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

Introdução à Criptografia

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

Lista de exercícios (escolha 4 exercícios para entregar)

1) Codifique um algoritmo de cifra de fluxo **COM** a função XOR (funções de decifra-mento e ciframento). Para testar seu programa decifre o arquivo "**cifra_xor_a.txt**". Note que a sequência de chaves geradas deve ser idêntica para que o deciframento ocorra com sucesso. Assim, utilize o programa "**aleatorio.c**" para gerar as chaves e não utilize nenhuma semente. Ignore espaços e quebras de linha. As letras a, b, ..., z são representadas pelos números 0, 1, ... 25 (assim para cada caractere do texto lido faça: caractere - 'a'), também force os números aleatórios a ficarem no intervalo 0, 1, ... 25 (aleatorio() % 26).

2) A primeira vista, podemos pensar que um ataque por exaustão de chaves pode funcionar contra um sistema OTP. Por exemplo, suponha uma mensagem de 5 caracteres ASCII, representada por 40 bits, que foi cifrada utilizando um OTP de 40 bits. Explique exatamente porque um ataque por exaustão de chaves não vai funcionar contra esse ciframento, mesmo que os recursos computacionais sejam infinitos. Isto é um paradoxo pois é provado que a cifra OTP é incondicionalmente segura. Nota: você tem que resolver esse paradoxo. Respostas como: O OTP é incondicionalmente seguro e por isso um ataque por força bruta não vai funcionar não são válidas.

3) Suponha que Alice e Bob desejam trocar uma mensagem mas não possuem meios seguros para trocar uma chave. Então Alice tem a seguinte ideia:

- Alice faz $c_1 = m \oplus a$, e envia c_1 para Bob.
- Bob faz $c_2 = c_1 \oplus b$, e envia c_2 para Alice.
- Alice faz $c_3 = c_2 \oplus a$, e envia c_3 para Bob.
- Bob faz $m = c_3 \oplus b$, e recupera a mensagem m de Alice.

Esse protocolo para troca de mensagens é seguro? Explique.

4) Suponha uma cifra OTP semanticamente segura com espaço de chaves $K = \{0,1\}^\ell$. Um banco deseja quebrar a chave de deciframeno $k \in \{0,1\}^\ell$ em duas partes p_1 e p_2 de tal forma que ambas as partes são necessárias para a decifragem. A parte p_1 deve ser dada para um executivo e a parte p_2 a outro de tal forma que ambos precisam combinar suas partes para prosseguir com o deciframento.

O banco produz aleatoriamente $k_1 \in \{0,1\}^\ell$ e faz ${k_1}^* = k \oplus k_1$. Observe que $k = {k_1}^* \oplus k_1$. Assim, o banco pode dar k_1 para um executivo e ${k_1}^*$ para outro, e ambos devem estar presentes para o deciframento, pois cada chave individual não contém informação sobre a chave secreta k (note que cada parte da chave é um ciframento OTP de k).

Agora, suponha que o banco deseja quebrar k em três partes p_1, p_2 e p_3 de tal forma que duas partes permitam o deciframento de k. Isto assegura que mesmo que um executivo estiver doente, o deciframento pode prosseguir. Para realizar tal tarefa o banco produz aleatoriamente $(k_1, {k_1}^*)$ e $(k_2, {k_2}^*)$ conforme explicado anteriormente e que respeite $k_1 \oplus {k_1}^* = k_2 \oplus {k_2}^* = k$. Como o banco deve distribuir as partes, de tal maneira que duas partes qualquer possam decifrar utilizando o k, mas nenhuma parte sozinha consiga decifrar? Ou seja, qual das alternativas a seguir permite isso?

- (a) $p_1 = (k_1, k_2)$, $p_2 = ({k_1}^*, {k_2}^*)$, $p_3 = ({k_2}^*)$
- (b) $p_1 = (k_1, k_2)$, $p_2 = (k_2, {k_2}^*)$, $p_3 = ({k_2}^*)$
- (c) $p_1 = (k_1, k_2)$, $p_2 = ({k_1}^*, k_2)$, $p_3 = ({k_2}^*)$
- (d) $p_1 = (k_1, k_2)$, $p_2 = (k_1, k_2)$, $p_3 = ({k_2}^*)$
- (e) $p_1 = (k_1, k_2)$, $p_2 = ({k_1}^*)$, $p_3 = ({k_2}^*)$

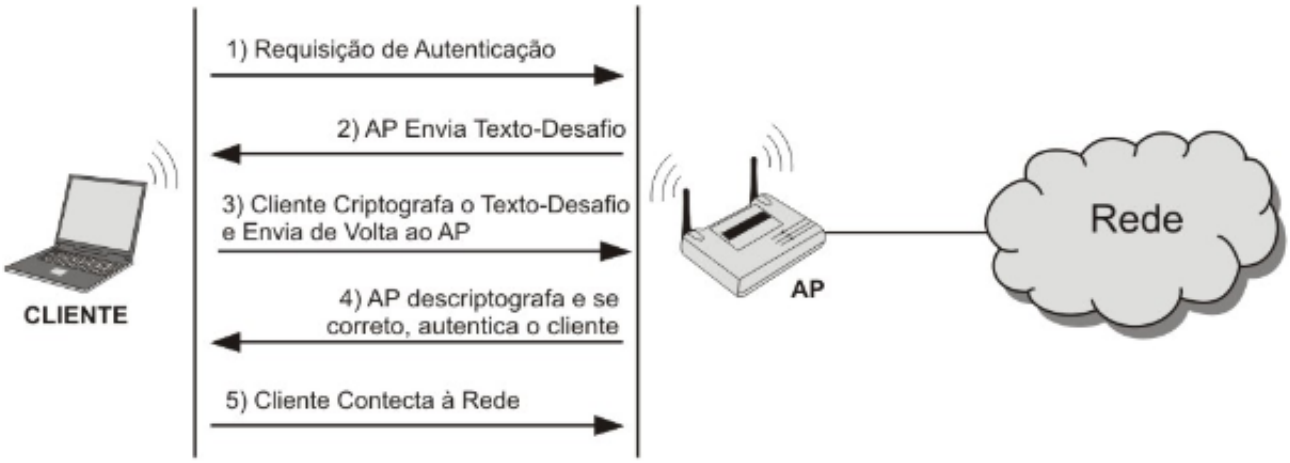
5) Codifique o algoritmo RC4 e decifre o conteúdo do arquivo '**cifrado.txt**' que foi criptografado com a chave '**rodrigo**'. Os caracteres de espaço e nova linha também foram cifradosm, não os trate de maneira diferente. Também não converta os caracteres para nenhum intervalo, use os tal como forem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

6) 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)
...
```

7) 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.

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



Discuta como um ataque pode ser realizado nesse cenário.

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