Criptografia com Maple

LNCC - Verão/2005

Fábio Borges & Renato Portugal

História

- 600 a 500 a.C. – O Livro de Jeremias e Cifras Hebraicas

História

- 600 a 500 a.C. – O Livro de Jeremias e Cifras Hebraicas
- $\pm$ 300 a.C. – Euclides e os Elementos

História

- 600 a 500 a.C. – O Livro de Jeremias e Cifras Hebraicas
- $\pm$ 300 a.C. – Euclides e os Elementos
- 50 a.C. – Código de César

História

- 600 a 500 a.C. – O Livro de Jeremias e Cifras Hebraicas
- $\pm$ 300 a.C. – Euclides e os Elementos
- 50 a.C. – Código de César
- 1586 – Blaise de Vigenère

História

- 600 a 500 a.C. – O Livro de Jeremias e Cifras Hebraicas
- $\pm$ 300 a.C. – Euclides e os Elementos
- 50 a.C. – Código de César
- 1586 – Blaise de Vigenère
- 1948 – Claude Elwood Shannon - Teoria Matemática da Comunicação

História

- 600 a 500 a.C. – O Livro de Jeremias e Cifras Hebraicas
- $\pm$ 300 a.C. – Euclides e os Elementos
- 50 a.C. – Código de César
- 1586 – Blaise de Vigenère
- 1948 – Claude Elwood Shannon - Teoria Matemática da Comunicação
- 1978 – RSA - R. Rivest, A. Shamir e L. Adleman

Necessidade da Criptografia

- Antigamente:

Necessidade da Criptografia

- Antigamente:
  - Diplomacia

Necessidade da Criptografia

- Antigamente:
  - Diplomacia
  - Guerra

Necessidade da Criptografia

- Antigamente:
  - Diplomacia
  - Guerra
  - Amor

Necessidade da Criptografia

- Antigamente:
  - Diplomacia
  - Guerra
  - Amor
- Hoje:

Necessidade da Criptografia

- Antigamente:
  - Diplomacia
  - Guerra
  - Amor
- Hoje:
  - Segurança:

Necessidade da Criptografia

- Antigamente:
  - Diplomacia
  - Guerra
  - Amor
- Hoje:
  - Segurança:
    - Acesso

Necessidade da Criptografia

- Antigamente:
  - Diplomacia
  - Guerra
  - Amor
- Hoje:
  - Segurança:
    - Acesso
    - Dinheiro

Necessidade da Criptografia

- Antigamente:
  - Diplomacia
  - Guerra
  - Amor
- Hoje:
  - Segurança:
    - Acesso
    - Dinheiro
    - Comunicação

Interdisciplinaridade

- Matemática

Interdisciplinaridade

- Matemática
  - Estruturas Algébricas

Interdisciplinaridade

- Matemática
  - Estruturas Algébricas
  - Teoria dos Números

Interdisciplinaridade

- Matemática
  - Estruturas Algébricas
  - Teoria dos Números
  - Probabilidade

Interdisciplinaridade

- Matemática
  - Estruturas Algébricas
  - Teoria dos Números
  - Probabilidade
- Computação

Interdisciplinaridade

- Matemática
  - Estruturas Algébricas
  - Teoria dos Números
  - Probabilidade
- Computação
  - Complexidade Computacional

Interdisciplinaridade

- Matemática
  - Estruturas Algébricas
  - Teoria dos Números
  - Probabilidade
- Computação
  - Complexidade Computacional
  - Software Básico

Interdisciplinaridade

- Matemática
  - Estruturas Algébricas
  - Teoria dos Números
  - Probabilidade
- Computação
  - Complexidade Computacional
  - Software Básico
  - Redes

Interdisciplinaridade

- Matemática
  - Estruturas Algébricas
  - Teoria dos Números
  - Probabilidade
- Computação
  - Complexidade Computacional
  - Software Básico
  - Redes
- Eletrônica, Física, Lingüística...

Terminologia

- Mensagem - Plaintext

Terminologia

- Mensagem - Plaintext
- Chave

Terminologia

- Mensagem - Plaintext
- Chave
- Criptossistema

Terminologia

- Mensagem - Plaintext
- Chave
- Criptossistema
- Criptograma - Ciphertext

Terminologia

- Mensagem - Plaintext
- Chave
- Criptossistema
- Criptograma - Ciphertext
- Criptografia

Terminologia

- Mensagem - Plaintext
- Chave
- Criptossistema
- Criptograma - Ciphertext
- Criptografia
- Criptoanálise

Terminologia

- Mensagem - Plaintext
- Chave
- Criptossistema
- Criptograma - Ciphertext
- Criptografia
- Criptoanálise
- Criptologia

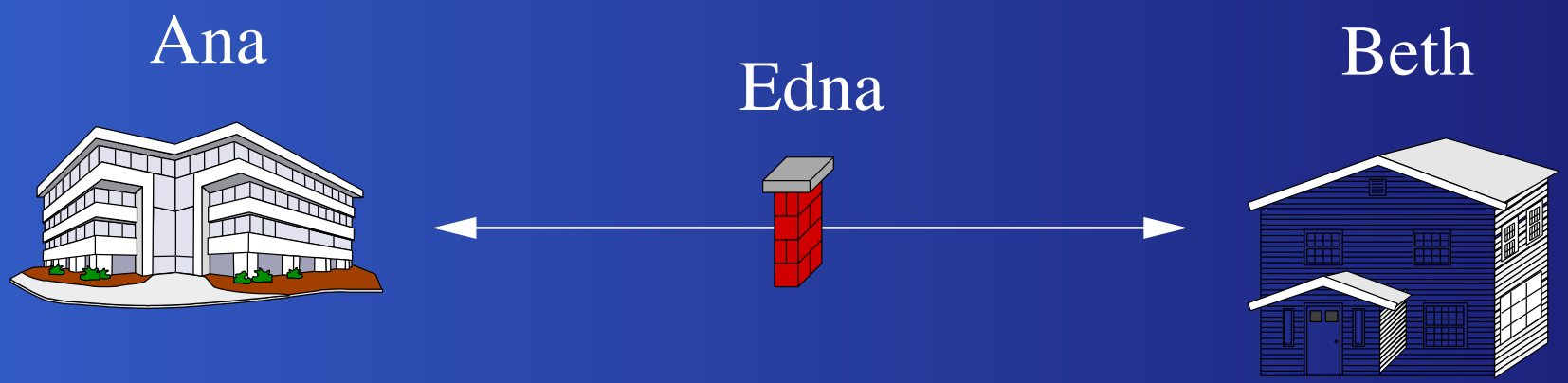
Terminologia

- Mensagem - Plaintext
- Chave
- Criptossistema
- Criptograma - Ciphertext
- Criptografia
- Criptoanálise
- Criptologia
- Entropia

Terminologia

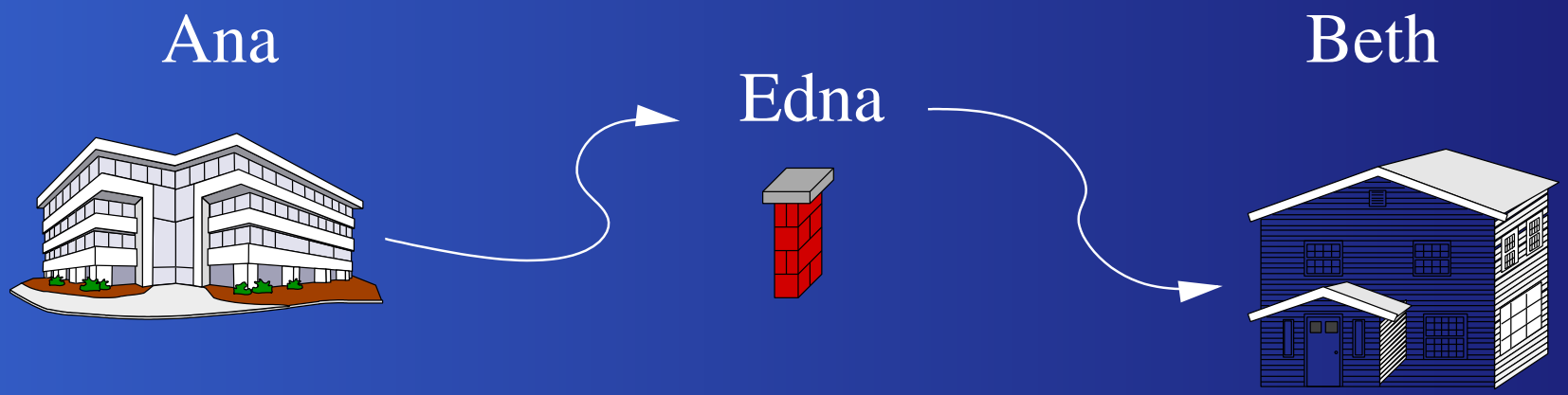
- Mensagem - Plaintext
- Chave
- Criptossistema
- Criptograma - Ciphertext
- Criptografia
- Criptoanálise
- Criptologia
- Entropia
- Esteganografia

Fluxo Normal

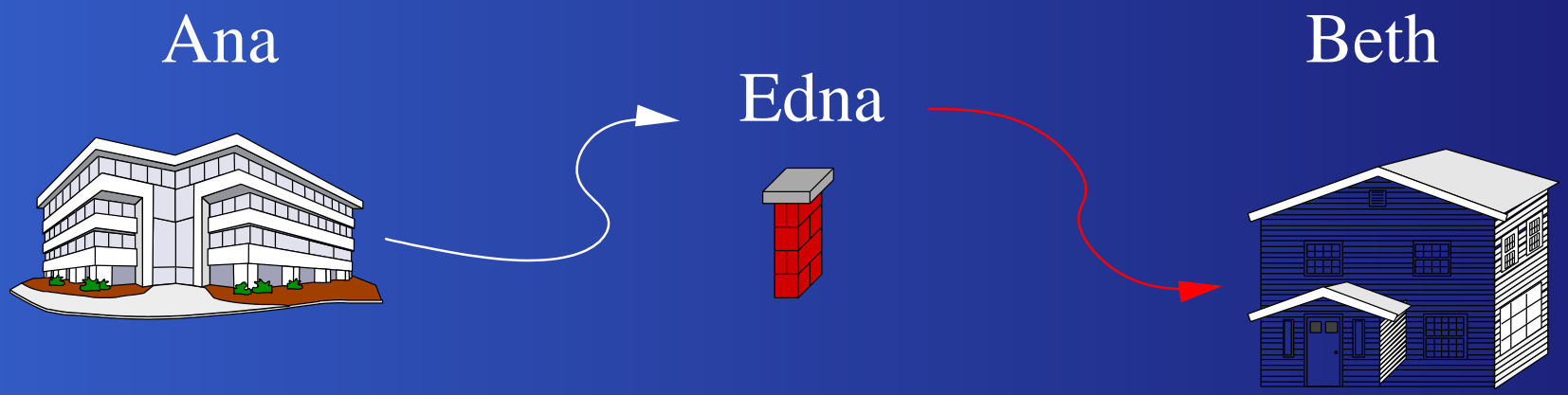


Ameaças eminentes.

Interceptação

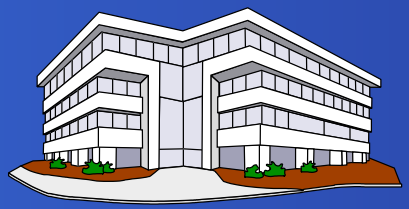


Alteração

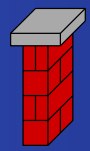


Fabricação

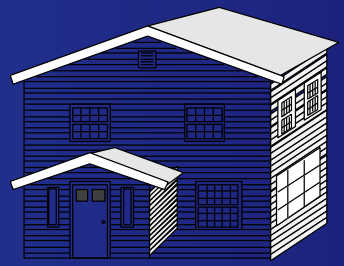
Ana



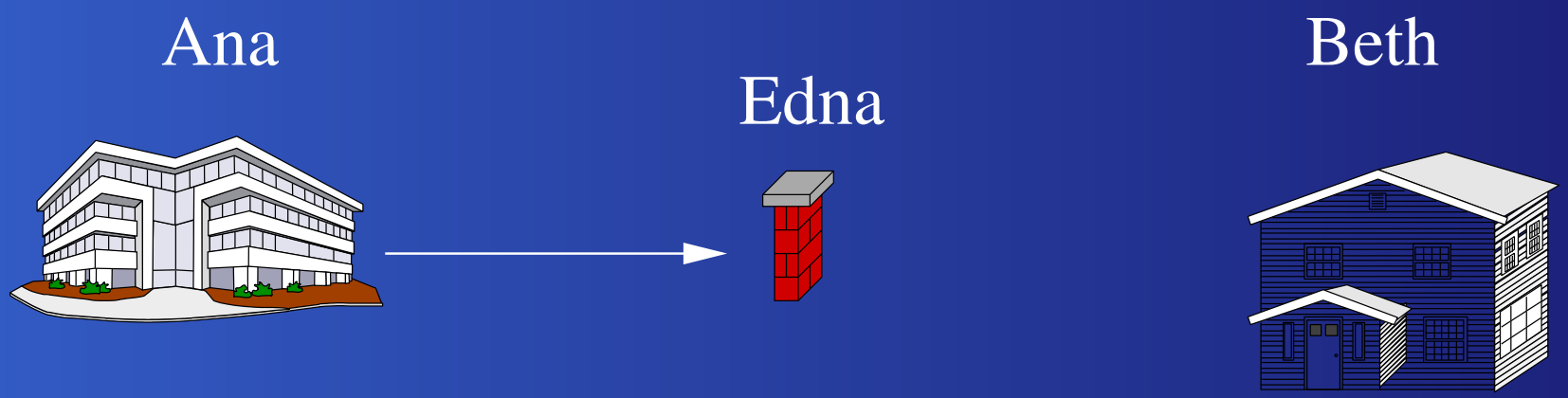
Edna



Beth



Interrupção



Echelon

- Espiona o tráfego via satélite, sinais de rádio e TV, ligações telefônicas e de fax, e-mail

Echelon

- Espiona o tráfego via satélite, sinais de rádio e TV, ligações telefônicas e de fax, e-mail
- Procura por palavras-chave.

Echelon

- Espiona o tráfego via satélite, sinais de rádio e TV, ligações telefônicas e de fax, e-mail
- Procura por palavras-chave.
- A existência do Echelon é negada oficialmente

Echelon

- Espiona o tráfego via satélite, sinais de rádio e TV, ligações telefônicas e de fax, e-mail
- Procura por palavras-chave.
- A existência do Echelon é negada oficialmente
- EUA, com a ajuda de Reino Unido, Canadá, Austrália e Nova Zelândia.

Echelon

- Espiona o tráfego via satélite, sinais de rádio e TV, ligações telefônicas e de fax, e-mail
- Procura por palavras-chave.
- A existência do Echelon é negada oficialmente
- EUA, com a ajuda de Reino Unido, Canadá, Austrália e Nova Zelândia.
- Hoje ninguém duvida da sua existência

Echelon

- Espiona o tráfego via satélite, sinais de rádio e TV, ligações telefônicas e de fax, e-mail
- Procura por palavras-chave.
- A existência do Echelon é negada oficialmente
- EUA, com a ajuda de Reino Unido, Canadá, Austrália e Nova Zelândia.
- Hoje ninguém duvida da sua existência
- Mas e a eficiência: caminho, só inglês?...

Após 11/Set/01

- Outros projetos

Após 11/Set/01

- Outros projetos
- Oficiais

Após 11/Set/01

- Outros projetos
- Oficiais
- Ressalva de não serem utilizados em cidadãos americanos

Após 11/Set/01

- Outros projetos
- Oficiais
- Ressalva de não serem utilizados em cidadãos americanos
- Um dos projetos previsto para ficar pronto em 2006, poderá identificar 90% dos veículos de uma cidade em duas horas.

Referências Oficiais

- www.mre.gov.br/portugues/noticiario/nacional/selecao_detalhe.asp?ID_RESENHA=8143
- www.radiobras.gov.br/anteriores/2001//sinopses_0710.htm

Esteganografia

Original:

Esteganografia:

Relação do Alfabeto

- $A \leftrightarrow Q$

Relação do Alfabeto

- A $\leftrightarrow$ Q
- B $\leftrightarrow$ V

Relação do Alfabeto

- A $\leftrightarrow$ Q
- B $\leftrightarrow$ V
- C $\leftrightarrow$ D

Relação do Alfabeto

- $A \leftrightarrow Q$
- $B \leftrightarrow V$
- $C \leftrightarrow D$
- $\vdots$

Relação do Alfabeto

- $A \leftrightarrow Q$
- $B \leftrightarrow V$
- $C \leftrightarrow D$
- $\vdots$
- $Z \leftrightarrow E$

Relação do Alfabeto

- $A \leftrightarrow Q$
- $B \leftrightarrow V$
- $C \leftrightarrow D$
- $\vdots$
- $Z \leftrightarrow E$
- "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

Relação do Alfabeto

- $A \leftrightarrow Q$
- $B \leftrightarrow V$
- $C \leftrightarrow D$
- $\vdots$
- $Z \leftrightarrow E$
- "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
- "QVDIJTPOCYHNGXAZWUSMFKRLBE"

Relação do Alfabeto

- $A \leftrightarrow Q$
- $B \leftrightarrow V$
- $C \leftrightarrow D$
- $\vdots$
- $Z \leftrightarrow E$
- "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
- "QVDIJTPOCYHNGXAZWUSMFKRLBE"
- $26! - 1 = 403291461126605635583999999$

Relação do Alfabeto

- A $\leftrightarrow$ Q
- B $\leftrightarrow$ V
- C $\leftrightarrow$ D
- $\vdots$
- Z $\leftrightarrow$ E
- "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
- "QVDIJTPOCYHNGXAZWUSMFKRLBE"
- $26! - 1 = 403291461126605635583999999$
- $26! \approx 4.03\ 10^{26}$

Leia

M473M471C0 (53N54C1ON4L):
4S V3235 3U 4C0RD0 M310 M473M471C0.
D31X0 70D4 4 4857R4Ç40 N47UR4L D3 L4D0
3 M3 P0NH0 4 P3N54R 3M NUM3R05, C0M0
53 F0553 UM4 P35504 R4C10N4L. 540 5373
D1550, N0V3 D4QU1L0... QU1N23 PR45
0NZ3... 7R323N705 6R4M45 D3 PR35UNT0...
M45 L060 C410 N4 R34L 3 C0M3Ç0 4 F423R
V3R505 H1NDU-4R481C05

Altas Freqüências

En	%	Fr	%	It	%	Es	%	Pt	%	Br	%
E	11.52	E	16.61	E	11.44	E	12.61	E	12.76	E	12.81
T	8.58	S	8.15	I	10.38	A	11.36	A	12.32	A	12.36
O	8.11	N	7.06	A	9.86	O	9.13	O	10.27	O	10.28
A	6.89	A	6.78	O	9.07	S	8.03	S	8.85	S	8.91
I	6.80	I	6.69	N	6.78	N	6.89	R	6.20	R	6.16
S	6.46	U	6.35	R	6.19	R	6.36	I	5.47	I	5.42
N	6.13	T	6.34	T	5.64	I	6.04	N	5.02	N	5.01
H	5.71	R	6.33	L	5.23	D	4.92	M	4.86	M	4.90
R	5.61	O	5.59	S	5.03	L	4.40	D	4.81	D	4.77
L	3.96	L	4.54	C	4.55	U	4.02	U	4.15	U	4.20

Relação em Blocos

- AAAA $\leftrightarrow$ GFHO

Relação em Blocos

- AAAA $\leftrightarrow$ GFHO
- AAAB $\leftrightarrow$ AFGI

Relação em Blocos

- AAAA $\leftrightarrow$ GFHO
- AAAB $\leftrightarrow$ AFGI
- $\vdots$

Relação em Blocos

- AAAA $\leftrightarrow$ GFHO
- AAAB $\leftrightarrow$ AFGI
- $\vdots$
- LNCC $\leftrightarrow$ ASDR

Relação em Blocos

- AAAA $\leftrightarrow$ GFHO
- AAAB $\leftrightarrow$ AFGI
- $\vdots$
- LNCC $\leftrightarrow$ ASDR
- $\vdots$

Relação em Blocos

- AAAA $\leftrightarrow$ GFHO
- AAAB $\leftrightarrow$ AFGI
- $\vdots$
- LNCC $\leftrightarrow$ ASDR
- $\vdots$
- ZZZZ $\leftrightarrow$ EYTO

Relação em Blocos

- AAAA $\leftrightarrow$ GFHO
- AAAB $\leftrightarrow$ AFGI
- $\vdots$
- LNCC $\leftrightarrow$ ASDR
- $\vdots$
- ZZZZ $\leftrightarrow$ EYTO
- $26^4 = 456976$

Relação em Blocos

- AAAA $\leftrightarrow$ GFHO
- AAAB $\leftrightarrow$ AFGI
- $\vdots$
- LNCC $\leftrightarrow$ ASDR
- $\vdots$
- ZZZZ $\leftrightarrow$ EYTO
- $26^4 = 456976$
- $26^4! \approx 3.28\ 10^{2387976}$

Relação em Blocos Compactos

- LNCC $\leftrightarrow$ AS

Relação em Blocos Compactos

- LNCC $\leftrightarrow$ AS
- LABO $\leftrightarrow$ GHR

Relação em Blocos Compactos

- LNCC $\leftrightarrow$ AS
- LABO $\leftrightarrow$ GHR
- RATO $\leftrightarrow$ YGUJ

Relação em Blocos Compactos

- LNCC $\leftrightarrow$ AS
- LABO $\leftrightarrow$ GHR
- RATO $\leftrightarrow$ YGUJ
- $\vdots$

Relação em Blocos Compactos

- LNCC $\leftrightarrow$ AS
- LABO $\leftrightarrow$ GHR
- RATO $\leftrightarrow$ YGUJ
- $\vdots$
- AAAA $\leftrightarrow$ GFHOGHD

Relação em Blocos Compactos

- LNCC $\leftrightarrow$ AS
- LABO $\leftrightarrow$ GHR
- RATO $\leftrightarrow$ YGUJ
- $\vdots$
- AAAA $\leftrightarrow$ GFHOGHD
- ZZZZ $\leftrightarrow$ EYTOYUI

Casos para Brincar

- Telefone Celular

Casos para Brincar

- Telefone Celular
- Acrônimos

Casos para Brincar

- Telefone Celular
- Acrônimos
- Diário de adolescentes

Casos para Brincar

- Telefone Celular
- Acrônimos
- Diário de adolescentes
- Confusão como escrever nas posições pares depois nas ímpares

Último Slide

- Obrigado.
- Quaisquer sugestões serão bem-vindas.

www.lncc.br/borges