ACH2076 – Segurança da Informação

Aula 02: Criptografia Clássica

Valdinei Freire

valdinei.freire@usp.br

http://www.each.usp.br/valdinei

Escola de Artes, Ciências e Humanidades - USP

2023

Livros Textos

1. William Stallings. Criptografia e Segurança de redes: princípios e práticas, 4ª edição. **Capítulo 2**
2. Marcio Moretto Ribeiro. Segurança da Informação (apostila).

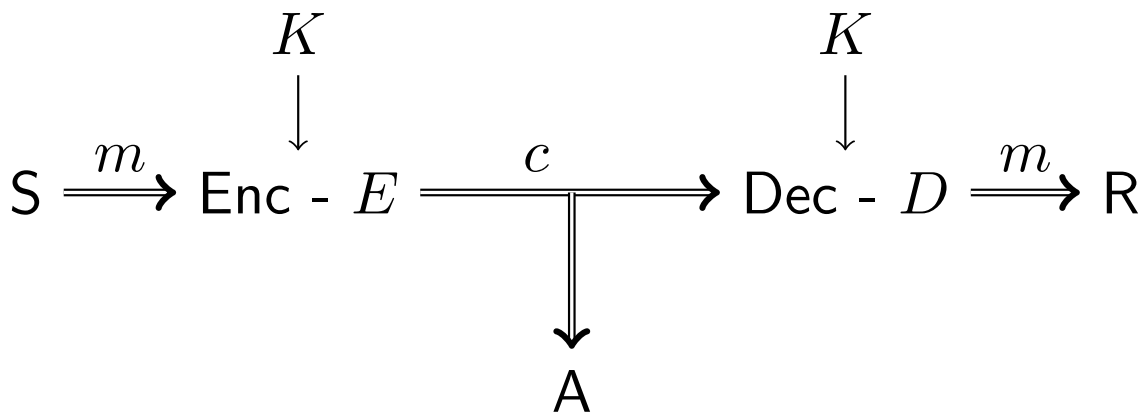
- Criptografia
- Cifras de Substituição
- Cifras de Transposição

Criptologia

kryptós: secreto, escondido
logia: estudo

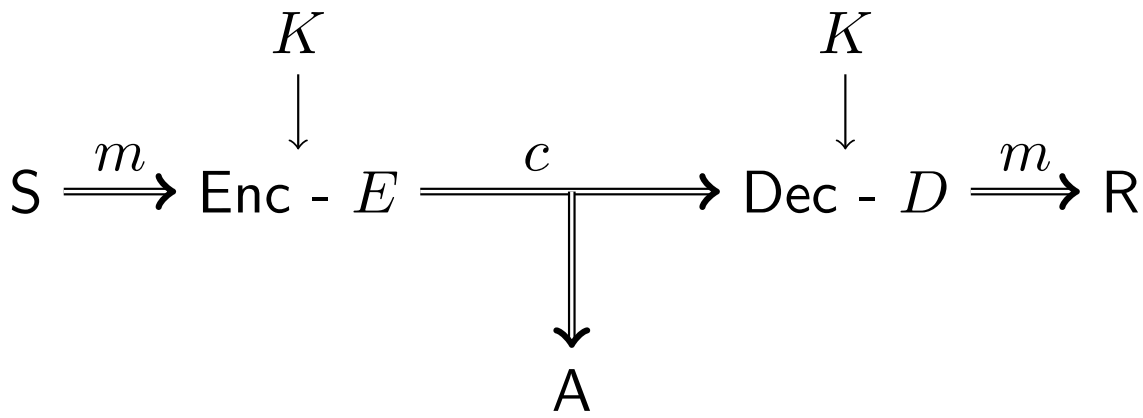
- **Criptologia:** Compreende a criptografia e a criptoanálise
- **Criptografia:** Processo de converter texto claro em texto cifrado e vice-versa
- **Criptoanálise:** Processo de decifrar uma mensagem cifrada sem conhecimento COMPLETO da criptografia

Confidencialidade: Criptografia Simétrica



- m - Texto claro: mensagem inteligível
- E - Algoritmo de criptografia: substituições, inserções e transposições no texto claro
- K - Chave secreta: parâmetro que indica como deve ocorrer substituições, inserções e transposições

Confidencialidade: Criptografia Simétrica



- c - Texto cifrado: mensagem IDEALMENTE ininteligível e depende de m, Enc e K

$$c = E_K(m)$$

- D - Algoritmo de decriptografia: o inverso do algoritmo de criptografia, isto é, dado a chave K e o texto cifrado c produz o texto claro original m

$$m = D_K(c) = D_K(E_K(m))$$

Criptografia: Propriedades

- Tipo de operações utilizadas
  - substituição: elemento do texto claro (bit, letra, grupo) mapeado em outro elemento
  - transposição: reorganização dos elementos no texto claro
  - inserção: preenchimento de dados não contidos no texto claro
- Número de Chaves utilizadas
  - Criptografia simétrica: emissor e receptor utilizam a mesma chave
  - Criptografia assimétrica: emissor e receptor utilizam chaves diferentes
- Modo como o texto claro é processado
  - Cifra de bloco: dado um bloco de elementos gera um bloco de saída
  - Cifra de fluxo: processa um elemento por vez

Cifras Clássicas

- Técnicas de Substituição
  - Cifra Monoalfabética (fluxo)
  - Cifra de César (fluxo)
  - Cifra Polialfabética (fluxo)
  - Cifra de Vigenère (fluxo)
  - Cifra de Hill (bloco)
- Técnicas de Transposição

Cifra Monoalfabética

- Cifra de Substituição: troca caractere por caractere
- Permite que a linha cifra seja qualquer permutação entre os 26 caracteres

claro	a	b	c	d	$\cdots$	w	x	y	z
cifra	X	Y	H	A	$\cdots$	G	C	D	R

- Qual é a chave nesse caso?
- Quantas chaves possíveis?
- Quantos bits são necessário para representar a chave?

Cifra Monoalfabética

- Qual é a chave nesse caso?
  K = XYHA...GCD(R)
- Quantas chaves possíveis?
  $26! \approx 4 \times 10^{26}$
- Quantos bits são necessário para representar a chave?
  - 5 bits por letra
    $5 \times 26 = 130$ bits ($5 \times 26 = 125$ bits)
  - 5 bits para 10 letras, 4 bits para 8 letras, 3 bits para 4 letras, 2 bits para 2 letras, 1 bit para 1 letra
    $5 \times 10 + 4 \times 8 + 3 \times 4 + 2 \times 2 + 1 \times 1 = 99$ bits
  - representando as chaves de forma enumerada
    $\lceil \log(26!) \rceil = 89$ bits

Cifra de César

- Cifra de César: substitui cada letra do alfabeto pela letra que fica três posições adiante

claro	a	b	c	d	$\cdots$	w	x	y	z
cifra	D	E	F	G	$\cdots$	Z	A	B	C

- Cifra de César Afim: considera uma chave $K = (\alpha, \beta)$ (na cifra de César $k = (1, 3)$) e a atribuição abaixo

texto	a	b	c	d	$\cdots$	w	x	y	z
número	0	1	2	3	$\cdots$	22	23	24	25

$$c_i = E_{K=(\alpha,\beta)}(m_i) = (\alpha m_i + \beta) \mod 26$$

Cifra de César: Perguntas?

- Utilizando a cifra de César qual é a cifra para "valdinei"?
- Utilizando a cifra de César Afim com a chave $K = (3, 5)$, qual é a cifra para "valdinei"?
- Algoritmo de Decriptografia?
- Quantas chaves de César Afim existem?

Cifra de César: Perguntas?

- Utilizando a cifra de César qual é a cifra para "valdinei"?
  YDOGLQHL
- Utilizando a cifra de César Afim com a chave $K = (3, 5)$, qual é a cifra para "valdinei"?
  QFMODSRD
- Algoritmo de Decriptografia?

$$m_i = D_{K=(\alpha,\beta)}(c_i) = ((c_i - \beta) \times \alpha^{-1}) \mod 26$$

- Quantas chaves de César Afim existem?
  $12 \times 26 = 312$

*Inverso Multiplicativo e Aditivo com Módulo

- Capítulo 5 – Corpos Finitos
- Álgebra Abstrata
  - Operações básicas: adição e multiplicação
  - Operações derivadas: subtração e divisão
  - Elementos identidade: 0 (adição) e 1 (multiplicação)
- Inverso Aditivo
  - y é inverso aditivo de x, se $y + x = 0$
  - Subtração é equivalente à adição por inverso aditivo
- Inverso Multiplicativo
  - y é inverso multiplicativo de x, se $y \times x = 1$
  - Divisão é equivalente à multiplicação por inverso multiplicativo

*Inverso Multiplicativo e Aditivo com Módulo

Sempre existe inverso multiplicativo?

- em um corpo, com exceção do 0, todos os números possuem inverso multiplicativo
- existem corpos de tamanho p, onde p é primo
  - $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$
  - considere adição e multiplicação módulo p
  - na operação $\mod n$, se n não é primo, então apenas números relativamente primos de n possuem inverso multiplicativo
- existem corpos de tamanho p^n, onde p é primo e $n \in \{1, 2, \ldots\}$
  - é chamado corpo de Galois (Galois Field), e denotado por $GF(p^n)$
  - represente os números por polinômios com coeficientes em $\mathbb{Z}_p$ e de grau $n-1$
  - considera um polinômio $r(x)$ de grau n que seja irredutível (primo)
  - considere adição e multiplicação como operações de polinômios módulo $r(x)$
  - utilizado no CRC (Cyclic redundancy check)

*Inverso Multiplicativo e Aditivo com Módulo

Propriedade Interessante: em um corpo finito, a tabela de multiplicação é uniforme.
Exemplos: multiplicação $\mod 8$ (não é corpo) e $\mod 7$ (é um corpo)

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

*Inverso Multiplicativo e Aditivo com Módulo

Exemplo: corpo finito $GF(2^3)$ (módulo $r(x) = x^3 + x + 1$):

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

*Inverso Multiplicativo e Aditivo com Módulo

Exercícios:

1. Se x está entre 0 e 25 inclusive, quanto vale x nos casos abaixo:
   - $(25 + x) \equiv 0 \mod 26$
   - $(13 + x) \equiv 0 \mod 26$
   - $(-7) \equiv x \mod 26$
   - $(3x) \equiv 1 \mod 26$
   - $(7x) \equiv 1 \mod 26$
   - $(2x) \equiv 1 \mod 26$
   - $(13x + 12) \equiv (2x + 4) \mod 26$
2. Construa as tabelas de adição e multiplicação do corpo $\mathbb{Z}_5$.

Cifras Polialfabéticas

- Considera um conjunto ordenado de regras monoalfabéticas
- A chave determina qual regra utilizar em cada substituição de caracteres no texto claro
- Exemplo: cifra de Vegenère
  - considera as 26 cifras César Afim com $\alpha = 1$
  - chave: qualquer palavra
  - cada letra da palavra-chave determina o valor de β
  - repete-se a chave para obter uma substituição infinita

Cifras Polialfabéticas

Exemplo: cifra de Vigenère

- Qual é a cifra para “valdinei” utilizando a chave “drn”?

Cifras Polialfabéticas

Exemplo: cifra de Vigenère

- Qual é a cifra para "valdinei" utilizando a chave "drn"?

claro	v	a	l	d	i	n	e	i
chave	d	r	n	d	r	n	d	r
cifra	Y	R	Y	G	Z	A	H	Z

Cifras Polialfabéticas

Exemplo: cifra de Vigenère Incrementada

- Ideia: Vegenère com chave infinita construída on-line
  - Chave Inicial (semente): $K_1 = K$
  - Próximas chaves: $K_i = C_{i-1}$
- Exemplo: "valdinei" com semente 'a'

Cifras Polialfabéticas

Exemplo: cifra de Vigenère Incrementada

- Ideia: Vegenère com chave infinita construída on-line
  - Chave Inicial (semente): $K_1 = K$
  - Próximas chaves: $K_i = C_{i-1}$
- Exemplo: "valdinei" com semente 'a'

claro	v	a	l	d	i	n	e	i
chave	a	v	v	g	j	r	e	i
cifra	V	V	G	J	R	E	I	Q

Cifra de Hill

- Substitui n letras de texto claro por n letras de texto cifrado
- Combinação linear entre os caracteres considerados
- Exemplo: $n = 3$

$$\begin{aligned} c_1 &= (K_{11}m_1 + K_{12}m_2 + K_{13}m_3) \mod 26 \\ c_2 &= (K_{21}m_1 + K_{22}m_2 + K_{23}m_3) \mod 26 \\ c_3 &= (K_{31}m_1 + K_{32}m_2 + K_{33}m_3) \mod 26 \end{aligned}$$

- chave: matriz K inversível $n \times n$

$$\begin{aligned} c = E_K(m) &= Km_{1,n}|Km_{n+1,2n}|Km_{n+1,2n}|\cdots \mod 26 \\ m = D_K(c) &= K^{-1}c_{1,n}|K^{-1}c_{n+1,2n}|K^{-1}c_{n+1,2n}|\cdots \mod 26 \end{aligned}$$

Cifra de Hill

- Exemplo:

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \quad K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

- Verique se $KK^{-1} = I$ (matriz identidade)
- Qual é a cifra para "valdineiz"?

Cifra de Hill

- Exemplo:

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \quad K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

- Verique se $KK^{-1} = I$ (matriz identidade)
- Qual é a cifra para "valdineiz"?

$c =$WWRSMJRZF

Cifra de Hill

- Como calcular a inversa de uma matriz?

$$K = \begin{bmatrix} 0 & 2 & 1 \\ 3 & 1 & 3 \\ 1 & 2 & 3 \end{bmatrix} \qquad K^{-1} = \frac{1}{det(K)} Adj(K)$$

- Os elementos x_{ij} da matriz X adjunta de K, isto é, $X = Adj(K)$ é obtido da seguinte forma:
  - Monte as matrizes X_{ij} removendo a linha i e a coluna j da matriz K
  - Então: $x_{ij} = (-1)^{i+j} det(X_{ji})$

Cifra de Hill

$$K^{-1} = \begin{bmatrix} 19 & 8 & 3 \\ 12 & 15 & 7 \\ 3 & 22 & 12 \end{bmatrix}$$

Técnicas de Transposição

- Permutações entre elementos do texto claro
- Exemplo 1:
  - Escreva mensagem original em um retângulo, linha por linha. Se $m =$ "valdineiz", temos:

v	a	l
d	i	n
e	i	z

  - Reconstrua a mensagem cifrada lendo coluna por coluna, para obter $c =$ "VDEAIILNZ"

Técnicas de Transposição

- Exemplo 2:
  - Escreva mensagem original em um retângulo, linha por linha. Se $m =$ "valdineiz", temos:

1	**2**	**3**
v	a	l
d	i	n
e	i	z

  - Reconstrua a mensagem cifrada lendo coluna por coluna na ordem [2,3,1], para obter $c =$ "AIILNZVDE"

Técnicas de Transposição

- Exemplo 3:
  - Escreva mensagem original em um retângulo, linha por linha. Se $m =$"valdineiz", temos:

1	**2**	**3**
v	a	l
d	i	n
e	i	z

  - Reconstrua a mensagem cifrada lendo coluna por coluna na ordem [2,3,1], para obter $c =$"AIILNZVDE"
  - Repita os passos anteriores a partir do c obtido $N = 2$ vezes, para obter $c =$"INDIZEALV"

Técnicas de Transposição

- Qual é a chave no exemplo 1?
- Qual é a chave no exemplo 2?
- Qual é a chave no exemplo 3?

Técnicas de Transposição

- Qual é a chave no exemplo 1?
  3 (número de colunas)
- Qual é a chave no exemplo 2?
  [2 3 1] (sequência das colunas)
- Qual é a chave no exemplo 3?
  [2 3 1] e N=2

Melhorias na Cifra de Vegenère

- considere uma chave do tamanho do texto aberto, isto é, $|m| = |K|$
- sorteie K aleatoriamente
- tamanho da chave? Pode-se utilizar a chave mais de uma vez?

Melhorias na Cifra Monoalfabética $\times$ Cifra de Hill

- Cifra Monoalfabética mantém a frequência das letras no texto cifrado, pois uma letra é sempre mapeada na mesma letra
- Cifra de Hill possui uma relação linear entre texto aberto e cifrado
- Considere a cifra monoalfabética aplicada em bloco
- Quantas permutações existem para blocos de 2 letras? 3 letras?
- Quantos bits são necessários para a chave?