Gabrieli Pereira Machado - 2003260

Segurança e Auditoria em Sistemas - Cifradores Simétricos - CCH 01
Cifrador de Vernam

• Como é feita a geração da chave?
• O algoritmo de Vernam é vulnerável à análise de frequências?

Neste projeto foi escolhida a linguagem JavaScript, pois possui diversas formas de criar strings aleatórias como chave onde é utilizada para o cifrador de Vernam, tendo como principal ponto a chave aleatória utilizada na sua criptografia, que é aplicada no texto para produzir a mensagem cifrada.
Essa cifra usa como chave um texto que nunca é repetido e que possui o mesmo tamanho da mensagem, uma das maneiras mais eficientes de gerar esta chave em JS é o método nativo *String.fromCharCode()* que retorna uma string criada ao usar uma sequência específica de valores Unicode. O cifrador de Vernam concatena cada um dos valores aleatórios gerados pelo tamanho do texto através de um laço *for.*
O Algoritmo de Vernam tem uma mensagem criptografada a partir de cada caractere de uma chave gerada na sua execução e não possui um padrão de deslocamento. Só é possível decifrar o Algoritmo de Vernam através da chave utilizada para criar a mensagem criptografada, o que o torna não vulnerável à análise de frequências, pois a mesma não suportaria a quantidade aleatoriedade na cifra.