Gabarito!

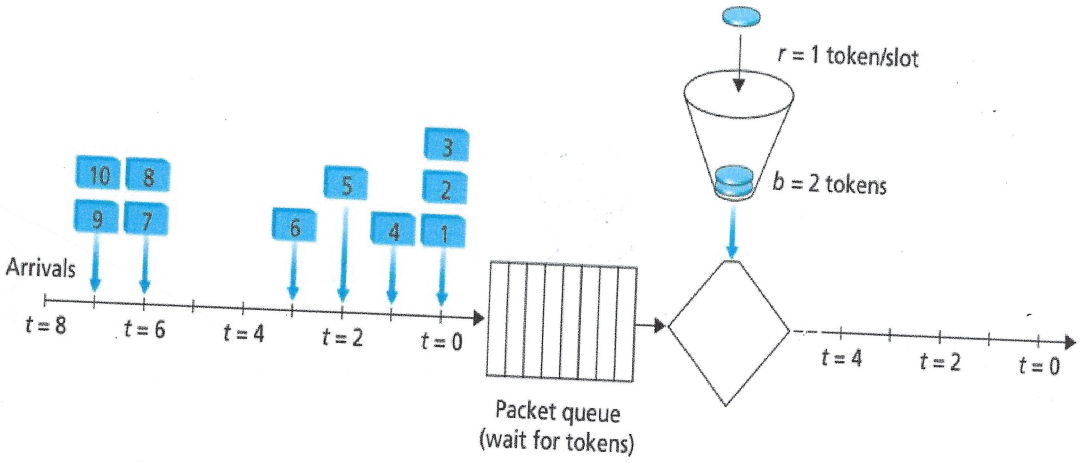
Escola Politécnica da Universidade de São Paulo
Departamento de Engenharia de Telecomunicações e Controle

Teste 5 de PTC2550 - Redes de Comunicação de Dados e Transporte Multimídia - 1o semestre 2017

Nome:_____ NUSP: _____

Assinatura: _____

1) Considere o seguinte policiamento balde de fichas que foi discutido em aula. O balde



inicialmente está cheio em $t = 0$. Considere dessa vez que $r = 2$ fichas/*slot*.

(a) Seguindo o que foi feito em aula, para cada *slot* de tempo, identifique os pacotes que estão na fila e o número de fichas no balde, imediatamente após as chegadas terem sido processadas mas antes dos pacotes terem passado a fila e retirado uma ficha. Assim, por exemplo, em $t = 0$, os pacotes 1, 2 e 3 estão na fila e existem 2 fichas no balde.

(b) Para cada *slot* de tempo indique quais pacotes são transmitidos após terem retirado uma ficha. Assim, por exemplo, em $t = 0$, os pacotes 1 e 2 são transmitidos.

2) Considere o RSA com $p = 7$ e $q = 13$.

a) Quais são os valores de n e z?

b) Seja $e = 17$. Essa é uma escolha aceitável para e?

c) Encontre d tal que $de = 1(\text{mod} z)$

d) Encripte a mensagem $m = 9$ usando a chave (n,e). Seja c o texto cifrado correspondente. Mostre todo o trabalho.

e) Mostre que decriptando-se c do item anterior obtém-se $m = 9$ novamente.

$N = rt + b$

t	balde (fichas)	fila
0	2	1 2 3
1	2	3 4
2	2	5
3	2	6
4	2	/
5	2	/
6	2	7 8
7	2	9 10
8	2	

0 - pacotes transmitidos no slot considerado

(2) (1) (2) (2) (1) (5)

(2) a) $n = 91$

$z = (p-1)\cdot(q-1) = 6 \cdot 12 = 72$ (2,0)

b) e não pode ter fatores comuns com z. Como 72 não é divisível por 17, $e = 17$ é aceitável (1,0)

c) $d = 17$

$17 \cdot 17 = 289$

$72 \cdot 4 = 288$

$d \cdot e \bmod z = 1$ (1,0)

d) $(n, e) = (91, 17)$

$C = m^e \bmod n = 3^{17} \bmod 91 =$

$= (3^{17} \bmod 91 \cdot 3^{17} \bmod 91) \bmod 91$

$= (61 \cdot 61) \bmod 91 = 81$ (1,0)

e) $m = c^d \bmod n = 81^{17} \bmod 91$

$= [(3^{17} \bmod 91)]^4 \bmod 91$

$= (61)^4 \bmod 91 = 9$ (1,0)