Universidade Tecnológica Federal do Paraná - UTFPR

Engenharia de Software - Disciplina de Segurança e Auditoria em Sistemas (SA28S)

Ricardo Andreis Balbinot, 1932888

CCH 1: Cifradores Simétricos

Sobre Cifradores de Vernam:

1 - Como é feita a geração da chave?

Um dos parâmetros fundamentais para o funcionamento do Cifrador de Vernam é a chave utilizada na criptografia. Essa chave tem que ter o mesmo número de caracteres que a frase fornecida e deve ser aleatória o bastante para não ser identificada.

A linguagem escolhida para o desenvolvimento do cifrador é o JavaScript. Com JS, várias maneiras podem ser utilizadas para criar uma string aleatória a ser utilizada como chave. Uma delas, sendo umas das utilizadas, trata do método nativo *String.fromCharCode()*, que retorna um valor do tipo string a partir de um valor Unicode.

No Cifrador de Vernam construído na ACCH 1, foi utilizado o método descrito acima para retornar uma string a partir de um *unicode* aleatório, sendo ele um valor inteiro aleatório de 0 a 1000. Cada um desses caracteres aleatórios foram concatenados um a um até a chave criada estar do mesmo tamanho da frase fornecida (utilizando um laço de repetição *for*). Essa chave, quando executado o comando de cifra com o parâmetro "-c", é criada e armazenada no arquivo fornecido.

2 - O algoritmo de Vernam é vulnerável à análise de frequências?

O algoritmo de Vernam não é vulnerável à análise de frequências, como acontece por exemplo com o Cifrador de César. Isso se dá pois, diferentemente do Cifrador de César, que tem um deslocamento padrão em comum para todos os caracteres, o Algoritmo de Vernam tem sua mensagem criptografada criada a partir de cada caractere de uma chave aleatória gerada na sua execução. Sendo assim, a análise de frequência não funcionaria com um número tão elevado de aleatoriedade na cifra, sendo possível decifrá-lo apenas fazendo uso da chave que foi usada para criar a mensagem criptografada