|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nome: Pedro Gabriel Garcia Ribeiro Balestra | | |  |  | Matrícula: 1551 |  |
| Curso: GEC |  |  | Período: P8 |  | Matéria: T106 |  |

**Tarefa 05**

Admita que um computador A precisa estabelecer uma chave de criptografia com um computador B. Os dois irão usar o acordo de Diffie-Helman para tal. Ilustre as fases do estabelecimento da chave simétrica entre os dois computadores, mostrando os cálculos intermediários até a conclusão do estabelecimento da chave. Admita os seguintes valores: p = 33, g = 15, a = 4 e b = 18.

Chave de autenticação pré-compartilhada

Chave de autenticação pré-compartilhada

K

K =

K =

A =

Computador 2

Computador 1

ISAKMP  
(Opções de Segurança)

ISAKMP  
(Opções de Segurança escolhida)

ISAKMP  
(g,B)

ISAKMP  
(g,A)

AES

AES

#

K

AES 128 bits  
SHA-1  
MODP-p

AES 128 bits  
SHA-1  
MODP-p

a=4  
p=33  
g=15

b=18  
p=33  
g=15

B =

Cálculos realizados na plataforma [WolframAlpha](https://www.wolframalpha.com/).