Universidade Tecnológica Federal do Paraná
Departamento de Eletrônica
Disciplina: Teoria da Informação
Professor: Dyson Pereira Junior

Exercícios para a Segunda avaliação

1) Marque *V* ou *F*.
a) ( ) Em uma criptografia de simétrica, a chave deve permanecer secreta em ambos os nós de comunicação.
b) ( ) Uma função unidirecional é difícil de calcular, mas fácil de se inverter.
c) ( ) Em uma criptografia de chave pública, a chave de ciframento *k* não precisa ser mantida secreta, ela pode ser tornar pública.

2) Cifrador de *Vigenère* – Um cifrador do tipo *Vigenère* possui os dados abaixo:
Espaço de mensagem $X = \{0, 1, ..., 25\}$
Espaço de texto cifrado $Y = \{0, 1, ... , 25\}$
Espaço da chave $k = \{0, 1,..., 25\}$
A função de deciframento: $E(X,Y) = (X+k)\ mod\ n$
Determine a função de deciframento.
Cifrar o seguinte texto usando a chave *hello* e assumindo que $n = 26$. Escreva sua resposta com blocos de 5 caracteres, ignore os espaços. Mostre os seus passos brevemente.

UNIVERSIDADE TECNOLOGICA

3) Assumir que dois usuários querem estabelecer uma chave secreta comum através de um canal inseguro usando um protocolo de troca de chave de *Diffie-Hellman*. A chave privada para o usuário *A* é 11 e para o usuário *B* é 14. Considere um número primo comum 17.
a) Encontre o menor elemento primitivo para $p = 17$. (Mostre seus passos).
b) Obtenha a chave comum usando o elemento primitivo encontrado acima (Mostre os seus passos).

4) Sistema *RSA* – O sistema *RSA* foi usado para cifrar a mensagem *M* no texto cifrado $C = 9$. A chave pública é dada por $n = 143$ e $e = 23$. Nós tentaremos quebrar o sistema e determinar a mensagem original *M*.
- Quais os parâmetros que englobam a chave pública e quais os parâmetros que englobam a chave privada?
- Quais passos são necessários para determinar a chave privada da chave pública?
- Determine a chave privada para o sistema dado.
- Qual é a mensagem original *M*?

5) (Troca de chaves *Diffie-Hellman*) – Assumir que dois usuários querem se comunicar usando ciframento simétrico. Cada um dos dois usuários possui uma chave privada que apenas ele conhece. Para o usuário *A* com chave privada 6, e usuário *B* com chave privada 12, e um número primo comum conhecido 71 e seu elemento primitivo 7, encontre a chave comum, e descreva o procedimento que os dois usuários irão usar para obter esta chave comum (ou seja, desenhe um diagrama seqüencial com todas as mensagens trocadas entre os dois, usando os valores específicos dados acima).

6) (Elementos Primitivos)
a) Explique em no máximo duas frases o que é um elemento primitivo.
b) Calcule o menor elemento primitivo para $p = 23$.

7) (*RSA*) – Por que a chave pública *c* e a chave privada *d* no ciframento *RSA* tem que satisfazer a equação $cd\ mod\ (p-1).(q-1) = 1$?
Tente explicar através de fórmulas em vez de texto, é muito mais fácil....

8) (Deciframento *RSA*) – Assumir uma chave pública para o deciframento *RSA* dada pelo par (143, 11). Encontre a chave privada para esta chave pública. Decodifique a mensagem (1114885711667), assumindo que as letras foram representadas por valores ASCII. Explique porque ninguém nunca usaria esta chave pública para um ciframento real, e o que poderia ser feito para torná-la realmente segura.

9) Considere o algoritmo *RSA*, em que a chave pública é (c, n) e a chave privada (d, n). Suponha que se escolheu $p = 7$, $q = 17$ e $c = 77$. Determine o valor de *d*.

10) Os interlocutores *Alice* e *Bob* usam o método *RSA* para cifrar as mensagens trocadas entre si. Admita que o usuário *Bob* publicou a sua chave pública (*c*, *n*).
a) Descreva o procedimento utilizado quando *Alice* pretende enviar uma mensagem a *Bob*.
b) Se pretendesse descobrir qual é a chave privada de *Bob* (*d*, *n*) qual seria o procedimento a seguir?
c) Suponha que a chave de *Bob* é (7, 33). Qual é a chave privada de Bob? Justifique a resposta.

11) Considere os métodos de ciframento clássicos baseados em substituição de caracteres.
a) Explique como funciona a cifra de César e de que forma é possível quebrá-la.
b) O método de cifra de *Vigenère* é uma forma de tornar as cifras de substituição mais resistentes à criptoanálise. Explique como funciona este método e indique como é que é possível quebrar cifras deste tipo.

12) Explique os princípios de operação do algoritmo *RSA* através de um exemplo em que $p = 3$ e $q = 11$. Diga qual é o valor numérico máximo que pode ser cifrado usando as chaves escolhidas.

13) Resuma o método de obtenção das chaves pública e privada usada pelo *RSA*. Explique, porque é que se forem usadas chaves com muitos bits é computacionalmente muito difícil quebrar esta cifra.

14) Indique as vantagens e inconvenientes dos métodos criptográficos com base em chave pública e privada (criptografia assimétrica) face à criptografia de chave secreta (criptografia simétrica).

15) Considere o método de ciframento *RSA*. Explique, por meio de um exemplo, a obtenção da chave pública e privada. Use para esse efeito os números primos 3 e 11. Indique o máximo valor numérico que pode ser cifrado usando a sua escolha de chaves.

16) Descreva resumidamente o método de ciframento *RSA*. Explique porque é que a chave privada é muito difícil de descobrir mesmo que se conheça a chave pública.