INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TRIÂNGULO MINEIRO
CAMPUS – Uberlândia-Centro

RESENHA CRÍTICA

Técnicas de transposição e máquina de rotor

Carlos Regis de faria

Uberlândia Mg
2020

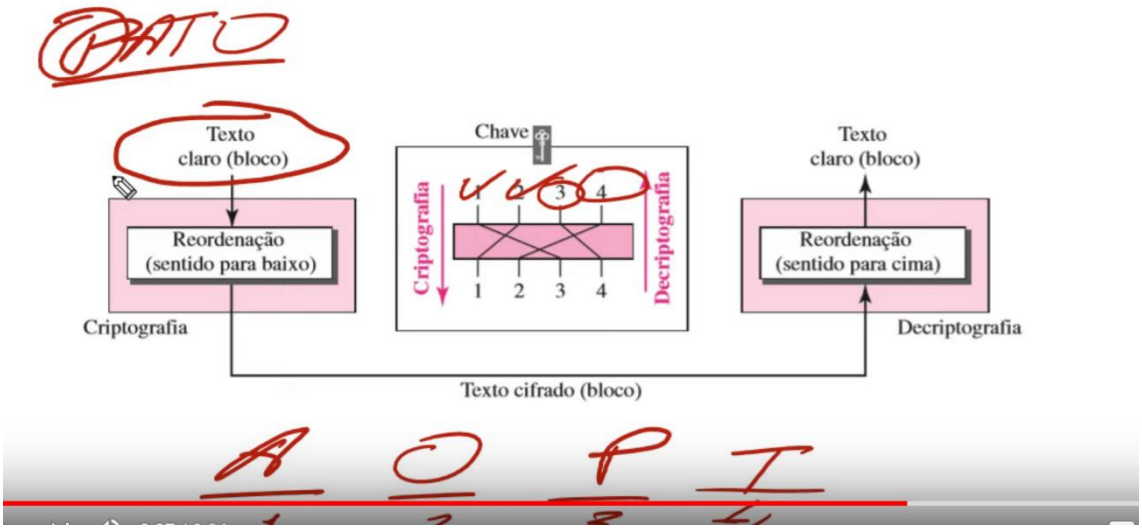
As técnicas de criptografia existiam muito antes de se pensar em computador. Foi uma técnica utilizada para envio de mensagens criptografadas entre Reis, imperadores e seus exércitos. Durante a segunda guerra mundial, nazistas alemães criaram a Enigma uma máquina considerada por eles alemães como indecifrável. E que realmente foi por muito tempo até que um belo dia um jovem matemático a serviço da inteligência britânica consegui o inimaginável decifrando seu algoritmo e dando vantagens aos aliados a partir desse momento por obterem informação valiosa. Há quem diga que esse fato encurtou a guerra em dois anos.

Nessa resenha falaremos sobre duas técnicas. Ambas como os mesmos objetivo criptografar mensagens, porém com características diferentes.

A técnica de transposição é obtida fazendo permutação entre seus elementos. Sua regra básica e misturar a ordem dos caráteres de um texto puro tornando o sem sentido para quem não conhece a regra. Um exemplo seria

Seu ponto fraco seria a facilidade em decifrar o algoritmo visto que é uma técnica primaria e para os dias de hoje um bom programa de computador ou até mesmos sites na internet podem facilmente quebrar seu algoritmo.

Exemplo de transposição da palavra Gato



Observe que foram alteradas as ordens dos caracteres formando AOPT que para leigos não faz nenhum sentido.

A máquina de rotor seria a criptografia da criptografia da criptografia. Várias etapas de criptografia para produzir um único algoritmo. Um número elevado de combinações que mesmo nos dias atuais seria muito difícil decifrar seu algoritmo.

Durante a segunda guerra os alemães utilizaram-se uma máquina de rotor chamada **Enigma** que teve seu código decifrado por Allan M Turing depois de anos de pesquisas. A quebra desse código foi um fator determinante para o final da guerra.

Pontos forte dificuldade em decifrar seu algoritmo pois as possibilidades são imensas e talvez o tempo não permitiria tal operação.

Como se pode observar criptografia não é um termo relacionado a computadores, é uma técnica utilizada a milhares de anos com objetivo de proteger a informação. Mesmo a milhares de anos como por exemplo na época do império romano Júlio Cesar desenvolveu um algoritmo de criptografia com o objetivo de proteger a informação. Portanto o tema segurança da informação sempre existiu.