Universidade Federal do Maranhão

São Luís, 21 de Novembro de 2019

Erickson Bruno Pereira Costa

**Algoritmo de Criptografia de Curvas Elípticas**

Este trabalho foi feito com o intuito de obtenção de nota na disciplina Introdução a Criptografia. O Algoritmo foi feito em linguagem de programação Python 3.

Imaginemos um cenário em que Bob precisa enviar uma mensagem para Alice. Ambos criam suas chaves (pública e privada). Bob disponibiliza sua chave pública a Alice e guarda sua chave privada em um local seguro, Alice faz o mesmo.

Para simular o breve cenário acima descrito, foram criadas três aplicações. A primeira, denominada CurvasElipticasCreateKeys.py é responsável pela criação das chaves pública e privada, esta por sua vez deve ser manipulada por ambas as partes, já que para criptografar uma mensagem Alice precisa da chave pública de Bob, sua própria chave privada e a mensagem clara. Para Bob descriptografar é necessário da sua própria chave privada, junto a mensagem criptografada.

O segundo programa, denominado CurvasElipticasCreateCrypt.py é responsável pela criptografia das mensagens, ele faz uso da chave pública da outra parte, da própria chave privada e do texto claro para criptografar as mensagens, salva em arquivo e envia ao destinatário.

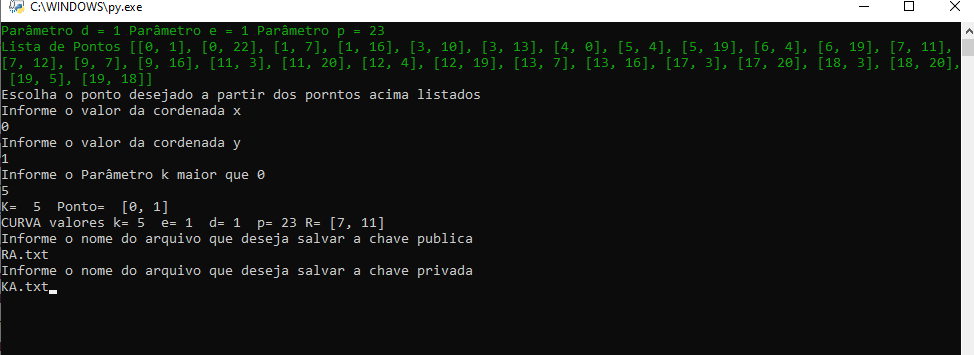
O terceiro e último programa é denominado CurvasElipticasCreateDecrypt.py e é responsável pela descriptografia das mensagens, o programa faz uso do arquivo contendo o texto criptografado e da própria chave privada para descriptografar a mensagem, salvando em arquivo o texto descriptografado.

**Usando os Programas**

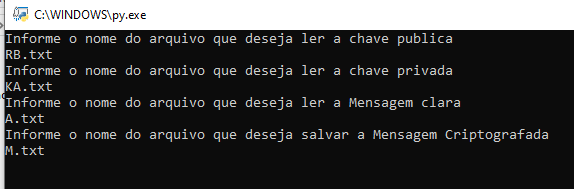
Para usar o programa CurvasElipticasCreateKeys.py basta clicar duas vezes no arquivo CurvasElipticasCreateKeys.py, ele abrirá o console python e lá você deve informar as coordenadas (x, y) referente ao ponto Q da curva E23(1,1) escolhido por ambas as partes, o inteiro k representando a chave privada escolhida. O programa irá calcular a chave pública R referente a sua chave privada k escolhida. Logo após o programa irá pedir pra informar o nome do arquivo para salvar a chave pública e o outro nome para o arquivo da chave privada. Repita o procedimento para ambas as partes (Alice e Bob), salvando as chaves com nomes diferentes. Caso queira visualizar o código basta abrir o arquivo usando um editor de código, como por exemplo VisualStudioCode.

Para usar o programa CurvasElipticasCreateCrypt.py basta clicar duas vezes no arquivo CurvasElipticasCreateCrypt.py, ele abrirá o console python e lá você deve informar o nome do arquivo da chave pública da outra parte. Exemplo Bob quer enviar uma mensagem para Alice, então Bob informa o arquivo referente a chave pública de Alice. Após isso o programa pedirá para Bob informar o nome do arquivo contendo a própria chave privada. Por fim o programa pedirá para informar o nome do arquivo da saída criptografada e ele salva.

Para usar o programa CurvasElipticasCreateDecrypt.py basta clicar duas vezes no script e ele abrirá o console python e pedirá para o usuário (ou o Bob como já comentamos) o nome do arquivo de chave pública (vale salientar que a chave pública contém os valores do ponto Q escolhido, e é só por isso que eu peço pro usuário informar), logo depois o programa pedirá para informar a própria chave privada, depois informar o nome do arquivo com a mensagem criptografada. O programa irá descriptografar a mensagem e salvar no arquivo cujo nome será informado pelo usuário.

Console programa CurvasElipticasCreateKeys.py. 

Console programa CurvasElipticasCreateCrypt.py



Console programa CurvasElipticasCreateDecrypt.py

