Rever entrega do teste: Mini-teste 2

Utilizador	Bruno Filipe Jardim Machado .
Curso	[21-22] Teoria de Números Computacional
Teste	Mini-teste 2
Iniciado	25-05-2022 19:30
Entregue	25-05-2022 20:06
Estado	Concluído
Pontuação da tentativa	60 de 60 pontos
Tempo decorrido	35 minutos de 45 minutos

Pergunta 1 10 de 10 pontos

São pseudo primos de Euler de base 3

Pergunta 2 10 de 10 pontos

Dada a chave pública ElGamal (p, r, b)=(39957963614327378639, 13, 2518634842003570977), a cifração de mens=1234, com o parâmetro aleatório k=4321, é

Pergunta 3 10 de 10 pontos

Considere o primo p= 19 e o natural a= 4 . Então o número dos menores resíduos de ka maiores que p/2, com k entre 1 e (p-1)/2 é igual a ___.

Pergunta 4 10 de 10 pontos

Considere o primo p=4874199776762032183 e a raiz primitiva r=1564111718413659456 de p. O índice de 2063484835043722125 na base r é igual a

Pergunta 5 10 de 10 pontos

Dada a chave pública ElGamal (p, r, b)=(59879295262580794019, 2, 46532948489070777896) , sabendo que o índice de 46532948489070777896 na base 2 é igual a 26889797028840904448 a decifração de (31508193067819085597, 42769957659645449029) é igual a ___.

Pergunta 6 10 de 10 pontos

Indique todos os elementos que são raiz primitiva de 223

Segunda-feira, 20 de Março de 2023 19H02m GMT

← **OK**