



UNIVERSIDADE FEDERAL DO CEARÁ

ENGENHARIA DA COMPUTAÇÃO CAMPUS SOBRAL

DISCIPLINA: REDE DE COMPUTADORES

ALUNO: KLAYVER XIMENES CARMO

MATRÍCULA: 427651

SOBRAL - CE

2021

AP3 - REDES DE COMPUTADORES 2021.1

1. [2,0 pts] No que concerne a Qualidade de Serviço (QoS) diferencie o funcionamento do algoritmo Leaky Bucket do algoritmo Token Bucket.

O **Leaky Bucket** (Balde furado) é um algoritmo que pode ser usado para determinar se alguma sequência de eventos discretos estão em conformidade com os limites definidos em suas taxas ou frequências médias e de pico, como um balde furado, onde a água pode entrar de forma variada, mas a saída flui de uma forma constante.

E comparando com um balde, se o balde estiver cheio, o pacote ou os dados serão descartados.

O algoritmo **Token Bucket** é utilizado em redes de computadores comutadas por pacotes e redes de telecomunicações. Podendo ser usado para verificar se as transmissões de dados, na forma de pacote estão de acordo com os limites definidos de largura de bandas e rajadas. Permitindo que a taxa de saída varie dependendo do tamanho do burst.

E diferente do Leaky Bucket, comparando com um balde, quando o balde estiver cheio, o token é descartado, mas não o pacote.

2. [2,0 pts] O que é um tráfego em rajada e quais os problemas que podem causar em uma rede?

O tráfego em rajada são os picos e vales inesperados em um volume de tráfego de dados e mudanças rápidas dos bits em pouquíssimo tempo. É um dos tipos de tráfegos mais difíceis para uma rede, por ser muito imprevisível, sendo os motivos principais das principais causas de congestionamento em uma rede.

3. [2,0 pts] Qual a função dos protocolos SMTP e FTP, e quais as numerações de portas utilizadas?

O SMTP (Simple Mail Transfer Protocol) é um protocolo de comunicação para transmissão de emails eletrônicos e define os procedimentos de comunicação entre um cliente e um servidor MTA (Message Transfer Agents) na internet. E as numerações de portas usadas são: 587, 465 e 25, porém no Brasil, a porta 25 foi fechada para diminuir o número de spams.

O FTP (File Transfer Programs) é um tipo de conexão que permite a troca de arquivos entre dois computadores conectados à internet e tem a função de copiar arquivos de um host para outro. As numerações de portas usadas são 21, para conexão de controle e 20 para conexão de dados.

4. [2,0 pts] Usando a cifra de Vigenère, decodifique a palavra “USJCNT” utilizando a chave “CODIF”:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Utilizando a cifra de Vigenère com a chave “CODIF”, a palavra decifrada da cifra “USJCNT” é “SEGUIR”.

5. [2,0 pts] O algoritmo de criptografia RSA possui as seguintes etapas:

- Escolher 2 números primos p e q
- Fazer $n = p \cdot q$
- $\Phi = (p-1) \cdot (q-1)$
- Escolher “ e ” aleatório que satisfaça a propriedade $(e \cdot d) \bmod \Phi = 1$
- Anunciar “ e ” e “ n ”; mantendo Φ e d secretos.

Foram escolhidos 3 e 7 como p e q , respectivamente, e 23 para “ e ” e 11 para d .

O texto cifrado é “11”. Qual o texto puro (original)? (use uma calculadora científica ou equivalente para auxiliar).

Texto 2.