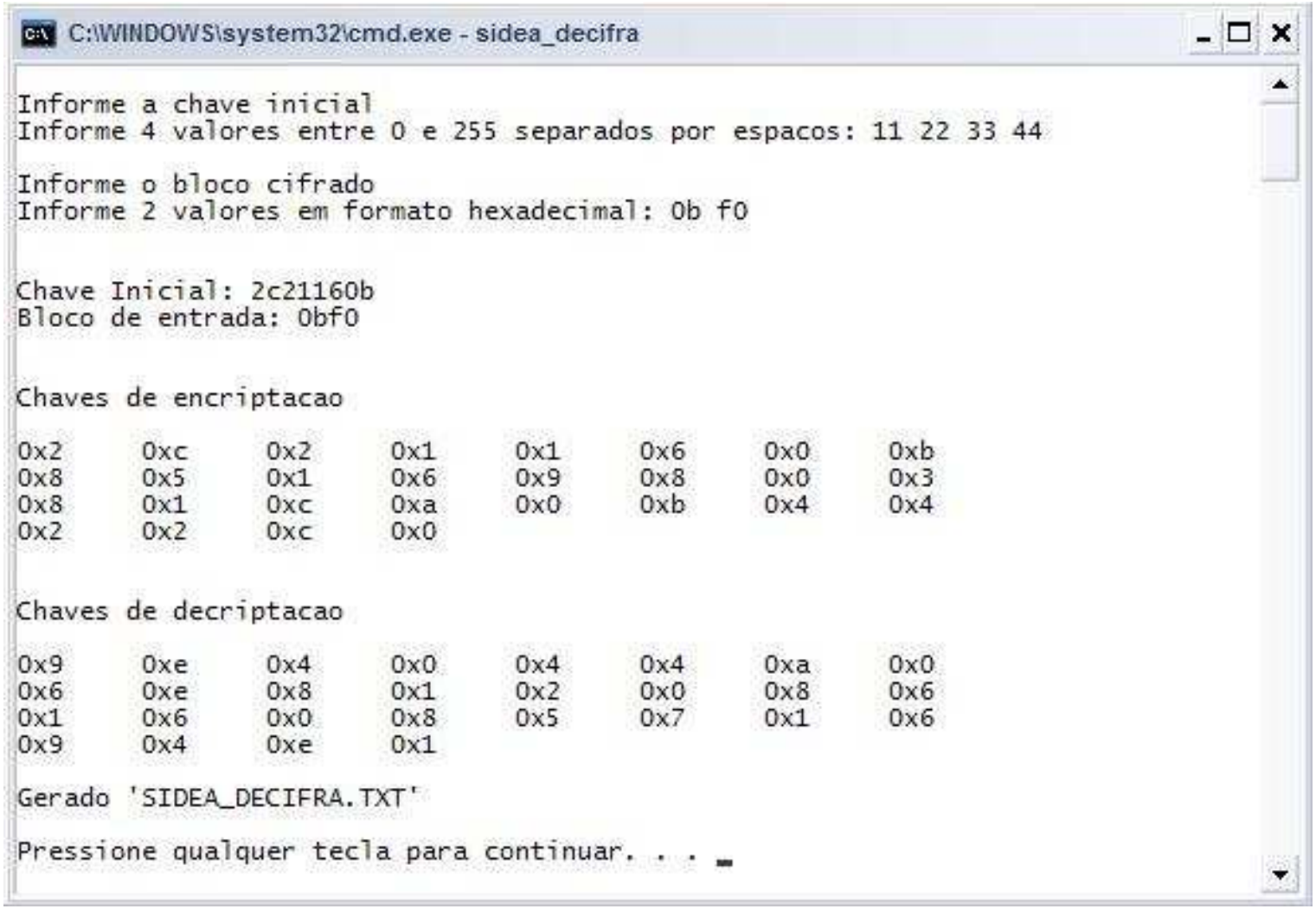
SIDEA - Cifra


sidea_cifra - Bloco de notas
Arquivo Editar Formatar Exibir Ajuda
Chave inicial (32 bits): 11 22 33 44
Bloco de entrada (plano): 10 20
**********SIDEA**********
* Geracao das subchaves utilizadas na cifragem. *
* Primeiramente pega-se a chave inicial de 32 bits *
* e gera-se 8 subchaves de 4 bits, faz-se a rotacao *
* circular a esquerda de 7 posicoes e gera-se mais *
* 8 subchaves e assim sucessuvamente ate gerar as *
* 28 subchaves. (0..27) *
Chaves de encriptacao (28)
0)0x2 1)0xc 2)0x2 3)0x1 4)0x1 5)0x6 6)0x0 7)0xb
8)0x8 9)0x5 10)0x1 11)0x6 12)0x9 13)0x8 14)0x0 15)0x3
16)0x8 17)0x1 18)0xc 19)0xa 20)0x0 21)0xb 22)0x4 23)0x4
24)0x2 25)0x2 26)0xc 27)0x0
**********SIDEA**********
* Na rodada 1, sao aplicadas as subchaves 0 ..5 *
* Na rodada 2, sao aplicadas as subchaves 6 ..11 *
* Na rodada 3, sao aplicadas as subchaves 12..17 *
* Na rodada 4, sao aplicadas as subchaves 18..23 *
* Na transformacao final, aplica-se 24..27 *
Bloco cifrado: 0b f0

SIDEA - Decifra



SIDEA - Decifra



SIDEA - Decifra

Conclusões

FURB

Conclusões

- Objetivos alcançados
  - Versão didática
  - Implementação manual (*nibbles)*
- Protótipo inédito
  - Estudantes e pesquisadores
- Código IDEA
  - Obtenção
  - Entendimento

FURB

Extensões

- Modelos simplificados - IDEA
  - Exploração de falhas
  - Melhora de desempenho
- SIDEA
  - Leitura de arquivos de tamanho qualquer
  - Utilização em sockets (cliente/servidor)

Obrigado !

megamega@inf.furb.br
paulofernando@furb.br

FURB