Criptografia com Maple

LNCC - Verão/2005

Fábio Borges & Renato Portugal

Grupo $(G, \oplus)$

Fechado	Se $a, b \in G$ então $a \oplus b \in G$
Associativa	$a \oplus (b \oplus c) = (a \oplus b) \oplus c \quad \forall a, b, c \in G$
Identidade	$\exists\, 0 \in G : a \oplus 0 = a \quad \forall a \in G$
Inversa	$\forall a \in G \quad \exists\, b \in G : a \oplus b = 0$

Exemplo $(\mathbb{Z}_5, +)$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Grupo Abeliano

Fechado	Se $a, b \in G$ então $a \oplus b \in G$
Associativa	$a \oplus (b \oplus c) = (a \oplus b) \oplus c$
Identidade	$\exists 0 \in G : a + 0 = a \quad \forall a \in G$
Inversa	$\forall a \in G \quad \exists b \in G : a \oplus b = 0$
Comutatividade	$a \oplus b = b \oplus a \quad a, b \in G$

Contra Exemplo

- Matrizes M com dimensão $n \times n$ e $\det(M) \neq 0$

Contra Exemplo

- Matrizes M com dimensão $n \times n$ e $\det(M) \neq 0$
-

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 8 & 5 \\ 20 & 13 \end{bmatrix}$$

Contra Exemplo

- Matrizes M com dimensão $n \times n$ e $\det(M) \neq 0$
-
$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 8 & 5 \\ 20 & 13 \end{bmatrix}$$
-
$$\begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 13 & 20 \\ 5 & 8 \end{bmatrix}$$

Anel $(R, \oplus, \odot)$

Grupo Abeliano	$(R^*, \oplus)$
Fechado	Se $a, b \in R$ então $a \odot b \in R$
Associativa	$a \odot (b \odot c) = (a \odot b) \odot c$
Distributivas	$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$
	$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$

$$\forall a, b, c \in R$$

Anel $(R, +, \cdot)$

Grupo Abeliano	$(R^*, +)$
Fechado	Se $a, b \in R$ então $ab \in R$
Associativa	$a(bc) = (ab)c$
Distributivas	$a(b+c) = ab + ac$
	$(a+b)c = ac + bc$

$$\forall a, b, c \in R$$

Anel Comutativo

Anel	$(R, +, \cdot)$
Comutatividade	$ab = ba \quad a, b \in R$

Exemplo $(\mathbb{Z}_6, +, \cdot)$

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Domínio de Integridade

Anel Comutativo	$(R, +, \cdot)$ Comutativo
Identidade	$\exists 1 \in R : a1 = a$
Sem divisor de zero	$ab = 0 \Leftrightarrow a = 0$ ou $b = 0$

$$\forall a, b \in R$$

Exemplo $(\mathbb{Z}_5, +, \cdot)$

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Corpo

Domínio de Integridade

Inversa $\forall a \in F \quad \exists\, b \in F : ab = 0$

Exemplos $\mathbb{Z}_7$ e $\mathbb{Z}_8$

a	$-a$	a^{-1}
0	0	—
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

a	$-a$	a^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

Corpo

Grupos Abelianos	$(F, +)$ abeliano
	$(F, \cdot)$ abeliano
Distributivas	$a(b + c) = ab + ac$
	$(a + b)c = ac + bc$
Sem divisor de zero	$ab = 0 \Leftrightarrow a = 0$ ou $b = 0$

$$\forall a, b, c \in F$$

Criptossistema

- Um alfabeto L que contém todos os símbolos usados

Criptossistema

- Um alfabeto L que contém todos os símbolos usados
- Um anel R comutativo com identidade tal que $|R| = |L|$

Criptossistema

- Um alfabeto L que contém todos os símbolos usados
- Um anel R comutativo com identidade tal que $|R| = |L|$
- Bijeções $\alpha : L \rightarrow R$ e $f : R \rightarrow R$

Criptossistema

- Um alfabeto L que contém todos os símbolos usados
- Um anel R comutativo com identidade tal que $|R| = |L|$
- Bijeções $\alpha : L \to R$ e $f : R \to R$
- $L = \{\not\emptyset, A, B, \ldots, Z\}$

Criptossistema

- Um alfabeto L que contém todos os símbolos usados
- Um anel R comutativo com identidade tal que $|R| = |L|$
- Bijeções $\alpha : L \to R$ e $f : R \to R$
- $L = \{\not\emptyset, A, B, \ldots, Z\}$
- $R = \mathbb{Z}_{27}$

Método para Criptografar (César)

$$f: \quad R \to R$$
$$f(x): \quad x \mapsto ax \mod |R|$$

Para algum $a \in R$

Método para Criptografar (César)

$$f: \ R \to R$$
$$f(x): \ x \mapsto ax \mod |R|$$

Para algum $a \in R$

Com $(a, |R|) = 1$

Método II (César)

$$f: \ R \to R$$
$$f(x): \ x \mapsto ax + b \mod |R|$$

Para algum $a, b \in R$

Método II (César)

$$f: \ R \to R$$
$$f(x): \ x \mapsto ax + b \mod |R|$$

Para algum $a, b \in R$
Com $(a, |R|) = 1$

Exemplo

- {1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26}
  Grupo das Unidades

Exemplo

- {1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26}
  Grupo das Unidades
- $f(x) = 5x + 3 \mod 27$

Exemplo

- {1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26}
  Grupo das Unidades
- $f(x) = 5x + 3 \mod 27$
- $5 \times 11 \equiv 55 \equiv 1 \mod 27$

Exemplo

- {1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26}
  Grupo das Unidades
- $f(x) = 5x + 3 \mod 27$
- $5 \times 11 \equiv 55 \equiv 1 \mod 27$
- $f^{-1}(x) = a^{-1}(x - b) = 11(x - 3)$

Exemplo

- {1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26} Grupo das Unidades
- $f(x) = 5x + 3 \mod 27$
- $5 \times 11 \equiv 55 \equiv 1 \mod 27$
- $f^{-1}(x) = a^{-1}(x - b) = 11(x - 3)$
- α : "LNCC" $\mapsto [12, 14, 3, 3]$

Exemplo

- {1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26} Grupo das Unidades
- $f(x) = 5x + 3 \mod 27$
- $5 \times 11 \equiv 55 \equiv 1 \mod 27$
- $f^{-1}(x) = a^{-1}(x - b) = 11(x - 3)$
- α : "LNCC" $\mapsto [12, 14, 3, 3]$
- $f : [12, 14, 3, 3] \mapsto [9, 19, 18, 18]$

Exemplo

- {1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26} Grupo das Unidades
- $f(x) = 5x + 3 \mod 27$
- $5 \times 11 \equiv 55 \equiv 1 \mod 27$
- $f^{-1}(x) = a^{-1}(x - b) = 11(x - 3)$
- α : "LNCC" $\mapsto [12, 14, 3, 3]$
- $f : [12, 14, 3, 3] \mapsto [9, 19, 18, 18]$
- "ISRR"

Método de Hill

Seja uma matriz $K_{n\times n}$ invertível sobre R, i.e.,

$$(\det K, |R|) = 1.$$

Agrupe a mensagem em vetores P_i de comprimento n e defina

$$f : R^n \to R^n$$

$$f(P_i) \mapsto P_i K$$

Exemplo de Hill

- Mensagem: LNCC

Exemplo de Hill

- Mensagem: LNCC
- $K = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$

Exemplo de Hill

- Mensagem: LNCC
- $K = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$
- $\det(K) = -2 \equiv 25 \mod 27$

Exemplo de Hill

- Mensagem: LNCC
- $K = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$
- $\det(K) = -2 \equiv 25 \mod 27$
- α : "LNCC" $\mapsto [12, 14, 3, 3]$

Exemplo de Hill

- Mensagem: LNCC
- $K = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$
- $\det(K) = -2 \equiv 25 \mod 27$
- α : "LNCC" $\mapsto [12, 14, 3, 3]$
- $P_1K = [0, 26] \qquad P_2K = [12, 18]$

Exemplo de Hill

- Mensagem: LNCC
- $K = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$
- $\det(K) = -2 \equiv 25 \mod 27$
- α : "LNCC" $\mapsto [12, 14, 3, 3]$
- $P_1 K = [0, 26] \qquad P_2 K = [12, 18]$
- $\alpha^{-1} : [0, 26, 12, 18] \mapsto$ "ø/ZLR"

Hill f^{-1}

- $f^{-1}(C_i) = C_i K^{-1}$

Hill f^{-1}

- $f^{-1}(C_i) = C_i K^{-1}$
- $K^{-1} = \frac{1}{\det(K)}(\text{adj}\, K)$

Hill f^{-1}

- $f^{-1}(C_i) = C_i K^{-1}$
- $K^{-1} = \frac{1}{\det(K)}(\text{adj}\, K)$
- $C_{ij} = (-1)^{i+j} M_{ij} \qquad i, j = 1, \cdots, n$

Hill f^{-1}

- $f^{-1}(C_i) = C_i K^{-1}$
- $K^{-1} = \frac{1}{\det(K)}(\text{adj}\, K)$
- $C_{ij} = (-1)^{i+j} M_{ij} \qquad i, j = 1, \cdots, n$
- $$\text{adj}\, K = \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{12} & C_{22} & \cdots & C_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ C_{1n} & C_{2n} & \cdots & C_{nn} \end{bmatrix}$$

Decifrando o Exemplo de Hill

- Criptograma: ⁄ØZLR

Decifrando o Exemplo de Hill

- Criptograma: ∅ZLR
- $K^{-1} = \frac{1}{25}\begin{bmatrix} 4 & -3 \\ -2 & 1 \end{bmatrix}$

Decifrando o Exemplo de Hill

- Criptograma: ∅ZLR
- $K^{-1} = \frac{1}{25}\begin{bmatrix} 4 & -3 \\ -2 & 1 \end{bmatrix}$
- $K^{-1} = 13\begin{bmatrix} 4 & 24 \\ 25 & 1 \end{bmatrix} \equiv \begin{bmatrix} 25 & 1 \\ 15 & 13 \end{bmatrix}$

Decifrando o Exemplo de Hill

- Criptograma: ⁄ZLR
- $K^{-1} = \frac{1}{25}\begin{bmatrix} 4 & -3 \\ -2 & 1 \end{bmatrix}$
- $K^{-1} = 13\begin{bmatrix} 4 & 24 \\ 25 & 1 \end{bmatrix} \equiv \begin{bmatrix} 25 & 1 \\ 15 & 13 \end{bmatrix}$
- $f^{-1} : [0, 26, 12, 18] \mapsto [12, 14, 3, 3]$

Decifrando o Exemplo de Hill

- Criptograma: ∅ZLR
- $K^{-1} = \frac{1}{25}\begin{bmatrix} 4 & -3 \\ -2 & 1 \end{bmatrix}$
- $K^{-1} = 13\begin{bmatrix} 4 & 24 \\ 25 & 1 \end{bmatrix} \equiv \begin{bmatrix} 25 & 1 \\ 15 & 13 \end{bmatrix}$
- $f^{-1} : [0, 26, 12, 18] \mapsto [12, 14, 3, 3]$
- $\alpha^{-1} : [12, 14, 3, 3] \mapsto$ "LNCC"

Deficiência

- U♭NPBUJLPIKAANFRVWRL

Deficiência

- U♭NPBUJLPIKAANFRVWRL
- [21,0,14,16,2,21,10,12,16,9,11,1,1,14,6,18,22,23,18,12]

Deficiência

- U♭NPBUJLPIKAANFRVWRL
- [21,0,14,16,2,21,10,12,16,9,11,1,1,14,6,18,22,23,18,12]
- Termina com LNCC isto é [12, 14, 3, 3]

Deficiência

- U♭NPBUJLPIKAANFRVWRL
- [21,0,14,16,2,21,10,12,16,9,11,1,1,14,6,18,22,23,18,12]
- Termina com LNCC isto é [12, 14, 3, 3]
- $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

Deficiência

- U♭NPBUJLPIKAANFRVWRL
- [21,0,14,16,2,21,10,12,16,9,11,1,1,14,6,18,22,23,18,12]
- Termina com LNCC isto é [12, 14, 3, 3]
- $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$
- $[12, 14]K = [22, 23]$ e $[3, 3]K = [18, 12]$

Deficiência

- $$\begin{bmatrix} 12 & 14 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 22 & 23 \\ 18 & 12 \end{bmatrix}$$

Deficiência

- $$\begin{bmatrix} 12 & 14 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 22 & 23 \\ 18 & 12 \end{bmatrix}$$
- $$\begin{bmatrix} 12\,a + 14\,c & 12\,b + 14\,d \\ 3\,a + 3\,c & 3\,b + 3\,d \end{bmatrix} = \begin{bmatrix} 22 & 23 \\ 18 & 12 \end{bmatrix}$$

Deficiência

- $$\begin{bmatrix} 12 & 14 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 22 & 23 \\ 18 & 12 \end{bmatrix}$$
- $$\begin{bmatrix} 12\,a + 14\,c & 12\,b + 14\,d \\ 3\,a + 3\,c & 3\,b + 3\,d \end{bmatrix} = \begin{bmatrix} 22 & 23 \\ 18 & 12 \end{bmatrix}$$
- Como os MDCs são 3 não tem solução única

Deficiência

- $$\begin{bmatrix} 12 & 14 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 22 & 23 \\ 18 & 12 \end{bmatrix}$$
- $$\begin{bmatrix} 12\,a + 14\,c & 12\,b + 14\,d \\ 3\,a + 3\,c & 3\,b + 3\,d \end{bmatrix} = \begin{bmatrix} 22 & 23 \\ 18 & 12 \end{bmatrix}$$
- Como os MDCs são 3 não tem solução única
- $$\begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix}$$

Deficiência

- $$\begin{bmatrix} 12 & 14 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 22 & 23 \\ 18 & 12 \end{bmatrix}$$
- $$\begin{bmatrix} 12\,a + 14\,c & 12\,b + 14\,d \\ 3\,a + 3\,c & 3\,b + 3\,d \end{bmatrix} = \begin{bmatrix} 22 & 23 \\ 18 & 12 \end{bmatrix}$$
- Como os MDCs são 3 não tem solução única
- $$\begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix}$$
- CRIPTOGRAFIA ∅NO ∅LNCC

Método de Hill Generalizado

Seja uma matriz $A_{n\times n}$ invertível sobre R. Agrupe a mensagem em vetores P_i de comprimento n e defina

$$f : R^n \to R^n$$

$$f(P_i) \mapsto P_i A + B_i$$

1. $B_i = P_{i-1}B$ onde $B_{n\times n}$ sobre R dada com P_0
2. $B_i = C_{i-1}B$ agora dada com C_0
3. $B_i = (r_i, r_{i+1}, \cdots, r_{i+n-1})$ onde $\{r_j\}$ é uma seqüência recursiva sobre R dado o valor inicial r_j

Involutória

- $K^2 = I$

Involutória

- $K^2 = I$
- Seja $A_{r \times s}$ e $B_{s \times r}$ ambos sobre R

Involutória

- $K^2 = I$
- Seja $A_{r \times s}$ e $B_{s \times r}$ ambos sobre R
- $$\begin{bmatrix} BA - I & B \\ 2A - ABA & I - AB \end{bmatrix}$$

Involutória

- $K^2 = I$
- Seja $A_{r \times s}$ e $B_{s \times r}$ ambos sobre R
- $$\begin{bmatrix} BA - I & B \\ 2A - ABA & I - AB \end{bmatrix}$$
- $M = XY$

Involutória

- $K^2 = I$
- Seja $A_{r \times s}$ e $B_{s \times r}$ ambos sobre R
- $$\begin{bmatrix} BA - I & B \\ 2A - ABA & I - AB \end{bmatrix}$$
- $M = XY$
- $MX = XM^{-1} \Rightarrow XYX = XYX$

Involutória

- $K^2 = I$
- Seja $A_{r \times s}$ e $B_{s \times r}$ ambos sobre R
- $$\begin{bmatrix} BA - I & B \\ 2A - ABA & I - AB \end{bmatrix}$$
- $M = XY$
- $MX = XM^{-1} \Rightarrow XYX = XYX$
- $MY = YM^{-1} \Rightarrow XYY = YYX$

Problema das Duas Mensagens

- K e K' Involutórias

Problema das Duas Mensagens

- K e K' Involutórias
- $C_i = P_i K$ e $C_i' = P_i K'$

Problema das Duas Mensagens

- K e K' Involutórias
- $C_i = P_i K$ e $C_i' = P_i K'$
- $C_i K = P_i$

Problema das Duas Mensagens

- K e K' Involutórias
- $C_i = P_i K$ e $C_i' = P_i K'$
- $C_i K = P_i$
- $C_i' = C_i K K$

Problema das Duas Mensagens

- K e K' Involutórias
- $C_i = P_i K$ e $C_i' = P_i K'$
- $C_i K = P_i$
- $C_i' = C_i K K$
- $S = [C_{i_1}, \cdots, C_{i_n}]$ e $T = [C_{i_1}', \cdots, C_{i_n}']$

Problema das Duas Mensagens

- K e K' Involutórias
- $C_i = P_i K$ e $C_i' = P_i K'$
- $C_i K = P_i$
- $C_i' = C_i K K$
- $S = [C_{i_1}, \cdots, C_{i_n}]$ e $T = [C_{i_1}', \cdots, C_{i_n}']$
- $T = S K K'$

Problema das Duas Mensagens

- K e K' Involutórias
- $C_i = P_i K$ e $C'_i = P_i K'$
- $C_i K = P_i$
- $C'_i = C_i K K$
- $S = [C_{i_1}, \cdots, C_{i_n}]$ e $T = [C'_{i_1}, \cdots, C'_{i_n}]$
- $T = S K K'$
- Se possível $K K' = S^{-1} T$ e $T^{-1} = K' K S^{-1}$

Problema das Duas Mensagens

- K e K' Involutórias
- $C_i = P_i K$ e $C'_i = P_i K'$
- $C_i K = P_i$
- $C'_i = C_i K K$
- $S = [C_{i_1}, \cdots, C_{i_n}]$ e $T = [C'_{i_1}, \cdots, C'_{i_n}]$
- $T = S K K'$
- Se possível $K K' = S^{-1} T$ e $T^{-1} = K' K S^{-1}$
- $(K K')X = X(K K')^{-1}$

Problema das Duas Mensagens

- K e K' Involutórias
- $C_i = P_i K$ e $C_i' = P_i K'$
- $C_i K = P_i$
- $C_i' = C_i K K$
- $S = [C_{i_1}, \cdots, C_{i_n}]$ e $T = [C_{i_1}', \cdots, C_{i_n}']$
- $T = S K K'$
- Se possível $K K' = S^{-1} T$ e $T^{-1} = K' K S^{-1}$
- $(K K')X = X(K K')^{-1}$
- $(K K')X = X(K' K)$

Vigenère-Vernam (One-time-pad)

- ∮TOYNIMCEYVS∮E∮

Vigenère-Vernam (One-time-pad)

- ∅TOYNIMCEYVS∅E∅
- 00,20,15,25,14,09,13,03,05,25,22,19,00,05,00

Vigenère-Vernam (One-time-pad)

- ∅TOYNIMCEYVS∅E∅
- 00,20,15,25,14,09,13,03,05,25,22,19,00,05,00
- A∅MENINA∅BRINCA

Vigenère-Vernam (One-time-pad)

- ∅TOYNIMCEYVS∅E∅
- 00,20,15,25,14,09,13,03,05,25,22,19,00,05,00
- A∅MENINA∅BRINCA
- 01,00,13,05,14,09,14,01,00,02,18,09,14,03,01

Vigenère-Vernam (One-time-pad)

- ∅TOYNIMCEYVS∅E∅
- 00,20,15,25,14,09,13,03,05,25,22,19,00,05,00
- A∅MENINA∅BRINCA
- 01,00,13,05,14,09,14,01,00,02,18,09,14,03,01
- 01,07,25,07,00,00,01,25,22,04,23,17,14,25,01

Vigenère-Vernam (One-time-pad)

- ␣TOYNIMCEYVS␣E␣
- 00,20,15,25,14,09,13,03,05,25,22,19,00,05,00
- A␣MENINA␣BRINCA
- 01,00,13,05,14,09,14,01,00,02,18,09,14,03,01
- 01,07,25,07,00,00,01,25,22,04,23,17,14,25,01
- ATACAR␣DE␣MANHA

Vigenère-Vernam (One-time-pad)

- ∅TOYNIMCEYVS∅E∅
- 00,20,15,25,14,09,13,03,05,25,22,19,00,05,00
- A∅MENINA∅BRINCA
- 01,00,13,05,14,09,14,01,00,02,18,09,14,03,01
- 01,07,25,07,00,00,01,25,22,04,23,17,14,25,01
- ATACAR∅DE∅MANHA
- 01,20,01,03,01,18,00,04,05,00,13,01,14,08,01

Vigenère-Vernam (One-time-pad)

- ∅TOYNIMCEYVS∅E∅
- 00,20,15,25,14,09,13,03,05,25,22,19,00,05,00
- A∅MENINA∅BRINCA
- 01,00,13,05,14,09,14,01,00,02,18,09,14,03,01
- 01,07,25,07,00,00,01,25,22,04,23,17,14,25,01
- ATACAR∅DE∅MANHA
- 01,20,01,03,01,18,00,04,05,00,13,01,14,08,01
- 01,00,13,05,14,09,14,01,00,02,18,09,14,03,01

Possibilidades (One-time-pad)

- ESTUDANDO ∅MUITO
- CADEIRA ∅AMARELA
- RENATO ∅PORTUGAL
- IR ∅EMBORA ∅AGORA
- EU ∅TO ∅COM ∅FOME ∅
- EU ∅AMO ∅O ∅FABIO ∅
- O ∅SAPATO ∅FURADO
- EVELIN ∅EH ∅LINDA

Segredo Perfeito

- $\mathbb{M} = \{M_1, \ldots, M_n\}$

Segredo Perfeito

- $\mathbb{M} = \{M_1, \ldots, M_n\}$
- $P(M_1), \ldots, P(M_n)$

Segredo Perfeito

- $\mathbb{M} = \{M_1, \ldots, M_n\}$
- $P(M_1), \ldots, P(M_n)$
- $\mathbb{E} = \{E_1, \ldots, E_n\}$

$$E = T_i M$$

Segredo Perfeito

- $\mathbb{M} = \{M_1, \ldots, M_n\}$
- $P(M_1), \ldots, P(M_n)$
- $\mathbb{E} = \{E_1, \ldots, E_n\}$

$$E = T_i M$$

- Criptoanalista intercepta E

$$P_E(M)$$

Def. Segredo Perfeito

Definimos *Segredo Perfeito* pela condição

$$P_E(M) = P(M)$$

para todo $M \in \mathbb{M}$ e todo $E \in \mathbb{E}$

Teo. One-Time-Pad

Teorema: One-Time-Pad é um segredo perfeito.

Teo. One-Time-Pad

Teorema: One-Time-Pad é um segredo perfeito.
Prova: Considere um alfabeto com n símbolos e

$$TM = E$$

Teo. One-Time-Pad

Teorema: One-Time-Pad é um segredo perfeito.
Prova: Considere um alfabeto com n símbolos e

$$TM = E$$

então

$$P(M) = \frac{1}{n}$$

Teo. One-Time-Pad

Teorema: One-Time-Pad é um segredo perfeito.
Prova: Considere um alfabeto com n símbolos e

$$TM = E$$

então

$$P_E(M) = \frac{1}{n}$$

Teo. One-Time-Pad

Teorema: One-Time-Pad é um segredo perfeito.
Prova: Considere um alfabeto com n símbolos e

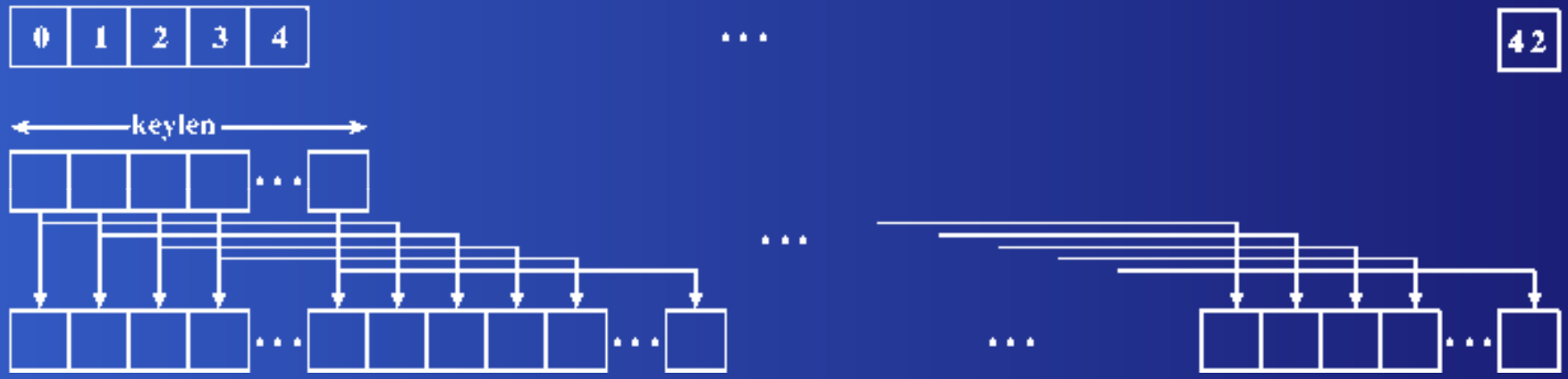
$$TM = E$$

então

$$P(M) = \frac{1}{n} = P_E(M)$$

QED

Esquema Vigenère



Vigenère

- Gerando uma senha do tamanho do texto, a partir de uma senha menor (Keystream)

Vigenère

- Gerando uma senha do tamanho do texto, a partir de uma senha menor (Keystream)
  - A∅MENINA∅BRINCA

Vigenère

- Gerando uma senha do tamanho do texto, a partir de uma senha menor (Keystream)
  - A∅MENINA∅BRINCA
  - 01,00,13,05,14,09,14,01,00,02,18,09,14,03,01

Vigenère

- Gerando uma senha do tamanho do texto, a partir de uma senha menor (Keystream)
  - A∅MENINA∅BRINCA
  - 01,00,13,05,14,09,14,01,00,02,18,09,14,03,01
  - SENHASENHASENHA

Vigenère

- Gerando uma senha do tamanho do texto, a partir de uma senha menor (Keystream)
  - A∅MENINA∅BRINCA
  - 01,00,13,05,14,09,14,01,00,02,18,09,14,03,01
  - SENHASENHASENHA
  - 19,05,14,08,01,19,05,14,08,01,19,05,14,08,01

Vigenère

- Gerando uma senha do tamanho do texto, a partir de uma senha menor (Keystream)
  - A␣MENINA␣BRINCA
  - 01,00,13,05,14,09,14,01,00,02,18,09,14,03,01
  - SENHASENHASENHA
  - 19,05,14,08,01,19,05,14,08,01,19,05,14,08,01
  - 20,05,00,13,15,01,19,15,08,03,10,14,01,11,02

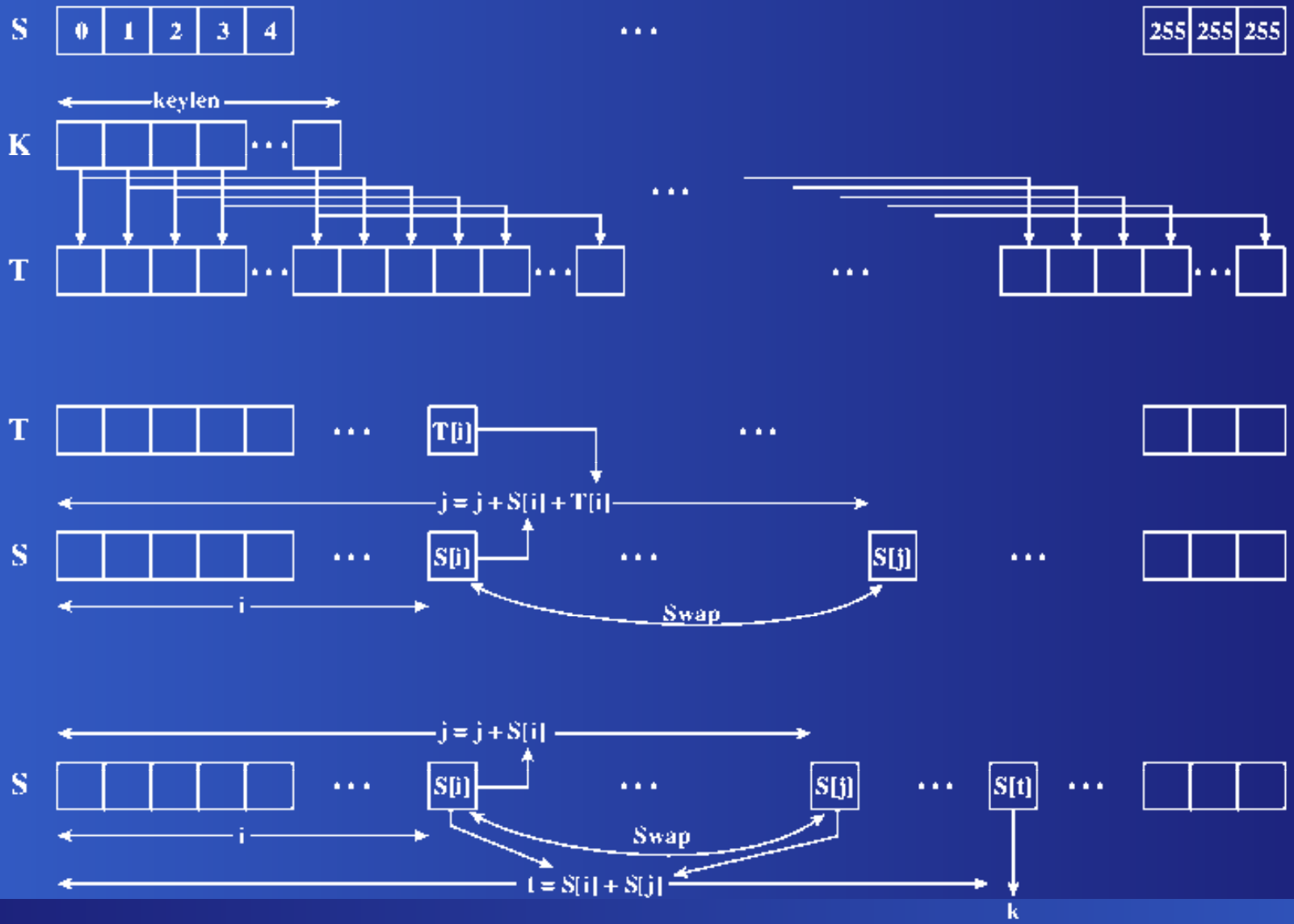
Vigenère

- Gerando uma senha do tamanho do texto, a partir de uma senha menor (Keystream)
  - A␣MENINA␣BRINCA
  - 01,00,13,05,14,09,14,01,00,02,18,09,14,03,01
  - SENHASENHASENHA
  - 19,05,14,08,01,19,05,14,08,01,19,05,14,08,01
  - 20,05,00,13,15,01,19,15,08,03,10,14,01,11,02
  - TE␣MOASOHCJNAKB

Desempenho

Cifra	Comprimento da senha	Mbps
DES	56	9
3DES	168	3
RC2	Variável	0,9
RC4	Variável	45

RC4


S
0
1
2
3
4
255
255
255
keylen
K
T
T
T[i]
j = j + S[i] + T[i]
S
S[i]
S[j]
i
Swap
j = j + S[i]
S
S[i]
S[j]
S[t]
i
Swap
t = S[i] + S[j]
k

RC4 - Inicialização

```
k é a senha
Para i de 0 até 26 faça
     s[i] = i
     t[i] = k[ (i mod tamanho(k)) +1]
fim
```

RC4 - Permutação

```
j = 0
Para i de 0 até 26 faça
     j = ( j + s[i] + t[i] ) mod 27
     Troque(s[j],s[i])
fim
```

RC4 - Criptografando

```
i = 0
j = 0
Para n de 1 até tamanho(mensagem) do
     i = i + 1 mod 27
     j = j + s[i] mod 27
     Troque(s[j],s[i])
     t = s[i] + s[j] mod 27
     imprima(mensagem[n] + s[t] mod 27)
fim
```

Último Slide

- Obrigado.
- Quaisquer sugestões serão bem-vindas.

www.lncc.br/borges

Domínio Euclidiano

- Seja D um Domínio de Integridade e $\delta : D^* \longrightarrow \mathbb{N}$

Domínio Euclidiano

- Seja D um Domínio de Integridade e $\delta : D^* \rightarrow \mathbb{N}$
- $\forall a \in D,\ b \in D^*\ \exists q, r \in D\ : a = bq + r$

Domínio Euclidiano

- Seja D um Domínio de Integridade e $\delta : D^* \rightarrow \mathbb{N}$
- $\forall a \in D,\ b \in D^*\ \exists q, r \in D\ : a = bq + r$
- com $r = 0$ ou $\delta(r) < \delta(b)$

Domínio Euclidiano

- Seja D um Domínio de Integridade e $\delta : D^* \rightarrow \mathbb{N}$
- $\forall a \in D,\ b \in D^*\ \exists q, r \in D\ : a = bq + r$
- com $r = 0$ ou $\delta(r) < \delta(b)$
- Exemplo: Anel dos polinômios $F[x]$ com $\delta(f(x)) = \deg(f(x))$

Domínio Euclidiano

- Seja D um Domínio de Integridade e $\delta : D^* \rightarrow \mathbb{N}$
- $\forall a \in D,\ b \in D^*\ \exists q, r \in D\ : a = bq + r$
- com $r = 0$ ou $\delta(r) < \delta(b)$
- Exemplo: Anel dos polinômios $F[x]$ com $\delta(f(x)) = \deg(f(x))$
- Exemplo: Anel dos inteiros $\mathbb{Z}$ com $\delta(n) = |n|$

Algoritmo Euclidiano

$$
\begin{aligned}
a &= bq_1 + r_1 && \delta(r_1) < \delta(b) \\
b &= r_1 q_2 + r_2 && \delta(r_2) < \delta(r_1) \\
r_1 &= r_2 q_3 + r_3 && \delta(r_3) < \delta(r_2) \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n && \delta(r_n) < \delta(r_{n-1}) \\
r_{n-1} &= r_n q_{n+1} + 0
\end{aligned}
$$

Algoritmo Euclidiano

$$
\begin{aligned}
a &= bq_1 + r_1 & \delta(r_1) < \delta(b) \\
b &= r_1 q_2 + r_2 & \delta(r_2) < \delta(r_1) \\
r_1 &= r_2 q_3 + r_3 & \delta(r_3) < \delta(r_2) \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n & \delta(r_n) < \delta(r_{n-1}) \\
r_{n-1} &= r_n q_{n+1} + 0
\end{aligned}
$$

- r_n divide a e b
- $\forall x \in D$ se $x|a$ e $x|b$ então $x|r_n$

Algoritmo Euclidiano

$$
\begin{aligned}
a &= bq_1 + r_1 & \delta(r_1) < \delta(b) \\
b &= r_1q_2 + r_2 & \delta(r_2) < \delta(r_1) \\
r_1 &= r_2q_3 + r_3 & \delta(r_3) < \delta(r_2) \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n & \delta(r_n) < \delta(r_{n-1}) \\
r_{n-1} &= r_nq_{n+1} + 0
\end{aligned}
$$

- r_n divide a e b
- $\forall x \in D$ se $x|a$ e $x|b$ então $x|r_n$
- $(a, b) = r_n$

Tabela do Algoritmo Euclidiano

- $(a, b) = au + bv$

Tabela do Algoritmo Euclidiano

- $(a, b) = au + bv$

n	q	r	u	v
-1	$-$	$r_{-1} = a$	$u_{-1} = 1$	$v_{-1} = 0$
0	$-$	$r_0 = b$	$u_0 = 0$	$v_0 = 1$
1	q_1	r_1	u_1	v_1
2	q_2	r_2	u_2	v_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	q_n	r_n	u_n	v_n

Relações da Tabela

- $(a, b) = au + bv$

Relações da Tabela

- $(a, b) = au + bv$
- $r_{n-2} = r_{n-1}q_n + r_n$

Relações da Tabela

- $(a, b) = au + bv$
- $r_{n-2} = r_{n-1}q_n + r_n$
- $r_n = r_{n-2} - r_{n-1}q_n$

Relações da Tabela

- $(a, b) = au + bv$
- $r_{n-2} = r_{n-1}q_n + r_n$
- $r_n = r_{n-2} - r_{n-1}q_n$
- $u_n = u_{n-2} - u_{n-1}q_n$

Relações da Tabela

- $(a, b) = au + bv$
- $r_{n-2} = r_{n-1}q_n + r_n$
- $r_n = r_{n-2} - r_{n-1}q_n$
- $u_n = u_{n-2} - u_{n-1}q_n$
- $v_n = v_{n-2} - v_{n-1}q_n$

Prova que $(a, b) = au + bv$

- $r_n = au_n + bv_n$ é verdadeira para $n = -1$ e $n = 0$

Prova que $(a, b) = au + bv$

- $r_n = au_n + bv_n$ é verdadeira para $n = -1$ e $n = 0$
- Assuma que seja válida de n até $k - 1$

Prova que $(a, b) = au + bv$

- $r_n = au_n + bv_n$ é verdadeira para $n = -1$ e $n = 0$
- Assuma que seja válida de n até $k - 1$

$$\begin{aligned} r_k &= r_{k-2} - r_{k-1}q_n \\ &= (au_{k-2} + bv_{k-2}) - (au_{k-1} + bv_{k-1})q_k \\ &= a(u_{k-2} - u_{k-1}q_k) + b(v_{k-2} - v_{k-1}q_k) \\ &= au_k + bv_k \end{aligned}$$

Achando o Inverso

- $27u + 10v = 1$

Achando o Inverso

- $27u + 10v = 1$
  - $27 = 10 \times 2 + 7$

Achando o Inverso

- $27u + 10v = 1$
  - $27 = 10 \times 2 + 7$
  - $10 = 7 \times 1 + 3$

Achando o Inverso

- $27u + 10v = 1$
  - $27 = 10 \times 2 + 7$
  - $10 = 7 \times 1 + 3$
  - $7 = 3 \times 2 + 1$

Achando o Inverso

- $27u + 10v = 1$
  - $27 = 10 \times 2 + 7$
  - $10 = 7 \times 1 + 3$
  - $7 = 3 \times 2 + 1$

n	q	v
-1	$-$	$v_{-1} = 0$
0	$-$	$v_0 = 1$
1	2	v_1
2	1	v_2
3	2	v_3

Achando o Inverso

- $27u + 10v = 1$
  - $27 = 10 \times 2 + 7$
  - $10 = 7 \times 1 + 3$
  - $7 = 3 \times 2 + 1$

n	q	v
-1	$-$	0
0	$-$	1
1	2	-2
2	1	
3	2	

Achando o Inverso

- $27u + 10v = 1$
  - $27 = 10 \times 2 + 7$
  - $10 = 7 \times 1 + 3$
  - $7 = 3 \times 2 + 1$

n	q	v
-1	$-$	0
0	$-$	1
1	2	-2
2	1	3
3	2	

Achando o Inverso

- $27u + 10v = 1$
  - $27 = 10 \times 2 + 7$
  - $10 = 7 \times 1 + 3$
  - $7 = 3 \times 2 + 1$

n	q	v
-1	$-$	0
0	$-$	1
1	2	-2
2	1	3
3	2	-8

Achando o Inverso

- $27u + 10v = 1$
  - $27 = 10 \times 2 + 7$
  - $10 = 7 \times 1 + 3$
  - $7 = 3 \times 2 + 1$
- $-8 \equiv 19 \mod 27$

Achando o Inverso

- $27u + 10v = 1$
  - $27 = 10 \times 2 + 7$
  - $10 = 7 \times 1 + 3$
  - $7 = 3 \times 2 + 1$
- $-8 \equiv 19 \mod 27$
- $10 \times 19 \equiv 190 \equiv 27 \times 7 + 1 \equiv 1 \mod 27$