Curso de Extensão em Tecnologias Microsoft

INF0998 Programação segura (segurança de software)

Atividades práticas de criptografia aplicada

As seguintes ferramentas são usadas ao longo das tarefas deste conjunto de playbooks:

- Cryptool Online https://www.cryptool.org/en/cto
- Cryptool para Windows https://www.cryptool.org/en/ct1
- JCryptool https://www.cryptool.org/en/jct/
- OpenPGP, GPG4win e Kleopatra https://www.openpgp.org/software
- OpenSSL (Usar o openssl da sua distribuição Linux preferida)

Atividades com CrypTool e JCrypTool

Encriptação e decriptação com a cifra de César

Abrir um novo arquivo vazio pelo menu File → New → Empty file in Texteditor. Usar seu p´roprio nome como texto claro.

A transformação criptográfica sempre ocorre sobre a janela ativa.

Para realizar a encriptação, deve-se ativar a cifra de César no menu ***Algorithms*** → ***Classic*** → ***Caeser***.

- Na tela da cifra de César (Caesar), escolher a opção ***Encrypt***, conferir as configurações e clicar no botão ***Next***.
- Na tela de pré-processamento, selecionar a opção ***All characteres*** to uppercase e clicar no botão ***Finish***.
- O JCrypTool mostrará uma janela de saída com o criptograma. A transformação criptográfica acontece sobre a janela de texto ativa.

Para realizar a decriptação sobre a janela ativa, aquela com o criptograma.

- Ativar a cifra de César no menu ***Algorithms*** → ***Classic*** → ***Caeser***.
- Escolher a opção ***Decrypt***. Usar as configurações padrões. Clicar em ***Finish.***
- A transformação criptográfica acontece sobre a janela de texto ativa, aquela com o criptograma.

Análise de frequência das cifras clássicas

Esta atividade usa a ferramenta JCrypTool para fazer a análise de frequência de um texto encriptado com a cifra de César e com a cifra de Vigenère. Realizar os passos a seguir:

- Na janela principal da JCrypTool, ativar a opção de menu *File* → *Open File*.
- Na janela de seleção de arquivos, selecionar o arquivo CancaoDoExilio.txt. Clicar no botão *OK.*
- Escolher a cifra de César no Menu *Algorithms* → *Classic* → *Caesar*.
- Na tela da cifra de César (Caesar), conferir as configurações e clicar no botão *Next*.
- Na tela de pré-processamento, selecionar a opção *All characteres to uppercase* e clicar no botão *Finish*. O JCrypTool mostrará uma janela de saída com o criptograma.
- Com a janela do criptograma ativa, escolher análise de frequência no Menu *Analysis* → *Frequency Analysis*. Na janela que aparece, escolher a opção *Simply give me diagram and numbers*.
- Clicar no botão *Load Text, selecionar o texto da janela de output (algo do tipo out00X.txt)*.
- Analisar o histograma exibido.
- A letra *C* é a mais frequente do criptograma e corresponde a letra *A* do texto claro?

- Confirme esta hipótese fazendo a análise para o texto claro CancaoDoExilio.txt
- Opcionalmente, repetir a atividade para outro texto claro. Por exemplo, o arquivo exemplo do JCrypTool unsaved001.txt.

Repetir a atividade para a cifra de Vigenère com o texto claro CancaoDoExilio.txt. Escolher uma chave alfabética. Por exemplo, “abcd”.

- Com a janela do criptograma Vigenère ativa, escolher a criptoanálise no Menu *Analysis* → *Vigenere Breaker*.
- Na janela, escolher a opção *Manual Analysis* e clicar em *Finish*.
- Escolher o comprimento da senha (lembre, você usou ABCD, então o comprimento é 4). Clicar em *NEXT*.
- Na janela do histograma, clicar no botão “*Determine Automatically”*. Na janela de diálogo que aparece, substituir a senha sugerida (“*Sugested password*”) pela correta (ABCD). Na realizada, esta decisão seria tomada com base na análise de frequências.
- Clicar no botão *Next* da janela do histograma.
- Visualizar o resultado na janela de saída que aparece.
- O criptograma foi decifrado? Fechar a janela de análise quando terminar.

A cifra de XOR

Esta atividade mostra a utilização automática de uma implementação da cifra de Vernam. Os passos da atividade são os seguintes.

1. Na tela da JCrypTool, carregar o arquivo CancaoDoExilio.txt na janela ativa.
2. Selecionar a encriptação com XOR no menu *Algorithms*-→ *Classic* → *XOR*. A janela do XOR abrirá.
3. Na janela XOR, selecionar a operação *Encrypt* e *manual input para key*. Digitar uma chave curta. Por exemplo, o nome completo do aluno, sem espaços. Clicar no botão *Next*.
4. Na janela de *Pre-operation transformation*, selecionar a opção *All characters to uppercase*. Clicar no botão *Preview* para ver a formatação do texto claro, clicar em *close* para fechar a visualização, e clicar no botão *Finish*.
5. A nova janela de saída mostra o resultado da encriptação com XOR.
6. Realizar os passos análogos para a decriptação.

Esta implementação se parece com a cifra de Vernam, mas é, na verdade, uma implementação insegura. Debater com a classe os motivos da insegurança. (DICA: a chave é menor que o texto claro.)

Algoritmos de encriptação de blocos

Encriptação com RC6, modo ECB e esquemas de *padding*

A encriptação simétrica com o encriptador de blocos RC6 segue os seguintes passos:

1. Na janela principal da JCryptTool, abrir o arquivo de trabalho 16blocostextclaro.txt.

2. Selecionar a opção de menu *Algorithms → Symmetric → RC6*.
3. Na janela RC6 encryption, selecionar as opções *Encrypt* e *Custom Key*.
4. No quadro *Custom key*, manter o tamanho em 128 bits e digitar a chave de teste 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.
5. No quadro *Mode and Padding Scheme*, selecionar o modo ECB e o preenchimento *No Padding*. Clicar em *Finish*. A janela de saída vai mostrar o criptograma no editor hexadecimal.
6. Inspecionar o criptograma e identificar os padrões repetidos do modo ECB. Verificar que não foi incluído bloco de preenchimento.
7. Repetir a operação mantendo a chave e o modo ECB, trocando apenas o esquema de padding. Em cada caso, Identificar o bloco de padding.
8. Decriptar cada um dos criptogramas com a mesma chave e o RC6/ECB, selecionando a opção “No padding” em todos os casos de decriptação. Assim é possível ver o conteúdo do padding. Em cada caso, identificar no texto claro decriptado: o bloco, o valor do bloco de padding remanescente.

Encriptação com RC6 e outros modos de operação

Esta atividade usa os outros modos de operação mais comuns dos encriptadores de bloco: CBC, CFB, OFB e CTR.

1. Na janela principal da JCryptTool, abrir o arquivo de trabalho 16blocostextclaro.txt, se elel ainda não estiver aberto.
2. Selecionar a opção de menu *Algorithms → Symmetric → RC6*.
3. Na janela RC6 encryption, selecionar as opções *Encrypt* e *Custom Key*.
4. No quadro *Custom key*, manter o tamanho em 128 bits e digitar a chave de teste 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.
5. No quadro *Mode and Padding Scheme*, selecionar o modo CBC e o preenchimento PKCS#5. Clicar em *Finish*. A janela de saída vai mostrar o criptograma no editor hexadecimal.
6. Inspecionar o criptograma e identificar o bloco de preenchimento.
7. Repetir a operação para o texto claro, mantendo a chave e o RC6, trocando apenas o modo de operação: CFB, OFB, CTR.

Algoritmos de encriptação de fluxo

A encriptação com um encriptador de fluxo ARC4 ocorre é a seguinte:

1. Na janela principal da JcryptTool, carregar o arquivo CancaoDoExilio.txt na janela ativa.
2. Selecionar a opção de menu *Algorithms → Symmetric → ARC4*.

3. Na janela ARC4, selecionar as opções *Encrypt* e ARC4.
4. No quadro *Key*, selecionar Hexadecimal e digitar a chave de teste 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF. Clicar em *Finish*.
5. A janela de saída vai mostrar o criptograma no editor hexadecimal. Inspecionar o criptograma.

Realizar a decriptação correspondente da janela ativa:

6. Selecionar a opção de menu *Algorithms* → *Symmetric* → *ARC4*.
7. Na janela ARC4, selecionar as opções *Encrypt* e ARC4.
8. No quadro K*ey*, selecionar Hexadecimal e digitar a chave de teste 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF. Clicar em *Finish*.
9. A janela de saída vai mostrar o criptograma no editor hexadecimal. Inspecionar o criptograma.

Encriptação com algoritmos e modos de operação

Esta atividade utiliza a ferramenta JCrypTool para a experimentação visual dos algoritmos e modos de operação diferentes.

Encriptação AES com modos de operação

A encriptação simétrica com o encriptador de blocos AES segue os seguintes passos:

1. Na janela principal da JCrypTool, abrir o arquivo de trabalho CancaoDoExilio.txt na pasta *Documents*.
2. Selecionar a opção de menu *Algorithms* → *Symmetric* → *AES*.
3. Na janela AES encryption, selecionar as opções *Encrypt* e *Custom Key*.
4. No quadro *Custom key*, manter o tamanho em 128 bits e digitar uma chave de teste qualquer. Por exemplo, a chave 00112233445566778899aabbccddeeff.
5. No quadro *Mode and Padding Scheme*, selecionar o modo ECB e o preenchimento *No Padding*. Clicar em *Finish*. A janela de saída vai mostrar o criptograma no editor hexadecimal.
6. Inspecionar o criptograma e identificar os padrões repetidos do modo ECB. Verificar que não foi incluído bloco de preenchimento.
7. Decriptar o criptograma com a mesma chave e a configuração AES/ECB/*No padding*.
8. Repetir as operações de encriptção e decriptação mantendo a mesma chave e o preenchimento (*No padding*), trocando apenas o modo de operação: CBC, CFB, OFB e CTR.

Padrões do modo ECB

Na encriptação com o modo ECB, padrões repetidos no texto claro geram padrões repetidos no criptograma. Duas atividades exploram maneiras diferentes de visualização desta característica do modo ECB.

Visualização de padrões do modo ECB

1. Na janela principal da JCrypTool, abrir o arquivo de trabalho 20blocostextoclaro.txt na pasta *Documents*.
2. Selecionar a opção de menu *Algorithms* → *Symmetric* → *AES*.
3. Na janela AES encryption, selecionar as opções *Encrypt* e *Custom Key*.
4. No quadro *Custom key*, manter o tamanho em 128 bits e digitar uma chave de teste qualquer. Por exemplo, a chave 00112233445566778899aabbccddeeff.
5. No quadro *Mode and Padding Scheme*, selecionar o modo ECB e o preenchimento *No Padding*. Clicar em *Finish*. A janela de saída vai mostrar o criptograma no editor hexadecimal.
6. Inspecionar o criptograma e identificar os padrões repetidos do modo ECB.

Propagação de erros nos modos de operação

Esta atividade usa a ferramenta JCrypTool e o arquivo 20blocostextclaro.txt. Em todas as tarefas, usar o mesmo algoritmo, padding e chave. Por exemplo, AES de 128 bits, padding PKCS#5 e chave 00112233445566778899AABBCCDDEEFF.

Adulteração de um byte no primeiro bloco

Para cada modo de operação (ECB, CBC, CFB, OFB e CTR) fazer o seguinte:

1. Encriptar o arquivo 20blocostextoclaro.txt no modo de operação;
2. Na janela do criptograma de saída, modificar um byte do primeiro bloco. (Por exemplo, o byte 02 pode ser modificado em um único bit pela substituição do valor atual pelo mesmo valor incrementado de um);
3. Decriptar o criptograma modificado;
4. Analisar o que acontece com o novo texto claro:
   a) O primeiro bloco foi corrompido totalmente ou parcialmente?
   b) O segundo bloco foi corrompido totalmente ou parcialmente?
   c) Os demais blocos foram perdidos ou preservados?

Repetir o processo para o encriptador de fluxo ARC4. O que acontece?

Explicação:

ECB:

- O primeiro bloco (do byte corrompido) é perdido;
- O segundo bloco não é afetado;

- Os demais blocos não são afetados.

CBC:

- O primeiro bloco (do byte corrompido) é perdido;
- O segundo bloco é afetado apenas no byte na mesma posição da adulteração no criptograma;
- Os demais blocos não são afetados.

CFB:

- O primeiro bloco é afetado apenas no byte corrompido;
- O segundo bloco não é perdido;
- Os demais blocos não são afetados.

OFB:

- O primeiro bloco é afetado apenas no byte corrompido;
- O segundo bloco não é afetado;
- Os demais blocos não são afetados.

CTR:

- O primeiro bloco é afetado apenas no byte corrompido;
- O segundo bloco não é afetado;
- Os demais blocos não são afetados.

ARC4:

- Perde somente o byte adulterado.

Perda de um bloco completo

Para cada modo de operação (ECB, CBC, CFB) fazer o seguinte:

1. Encriptar o arquivo CancaoDoExilio.txt no modo de operação;
2. Na janela do criptograma de saída, apagar o décimo bloco do criptograma;
3. Decriptar o criptograma modificado;
4. Analisar o que acontece com o novo texto claro:
   a) Os blocos antes do bloco perdido?
   b) Os blocos após o bloco perdido?

O que acontece com os modos OFB e CTR?
O que acontece com o encriptador de fluxo ARC4?

Explicação:

ECB:

- O bloco removido foi perdido, logo é irrecuperável;
- Os demais blocos não são afetados.

CBC:

- O bloco removido foi perdido, logo é irrecuperável;
- O bloco seguinte ao bloco perdido foi corrompido totalmente;
- Os demais blocos, antes e depois, não são afetados.

CFB:

- O bloco removido foi perdido, logo é irrecuperável;
- O bloco seguinte ao bloco perdido foi corrompido totalmente;
- Os demais blocos (antes e depois) não são afetados.

OFB e CTR:

- Perda de sincronia entre IV e bloco é irrecuperável e a decriptação não é possível ou perda total do texto claro decriptado a partir do bloco perdido.

ARC4:

- Perda total do texto claro decriptado a partir do bloco perdido.

Demonstração de sistema criptográfico RSA no CrypTool

Esta atividade usa o CrypTool para visualizar o funcionamento do sistema criptográfico RSA nas operações de encriptação e decriptação.

1. Na tela principal do CrypTool, selecionar a opção na barra de menu *Ind. Procedures → RSA Cryptosystem → RSA Demonstration.*
2. Seguir as instruções para encriptação.
    - No frame *Prime number entry* clicar no botão *Generate prime number*. No diálogo subsequente, clicar em *Generate prime numbers* e em seguida clicar em *Apply primes*.
    - No frame *RSA parameters*, clicar em *Update parameters*.
    - No frame *RSA encryption ...* selecionar *Input as Numbers* e digitar o seu texto claro (por exemplo, 123).
    - Clicar no botão *Encrypt*. O resultado aparece no campo *Encryption into ciphertext*.
3. Seguir as instruções para decriptação.
    - Copiar o criptograma/ciphertext gerado na encriptação (pode usar CTRL+C).
    - Colar o criptograma no campo de textoclaro e clicar no botão *Decrypt*.
    - O resultado aparece no campo *Decryption into plaintext.*

Demonstração de assinatura digital RSA no CrypTool

Esta atividade usa o CrypTool para visualizar o funcionamento do sistema criptográfico RSA nas operações de geração e verificação de assinaturas digitais.

1. Na tela principal do CrypTool, selecionar a opção na barra de menu *Ind. Procedures → RSA Cryptosystem → Signature demonstration (Signature generation).*
2. Na janela *Step by Step Signature Generation*, seguir os passos indicados no fluxograma clicando com o mouse em cada etapa.
    a. As etapas do fluxograma em verde já foram realizadas;
    b. As etapas em azul são informativas e para visualização de dados;
    c. As etapas em vermelho são passos pendentes (não realizados) e necessários para etapas seguintes;
    d. As etapas em cinza são passos futuros no fluxograma e ainda não foram realizados.

Assinatura digital DSA

O passo a passo da encriptação RSA ocorre é o seguinte:

1. Na janela principal da JCryptTool, abrir o arquivo CancaoDoExilio.txt localizado na pasta *Documents*.

2. Selecionar a opção de menu *Algorithms → Signature → DSA*.
3. Na janela DSA, selecionar as opções *Sign* e a chave privada da Alice “Whitehat”.
4. Escolher um local de armazenamento e um nome para o arquivo que guarda a assinatura. Clicar em *Finish*. Digitar a senha 1234.
5. A janela de saída vai mostrar a assinatura no editor hexadecimal.

Verificação da assinatura DSA sobre o arquivo CancaoDoExilio.txt na janela ativa:

1. Selecionar a opção de menu *Algorithms → Signature → DSA*.
2. Na janela DSA, selecionar as opções *Verify* e a chave pública de Alice Whitehat. No quadro *Signature File*, selecionar o arquivo onde a assinatura está armazenada. Clicar em *Finish*.
3. Uma caixa de diálogo avisa que a assinatura está correta.

Repetir o processo de verificação da assinatura com o arquivo que guarda a assinatura digital adulterada. Por exemplo, modificar um único byte do arquivo. A assinatura não será verificada.

Acordo de chaves Diffie-Hellman

Esta atividade usa o JCrypTool para experimentar o funcionamento do acordo de chaves Diffie-Hellman passo a passo. Será visualizado o Diffie-Hellman sobre curvas elípticas (ECDH).
Na tela principal do JCrypTool, selecionar a opção na barra de menu *Visuals→ Diffie-Hellman key exchange (EC)*.
Na janela *Diffie-Hellman key exchange (EC),* clicar no botão *Set public parameters*. Uma janela para a configuração dos parâmetros da curva aparecerá.

- No quadro *Curve type* selecionar a opção *F(p)*;
- No quadro *Curve size* selecionar a opção *Large;*
- No quadro domain parameters, escolher o padrão de segurança X9.62. (Há 4 opções de escolha: X9.62, SEC 2, Brainpool e CDC) e a curva prime192v1;
- Os parâmetros *a, b* e *p* da curva prime192v1 são mostrados na tela*;*
- Escolher um gerador pseudo-aleatório. Clicar em no botão *Finish*.

Na janela *Diffie-Hellman key exchange (EC), c*licar no botão *Choose secrets*.

- Gerar o segredo da Alice. Clicar no botão Secret da Alice, clicar no botão G*enerate secret* da janela de diálogo que aparecerá e depois clicar em *Finish*.
- Gerar o segredo de Bob. Clicar no botão Secret de bob, clicar no botão G*enerate secret* da janela de diálogo que aparecerá e depois clicar em *Finish*.

*C*licar no botão *Create shared keys* para gerar as chaves compartilhadasde Alice e Bob.

- Clicar no botão *Calculate* da Alice;
- Clicar no botão *Calculate* de bob.

*C*licar no botão *Exchance shared keys* para simular a troca das chaves públicas.
*C*licar no botão *Generate common key* para calcular o segredo compartilhado.

- Clicar no botão *Calculate* da Alice;
- Clicar no botão *Calculate* de bob.

Pronto. Isto termina o protocolo de acordo de chaves. Os segredos gerados por Alice e por Bob são iguais. Opcionalmente, repetir a simulação para outras curvas elípticas e inspecionar os parâmetros de cada curva.

Criptografia de curvas elípticas

Esta atividade usa o JCrypTool para visualizar o funcionamento da criptografia de curvas elípticas. Na janela principal do JCrypTool, selecionar a opção de menu *Visuals → Elliptic Curve Calculations*.

Curvas pequenas

Na janela *Elliptic Curve Calculations*, no quadro *Settings*, selecionar *Curve size small.*

Curvas elípticas com números reais

Selecionar *Curve type real numbers*. O quadro *Curve attributes*, escolher a = -8 e b = 10. Visualizar o gráfico da curva. Se a curva não couber na Janela, ajustar o controle de Z*oom graph*.

Soma de pontos da curva.

- No quadro *Calculations*, clicar em um ponto no gráfico da curva para escolher P.
- Selecionar a opção *Chose Q with your mouse*.
- Clicar em um ponto no gráfico da curva para escolher Q.
- O ponto R = P + Q é mostrado no gráfico da curva.

Multiplicação de ponto por escalar.

- Selecionar a opção *Chose Q as p*k*.
- Escolher o valor inteiro para k. Por exemplo, k = 4.
- Os pontos Q = k*P e R = P + Q são mostrados no gráfico da curva.

Curvas elípticas com inteiros de corpo primo

Selecionar *Curve type F(p)*. O quadro *Curve attributes*, escolher a = -8, b = 10 e p = 23. Visualizar os pontos da curva.

Soma de pontos.

- No quadro *Calculations*, clicar em um ponto para escolher P.
- Selecionar a opção *Chose Q with your mouse*.
- Clicar em um ponto para escolher Q.
- O ponto R = P + Q é mostrado no gráfico.

Multiplicação de ponto por escalar.

- Selecionar a opção *Chose Q as p*k*.
- Escolher o valor inteiro para k. Por exemplo, k = 4.
- Os pontos Q = k*P e R = P + Q são mostrados no gráfico.

Curvas grandes

Na janela *Elliptic Curve Calculations*, no quadro *Settings*, selecionar *Curve size Large.*

Selecionar *Curve type F(p)*. O quadro *Select curve attributes*, escolher o padrão e uma curva. Por exemplo, o padrão X9.62 e a curva prime192v1. Os parâmetros da curva são mostrados no quadro *Curve attributes*.

Soma de pontos:

- No quadro *Calculations*, selecionar a opção *Add P and Q*.
- No quadro *point P*, clicar no botão *Generate random point*.
- No quadro *point Q*, clicar no botão *Generate random point*.
- O ponto *R = P + Q* é mostrado no quadro *Point R*.

Multiplicação de ponto por escalar:

- No quadro *Calculations*, selecionar a opção *Multiply P by k*.
- Escolher o valor inteiro para k. Por exemplo, k = 8.
- *O ponto R = P + 7P = 4P + 4P correspondente ao k=8 está no quadro Point R.*

Opcionalmente:

- Repetir a atividade para curvas elípticas em outros padrões.
- Repetir a atividade para curvas elípticas binárias F(2^m).

Visualização do Handshake TLSv1.2 com JCrypTool

O objetivo dessa atividade é a visualização passo a passo das etapas do protocolo se saudação do SSL/TLS. Para tal, a simulação SSL/TLS da ferramenta JCrypTool será usada.

Na tela principal da ferramenta JCrypTool, selecionar a opção de menu *Visuals → SSL/TLS Handshake* para ativar a simulação da saudação SSL/TLS.

No quadro *Client*, configurar as opções da mensagem *Client hello*.

- Selecionar versão 1.2, clicar no botão *Generate* para o valor *Random*. Escolher uma *Cipher Suite.* Por exemplo, a *suite* a seguir está disponível na versão 1.2 do TLS: TLS_DHE_RSA_WITH_AES_256_GCM_SGA384.
- O botão *Information* exibe, em inglês, explicações sobre a etapa da tarefa. (Pode ser necessário rolar horizontalmente a tela para ver as explicações na caixa de texto à direita.) O mesmo botão também exibe os parâmetros selecionados.
- Clicar no botão *Next Step* e prosseguir para o próximo passo.

No quadro *Server*, configurar as opções da mensagem *Server hello*.

- Selecionar versão 1.2, clicar no botão *Generate* para o valor *Random*. Escolher uma *Cipher Suite.* Por exemplo, usar a mesma *suite* do passo anterior: TLS_DHE_RSA_WITH_AES_256_GCM_SGA384.
- O botão *Information/Parameters* exibe, em inglês, explicações sobre a etapa da tarefa ou os parâmetros selecionados.
- Clicar no botão *Next Step* e prosseguir para o próximo passo.

No quadro *Server Certificate*, visualizar os parâmetros DH na caixa de texto lateral.

- Clicar no botão *Show* para ver os detalhes do certificado do servidor. Após visualizar, clicar no botão OK.
- Clicar no botão *Next Step* e prosseguir para o próximo passo.

No quadro *Client Certificate*

- Visualizar na caixa de texto lateral o segredo do cliente.
- Não há certificado do cliente para visualização.
- Clicar no botão *Next Step* e prosseguir para o próximo passo.

No quadro *Server Chance Cipher Spec*

- Visualizar na caixa de texto lateral todos os parâmetros criptográficos gerados e usados na comunicação segura que se segue.
- Clicar no botão *Next Step* e prosseguir para o próximo passo.

O protocolo de saudação termina com cliente e servidor no mesmo estado seguro.

Visualização de ICP com JCrypTool

Esta atividade consiste na visualização de uma simulação dos passos de uma ICP, incluindo a operação de uma AC. Devido a grande quantidade de elementos gráficos envolvidos na visualização, esta atividade é melhor realizada em uma instalação local (na máquina física) da ferramenta JCrypTool.

Acessar a opção de menu *Visuals* → *Public Key Infrastructure*.

Na janela *Public Key Infrastructure,* clicar no botão C*ontinue to plugin*.

Na janela *JCrypTool Public Key Infrastructure (*JCT-PKI*),* realizar os quatro passos do tutorial, uma a um, nas abas/guias da esquerda para a direita, *User*, *Registration Authority (RA)*, *Certification Authority(CA)* e *2nd User*.

Seguir as instruções na caixa de texto no lado direito da janela.

Rolar a janela para visualizar as instruções, se necessário.