Universidade Tecnológica Federal do Paraná (UTFPR)
Departamento Acadêmico de Informática (DAINF)

Introdução à Criptografia

Professor: Rodrigo Minetto (rodrigo.minetto@gmail.com)

Lista de exercícios

1) Codifique o algoritmo RC4 e decifre o conteúdo do arquivo '**cifrado.txt**' que foi criptografado com a chave '**rodrigo**'. Os caracteres de espaço e nova linha também foram cifradosm, não os trate de maneira diferente. Também não converta os caracteres para nenhum intervalo, use os tal como forem lidos. Em anexo ao material da aula existem alguns protótipos em C, Python e Java.

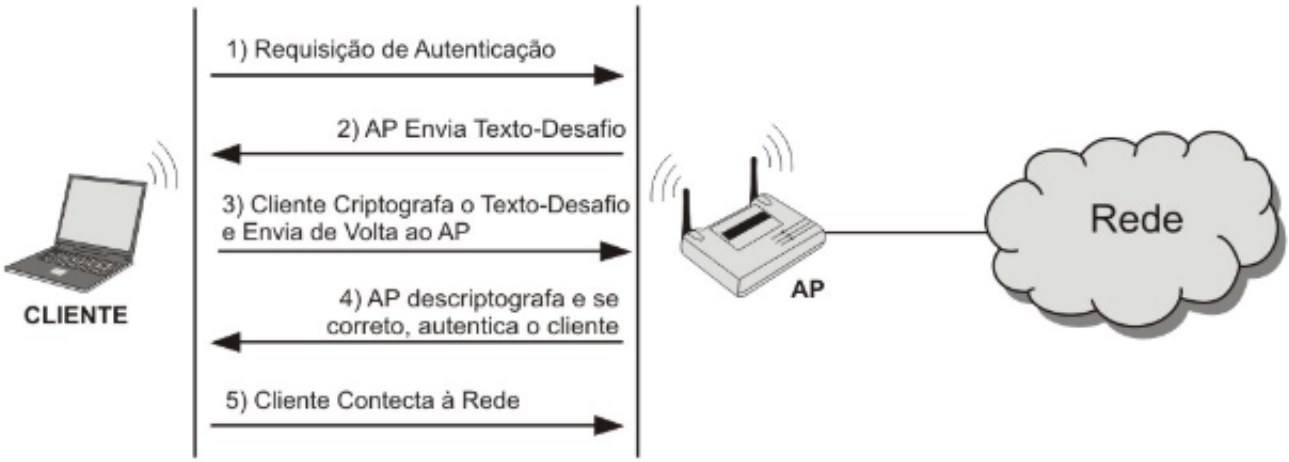
2) Qual o valor de chave que não embaralha o vetor **S** durante a inicialização? Ou seja, após a execução do algoritmo KSA, os valores no vetor **S** permanecem em ordem crescente de 0 a 255.

3) Qual o número de estados diferentes que o algoritmo RC4 pode produzir na inicialização pelo KSA? Por exemplo

```
0 1 2 3 ... 254 255 (primeiro estado)
0 1 2 3 ... 255 254 (segundo  estado)
...
```

4) Pesquise o porque do protocolo WEP adicionar um IV (initialization vector) junto com a senha secreta da rede antes de utilizar o algoritmo RC4. Liste as redes de internet Wi-Fi para determinar que tipo de algoritmo criptográfico utilizam.

5) O protocolo de autenticação WEP é realizado da seguinte forma:



Discuta como um ataque pode ser realizado nesse cenário.

6) Pesquise e descreva o uso do algoritmo RC4 em Ransomwares.