

Marco Petry 1930800

Como é feita a geração da chave?

A geração da chave é feita com base no tamanho do texto a ser criptografado. É gerado cada character randômico com base na tabela ASCII, depois convertido para binário equivalente.

Após isso, é realizada a operação de ou exclusivo para cálculo do texto criptografado e armazenado. Para descriptografá-lo, é só realizar a operação inversa.

O algoritmo de Vernam é vulnerável à análise de frequências?

Não é vulnerável a análise de frequências pois não segue um padrão para toda a criptografia. Cada caractere tem uma chave aleatória correspondente, logo, não tem cálculo matemático preciso para realizar uma análise de frequência no texto e encontrar algum padrão.