Disciplina: Segurança e Auditoria em Sistemas (SA28S)

Estudante: Gabriel Lopes Guilherme

Cifrador de Vernam

1) **Como é feita a geração da chave?**

   A geração da chave é feita através de um loop (for), que vai de 0 até o tamanho da mensagem passada para ser cifrada, esse loop fica responsável por gerar um número aleatório de 0 até 1000 e recuperar o carácter equivalente ao número gerado e acrescentar esse carácter a chave até completar o mesmo tamanho da mensagem.

2) **O algoritmo de Vernam é vulnerável à análise de frequências?**

   O algoritmo de Vernam não é vulnerável à análise de frequência, pois a mensagem cifrada é gerada a partir de uma chave aleatória, e não de uma mudança de posição como é feita no Cifrador de César. Para poder decifrar a mensagem cifrada pelo algoritmo de Vernam, é necessário ter a chave aleatória que foi gerada para cifrar a mensagem.