(points: 72; bonus: 24^b; time: 100')

Nome:

02/12/2019

Regras:

- I. Não vires esta página antes do começo da prova.
- II. Nenhuma consulta de qualquer forma.
- III. Nenhum aparelho ligado (por exemplo: celular, tablet, notebook, etc.).
- IV. Nenhuma comunicação de qualquer forma e para qualquer motivo.
- V. $(\forall x) [\text{Colar}(x) \implies \neg \text{Passar}(x, \text{FMC1})].^2$
- VI. Use caneta para tuas respostas.
- VII. Responda dentro das caixas indicadas.
- VIII. Escreva teu nome em cada folha de rascunho extra antes de usá-la.
 - IX. Entregue todas as folhas de rascunho extra, juntas com tua prova.
 - X. Nenhuma prova será aceita depois do fim do tempo—mesmo se for atraso de 1 segundo.
 - **XI.** Os pontos bônus podem ser usados para aumentar uma nota de qualquer unidade, dado que a nota original é pelo menos 5,0.3

Boas provas!

¹Ou seja, deslique antes da prova.

²Se essa regra não faz sentido, melhor desistir desde já.

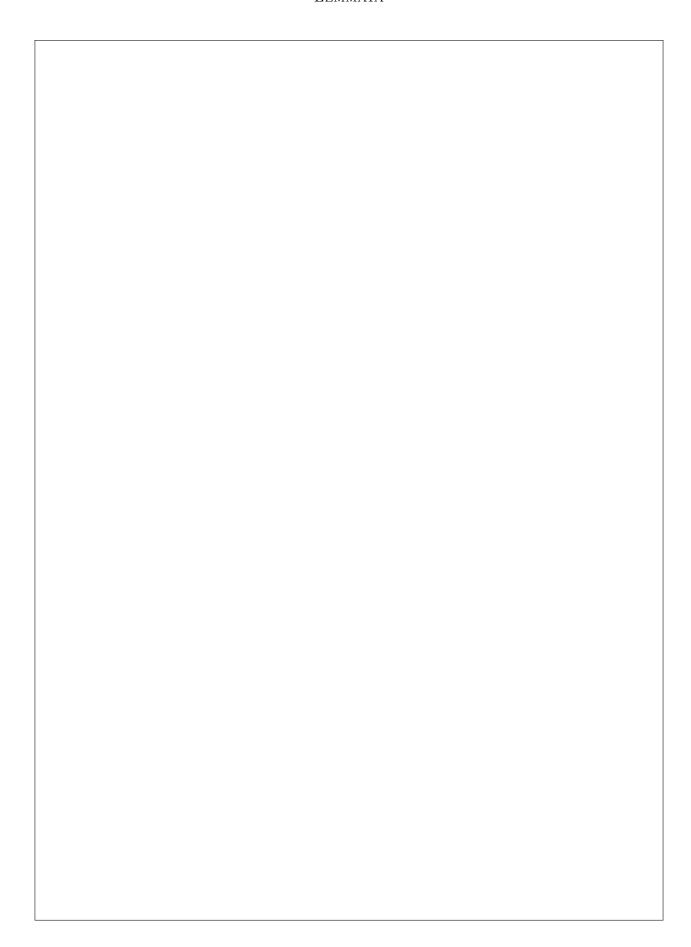
³Por exemplo, 25 pontos bonus podem aumentar uma nota de 5,2 para 7,7 ou de 9,2 para 10,0, mas de 4,9 nem para 7,4 nem para 5,0. A 4,9 ficaria 4,9 mesmo.

DEMONSTRAÇÃO			
\mathbf{F}			
Uma anta (A) e ı	ım burro (B) querem comuni	icar com segurança,	usando o RSA.
A chave pública o	da A é o par $(e = 5, N = 65)$.		
Ela recebeu a me	nsagem do B criptografada (e	ciphertext): foi o 42.	
Qual a chave priv RESPOSTA.	vada da A? $(p, q, \varphi(N), d)$		
TEEST OS IA.			
		B mandou para A?	

(16) \mathbf{E}

(56)	G		
	Sejam p primo e m inteiro positivo. Demonstre completamente até um dos teoremas seguintes.		
(42)	G1. Para todo inteiro $a \text{ com } 1 < a < p, a^{p-1} \equiv 1 \pmod{p}$.		
(42)	G2. Para todo inteiro $a, a^p \equiv a \pmod{p}$.		
(56)	G3. Para todo inteiro a coprimo com m , $a^{\varphi(m)} \equiv 1 \pmod{m}$.		
(56)	G4. A função φ de Euler é multiplicativa.		
(42)	G5. Para todo natural n, n é primo se e somente se $(n-1)! \equiv -1 \pmod{n}$		
	Demonstração de		

LEMMATA



LEMMATA



RASCUNHO

RASCUNHO