Pontifícia Universidade Católica de Minas Gerais
ICEI – Engenharia de Software
Unidade Praça da Liberdade
Disciplina: Projeto e Análise de Algoritmos
Professor: Sandro Jerônimo de Almeida

Lista de Exercícios I – Parte B (2 Pontos)

1- Seja S_k (M) o algoritmo de criptografia de substituição (*Método de César)* que criptografa M usando a chave k. Seja T_y (N) um algoritmo de criptografia de Transposição que criptografa N usando a chave y.

a) Criptografe Z usando o algoritmo de criptografia H_{yk} (Z) = (T_y (S_k (Z)).
Z deverá ser primeiro seu nome. Escolha os valores das chaves y e k a seu critério.
b) Descriptografe Z posteriormente.

2- Criptografe e descriptografe o seu primeiro nome usando o algoritmo RSA. Indique os valores adotados para os parâmetros do algoritmo (p, q, z, d, e, n). Utilize a codificação a=1, b=2, c=3,..,z=26).

3- Discorra sobre a complexidade de quebra da criptografia dos seguintes algoritmos:

a) Método de Substituição (Monoalfabética)
b) Método de César
c) Cifra de Vigenère
d) RSA

4- Determine o tempo necessário para quebrar uma senha de 8 dígitos utilizando sistema de força bruta e uma máquina com capacidade de testar cada senha em 1 milésimo de segundos. Sabe-se que a senha poderá ser composta por número (0-8), letras maiúsculas e minúsculas.

5- Seja a função $f(x) = ax^2 + bx + c$, uma função de criptografia. Responda: a função *f(x)* é adequada para ser utilizada como método de criptografia simétrico? Justifique sua resposta.

6- As questões a seguir foram retiradas, parcialmente, da Prova de conhecimentos específicos para o cargo de Perito Criminal - Área 3 (Computação científica) – do concurso da Polícia Federal. Julgue cada item das questões como Certo (C), Errado (E) ou deixe o item “em branco”.

6.1) As técnicas de criptografia constituem os recursos básicos para implementação de boa parte das ferramentas que disponibilizam serviços de segurança para os níveis de rede, sistema e serviços (aplicações). Assim, os riscos para cada serviço de segurança estão muitas vezes associados aos riscos de quebra dos sistemas e algoritmos criptográficos utilizados. Acerca de técnicas de quebra de sistemas e algoritmos criptográficos e seus riscos, julgue os itens a seguir.

a) ____ A quebra de sistemas criptográficos simétricos sempre depende exclusivamente da descoberta da chave secreta utilizada no processo criptográfico.

b) ____ Um princípio básico para a utilização de senhas em serviços de segurança, tais como autenticação e controle de acesso, consiste em não armazenar a senha diretamente pois o acesso a tal entidade de armazenamento poria em risco toda a segurança do sistema. Ao contrário, é armazenado um resumo da senha, gerado normalmente por algum tipo de função digestora unidirecional. Ataques de força bruta a esses sistemas podem ser bem sucedidos, caso se encontre a mensagem original utilizada na entrada da função (isto é, a senha) ou alguma outra mensagem que resulte em um mesmo resumo que aquele gerado para a mensagem original.

c) ____ Chaves criptográficas consideradas seguras contra ataques de força bruta, para os padrões de processamento atuais, devem possuir pelo menos 128 bits, tanto para criptografia simétrica quanto para criptografia assimétrica.

6.2) Um sistema criptográfico é constituído por uma tripla (M,K,C), em que M é o espaço das mensagens, K é o espaço das chaves, e C é o espaço dos criptogramas. Associado a esses, tem-se um algoritmo criptográfico, o qual transforma qualquer mensagem $m \rightarrow M$ em um criptograma $c \rightarrow C$, de forma controlada por uma chave $k \rightarrow K$. Pode se representar essa transformação por $c = E_k(m)$, que corresponde à operação de cifração, e por $m = D_k(c)$, a operação inversa, de decifração. A respeito de sistemas criptográficos em geral, julgue os itens subseqüentes.

a) ____ Em um determinado sistema criptográfico, para cada mensagem possível m, existe apenas um criptograma possível, c, que será o resultado da cifração de m com determinada chave k. Não obstante, mensagens distintas podem resultar em um mesmo criptograma, se utilizadas chaves distintas.

b) ____ Sistemas criptográficos são ditos simétricos ou de chave secreta quando a chave utilizada para cifrar é a mesma utilizada para decifrar. Sistemas assimétricos ou de chave pública utilizam chaves distintas para cifrar e decifrar. Algoritmos simétricos são geralmente mais eficientes computacionalmente que os assimétricos e por isso são preferidos para cifrar grandes massas de dados ou para operações on-line.

c) ____ Diz-se que um sistema criptográfico tem segredo perfeito quando, dado um criptograma c, a incerteza que se tem em relação à mensagem m que foi cifrada é a mesma que se tinha antes de conhecer o criptograma. Uma condição necessária para que um sistema criptográfico tenha segredo perfeito é que o espaço de chaves seja pelo menos tão grande quanto o espaço de mensagens, ou seja, $|K| = |M|$.