

**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA**

**DO TRIÂNGULO MINEIRO – CAMPUS UBERLÂNDIA CENTRO**

**CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS PARA INTERNET**

**ROBERTO EUGENIO DOS SANTOS**

**“Algoritmo Diffie-Hellman”,**

**UBERLÂNDIA, MG**

**2019**

**ROBERTO EUGÊNIO DOS SANTOS**

**“Teste de Algoritmo Diffie-Hellman”,**

Conceito do Diffie-Hellman

Orientador: **Guilherme Moraes**

**UBERLÂNDIA, MG**

**201****9**

# Conceito diffie-hellman

Roberto e Sara queiram trocar e-mails secretos de forma segura. Porém, os dois nunca tiveram oportunidade de combinar uma PSK (Pre-Shared key) de forma segura. Como fazer?Vamos usar esse email como exemplo para entender melhor.

Roberto, vamos utilizar o algoritmo Diffie-Hellman para trocar uma [chave pública](http://pt.wikipedia.org/wiki/Chave_p%C3%BAblica). Esta chave, combinada com um algoritmo de criptografia [AES (Advanced Encryption Standard)](http://pt.wikipedia.org/wiki/AES), também conhecido por Rijndael, de 256 bits, fará com que o conteúdo de nossos e-mails sejam encriptados. Assim, só quem conhece a [chave privada](http://pt.wikipedia.org/wiki/Chave_privada) (que será gerada pelo algoritmo Diffie-Hellman e só nós vamos conhecer) poderá ler o e-mail.

**Passo a passo ficaria da seguinte forma:**

**1. Eu escolherei dois números que utilizaremos em comum. A = 11 e B = 7.**

**2. Escolho um número que só eu sei, que chamarei de X. Você também escolhe um número (não conte a ninguém), chamado de Y.**

**3. Eu aplico a seguinte fórmula: Ra = (AX) mod B. E vou te passar o resultado Ra.**

**4. Você aplica a mesma fórmula, substituindo X pelo seu número secreto Y. Rb = (AY) mod B. E você me passará o valor de Rb.**

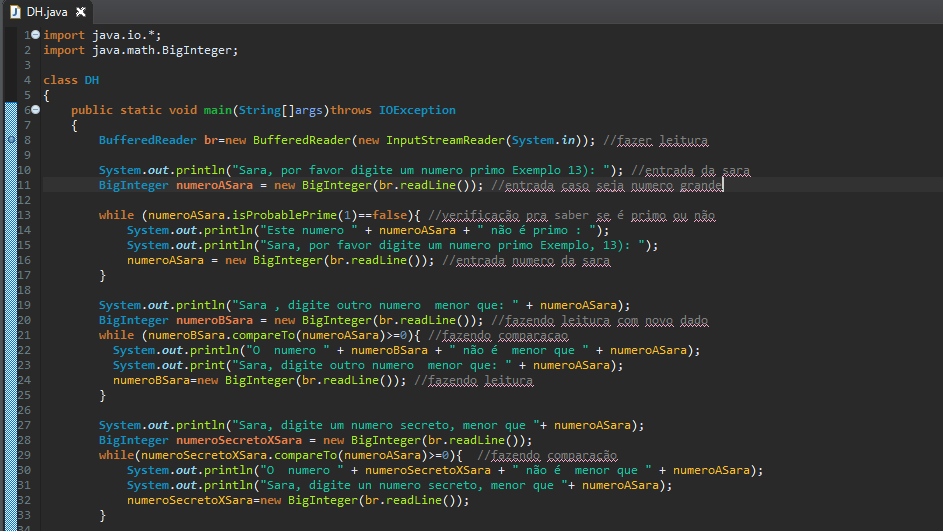
**5. Agora, eu aplico a seguinte fórmula para descobrir nossa chave privada: PSK = (RbX) mod B.**

**6. Para você descobrir a chave privada, use a fórmula: PSK = (RaY) mod B.**

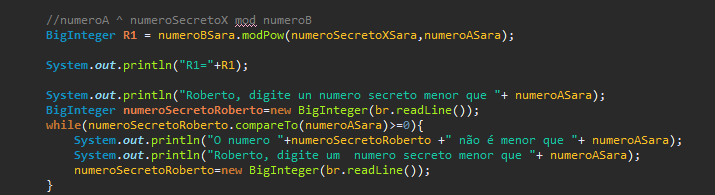
**7. Agora, é só nos dois utilizarmos a chave privada como insumo na função de criptografia AES.**

Mesmo se alguém souber A, B, Ra e Rb. Mesmo sabendo esses valores, ficará quase impossível alguém descobrir qual os números X ou Y que geraram a chave privada.

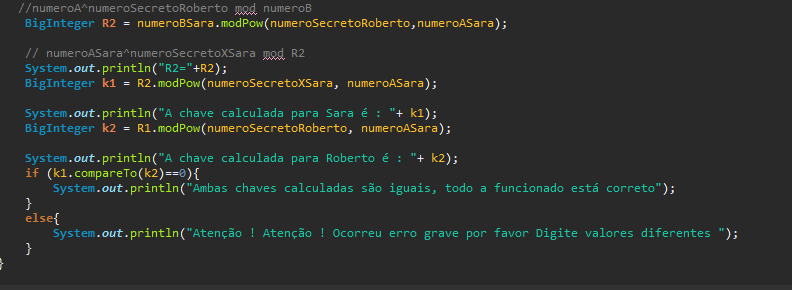
**Exemplo código em Java**



Entrada de numeroA, numeroB e o numero secreto escolhido pela Sara

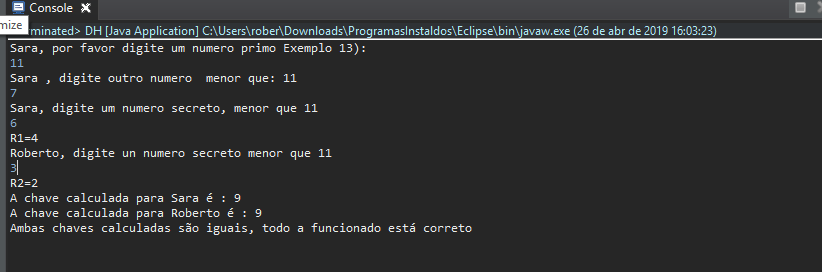


Calculando o valor de R1 da Sara, e logo abaixo o número secreto que o Roberto escolherá.



Calculando o valor de R2 do Roberto, e assim descobrindo o valor da chave1 e chave2 e com

isso comparando as duas chaves se estão iguais ou não

.Resposta do Algoritmo