# Criptografia Simétrica

## Segurança e Auditoria em Sistemas

Profa. Natássya Barlate Floro da Silva

Universidade Tecnológica Federal do Paraná -– Câmpus Cornélio Procópio

10 de Março de 2020

# Roteiro

1. Técnicas de Transposição
   - Cerca de Trilho
   - Cifra de Transposição

# Cerca de Trilho

- Texto claro escrito como uma sequência de diagonais e lido como uma sequência de linhas.
- Exemplo com profundidade 3:

c p g f e e o
r t r i a l r
i o a a m h

Texto cifrado: cpgfeeortialrioaamh

# Cifra de Transposição

- Escrita do texto claro em um retângulo e leitura das colunas na ordem definida pelas chaves.
- Exemplo:

| | |
|---|---|
| Chave: | 4 1 3 2 5 |
| Texto claro: | c r i p t |
| | o g r a f |
| | i a e a m |
| | e l h o r |
| Texto cifrado: | rgalpaaoirehcoietfmr |

# Cifra de Transposição

- Criptoanálise é facilitada pois basta escrever o texto cifrado em matrizes e alterar suas colunas.
- A cifra se torna bem mais segura quando são realizados mais de um estágio de transposição, aplicando-se o algoritmo novamente no texto cifrado.
- Exemplo: (continuação)

| | |
|---|---|
| Chave: | 4 1 3 2 5 |
| Texto claro: | r g a l p |
| | a a o i r |
| | e h c o i |
| | e t f m r |

Texto cifrado: gahtliomaocfraeeprir

# Exercício

## Exercício

Faça a criptoanálise encontrando o texto claro e a chave das seguintes mensagens:

- Cifra de Transposição com um estágio e chave de tamanho 3: iaegnm
- Cifra de Transposição com dois estágios e chave de tamanho 5: aranunitlg