1° Cifra Playfair

A cifra Playfair é uma substituição polialfabética em bloco bigrâmico (ou digrâmico). Nesta substituição, as letras são tomadas duas a duas (bloco bigrâmico), de acordo com regras aplicadas a uma grade de 5 por 5 que contém o alfabeto cifrante.

A segurança desta cifra é baixa e seu interesse é apenas histórico. A criptoanálise pode ser feita através da análise da frequência de dígrafos. Por ser uma cifra polialfabética, a Playfair dificulta um pouco a criptoanálise e, por ser uma cifra de dígrafos, é preciso fazer uma análise da frequência de dígrafos. Como existem mais dígrafos do que letras, o número de elementos disponíveis para a análise diminui. Por exemplo: numa mensagem de 100 letras, cifrada com uma substituição simples, temos 100 elementos derivados de uma escolha de 26; numa mensagem de 100 letras, cifrada em dígrafos, temos 50 elementos derivados de uma escolha de 676.

A Playfair possui outras vantagens: não precisa de tabelas ou dispositivos complicados, possui uma palavra-chave que pode ser memorizada ou trocada com facilidade, é muito fácil de ser implementada e pouco sujeita a erros. Devido a estas características o sistema é perfeito para ser usado como uma “cifra de campo”.

2° Cifra de Hill

é um tipo de cifra de substituição baseado em álgebra linear usado para codificação de mensagens. Foi inventada pelo matemático norte americano Lester S. Hill em 1929.

Máquina de Cifra de Hill

Uma mensagem codificada com uma matriz NxN é chamada de “N-Cifra de Hill”. Logo, uma mensagem codificada com uma matriz 2x2 é chamada “2-Cifra de Hill”.

CODIFICAÇÃO:

Primeiro converte-se as letras em números, depois agrupa-se os números n a n e multiplica-se cada grupo por uma matriz quadrada de ordem invertível (ou seja determinante diferente de 0). Os números resultantes são novamente passados para letras, e assim tem-se a mensagem codificada.

Caso algum resultado da multiplicação seja um número maior que o número de letras do alfabeto utilizado, então deve-se utilizar o resto desse número pelo número de letras do alfabeto.

Numerar cada letra do alfabeto de 1 a 25 e daremos o valor de 0 a letra A. Cada letra é representada por um número módulo 26. Embora esta não seja uma característica essencial da cifra, este esquema simples é frequentemente usado: [2]estará bem determinada por seu número correspondente.

EXEMPLOS DE CHAVES SIMETRICAS E ASSIMETRICAS UTILIZADOS HOJE EM DIA

Algoritmos de Criptografia Simétrica:

1. Blowfish: Um algoritmo de chave simétrica que usa chaves variáveis de 32 a 448 bits. É rápido e ainda é amplamente usado em software de segurança e criptografia de dados.

2. ChaCha20: Um algoritmo de fluxo simétrico moderno que oferece alta segurança e desempenho superior ao AES em dispositivos móveis e sistemas com menos recursos.

Algoritmos de Criptografia Assimétrica:

1. DAS (Digital Signature Algorithm): Usado principalmente para a criação de assinaturas digitais, o DAS é um padrão adotado pelo governo dos EUA para autenticação e integridade de dados.

2. ElGamal: Baseado no problema do logaritmo discreto, o ElGamal é usado para criptografia de chave pública e é frequentemente empregado em sistemas de assinatura digital.