Assimétrico

Tempo	BOB	ALICE
1	Selecionar arquivo	Abrir server socket
2	Ler arquivo	Gerar par de chaves
3	Conectar Alice	Aguardar conexão
4	Receber chave pública	Enviar chave pública
5	Criptografar arquivo	Receber arquivo
6	Enviar	Decifrar arquivo
7	Fecha coenxaõ	Fecha conexão
8		Grava no disco

Confidencialidade

Tempo	BOB	ALICE
1	Selecionar arquivo	Abrir server socket
2	Ler arquivo	Gerar par de chaves
3	Conectar Alice	Aguardar conexão
4	Receber chave pública	Enviar chave pública
5	Criar chave de sessão	Receber arquivo e chave de sessão
6	Criptografar arquivo com chave de sessão	Decifrar chave de sessão
7	Criptografia chave de sessão com chave pública	Decifrar o arquivo com chave de sessão
8	Envia arq. e chave de sessão criptografado	Fecha a conexão
9	Fecha a conexão	Grava no disco

Integridade

Tempo	**BOB**	**ALICE**
1	Selecionar Arquivo	Abrir server socket
2	Ler Arquivo	Aguardar conexão

3	Aplicar Hash	Recebe pública,Resumo,Arquivo
4	Gera par de chaves	Aplicar hash arquivo recebido
5	Criptografa o Hash com ch Privada	Decifrar resumo ch pública Bob
6	Conectar Alice	Comparar Resumos
7	Envia chave pública,Resumo,Arquivo	Se verdadeiro grava no disco
8	Conexão fechada .	Fecha a conexão

Integridade e Confidencialidade

Tempo	**BOB**	**ALICE**
1	Selecionar Arquivo	Abrir server socket
2	Ler Arquivo	Gera par de chaves
3	Gera par de chaves	Aguarda Conexão
4	Cria hash arquivo	Enviar chave pública
5	Recebe ch publica Alice	Recebe dados de Bob
6	Criptogafa hash ch priv Bob	Descriptografar hash com ch pub Bob
7	Criar ch sessão para arquivo	Descriptografa ch sessão do Bob com ch priv Alice
8	Cripto arquivo ch sessão	Descriptografar arquivo com ch de sessão do Bob
9	Cripto ch sessão com ch pub Alice	Criar hash do arquivo recebido de Bob
10	Envia para Alice (Arquivo,ch sessão,hash TodosCripto),ch pub	Compara as hash
11	Fecha conexão	Se verdadeiro grava no disco
12		Fecha conexão

Integridade, Confidencialidade e Autenticidade

Tempo	BOB	ALICE
1	Selecionar Arquivo	Abrir server socket
2	Ler Arquivo	Gera par de chaves
3	Ler par de chaves	Aguarda Conexão
4	Cria hash arquivo	Enviar chave pública
5	Recebe ch publica Alice	Recebe dados de Bob
6	Criptogafa hash ch priv Bob	Descriptografar hash com ch pub Bob
7	Criar ch sessão para arquivo	Descriptografa ch sessão do Bob com ch priv Alice
8	Cripto arquivo ch sessão	Descriptografar arquivo com ch de sessão do Bob
9	Cripto ch sessão com ch pub Alice	Criar hash do arquivo recebido de Bob
10	Envia para Alice (Arquivo,ch sessão,hash TodosCripto),ch pub	Compara as hash
11	Fecha conexão	Se verdadeiro grava no disco
12		Fecha conexão

Integridade, Confidencialidade, Autenticidade com Certificado(**Certo**)

Tempo	BOB	ALICE
1	Selecionar Arquivo	Abrir server socket
2	Ler Arquivo	Aguarda Conexão
3	Conecta Alice	Enviar certificado a Bob
4	Recebe Certificado	Recebe dados de Bob
5	Verificar autenticidade certificado Alice **5.1** Verifica validade(Data) **5.2** Retira assinatura	Verificar autenticidade certificado Bob **5.1** Verifica validade(Data) **5.2** Retira assinatura

<table>
<tr><td></td><td><table>
<tr><td></td><td>certificado da Alice</td></tr>
<tr><td>5.3</td><td>Ler ch publica CA</td></tr>
<tr><td>5.4</td><td>Descriptografa assinatura do certificado com chave pub da CA</td></tr>
<tr><td>5.5</td><td>Gerar hash (nome, data de validade e chave pub)</td></tr>
<tr><td>5.6</td><td>Comparar com hash da assinatura descriptografado do certificado</td></tr>
<tr><td>5.7</td><td>Se igual o certificado é válido</td></tr>
</table></td><td><table>
<tr><td></td><td>certificado do Bob</td></tr>
<tr><td>5.3</td><td>Ler ch publica CA</td></tr>
<tr><td>5.4</td><td>Descriptografa assinatura do certificado com chave pub da CA</td></tr>
<tr><td>5.5</td><td>Gerar hash (nome, data de validade e chave pub)</td></tr>
<tr><td>5.6</td><td>Comparar hash gerados com a assinatura descriptografa do certificado</td></tr>
<tr><td>5.7</td><td>Se igual o certificado é válido</td></tr>
</table></td></tr>
<tr><td>6</td><td>Criar chave de sessão</td><td>Descriptografa ch sessão com ch priva Alice</td></tr>
<tr><td>7</td><td>Criptografa arquivo com ch sessão</td><td>Descriptografa arquivo com ch sessão Bob</td></tr>
<tr><td>8</td><td>Cripatografa ch sessão com ch pub Alice</td><td>Gera hash arquivo descripto</td></tr>
<tr><td>9</td><td>Gera hash arquivo</td><td>Descriptografa hash do Bob com ch publica de Bob</td></tr>
<tr><td>10</td><td>Criptografa hash c/ ch privada de Bob</td><td>Compara o hash gerado com o hash recebido</td></tr>
<tr><td>11</td><td>Envia para Alice
(Arquivo cripto,
Nome arquivo,
Chave sessão cripto,
Certificado do Bob,
Hash cripto)</td><td>Se verdadeiro grava no disco</td></tr>
<tr><td>12</td><td>Fecha conexão</td><td>Fecha conexão</td></tr>
</table>

Integridade, Confidencialidade, Autenticidade com Certificado(A gente fez)

Tempo	**BOB**	**ALICE**
1	Selecionar Arquivo	Abrir server socket
2	Ler Arquivo	Le certificado da Alice
3	Ler certificado Bob	Aguarda conexão
4	Ler chave privada Bob	Envia certificado para Bob
5	Ler chave pública da CA	Recebe dados de Bob
6	Conecta Alice	Converter Bytes xml para Arquivo xml
7	Recebe certificado Alice(ObjetoTroca)	Ler certificado Bob e instanciar Objeto(Ler dados certificados)
8	Converter Bytes xml para Arquivo xml	Verifica data de validade do certificado da Alice
9	Ler certificado Alice e instanciar Objeto(Ler dados certificados)	Se for válida descriptografa assinatura do certificado de Bob com a chave pub CA
10	Verifica data de validade do certificado da Alice	Cria hash com nome + data validade + ch pub Bob
11	Se for válida descriptografa assinatura do certificado de Alice com a chave pub CA	se valido ler chave privada de Alice e descriptografar a chave de sessão do arquivo
12	Cria hash com nome + data validade + ch pub Alice	Descriptografar arquivo com chave de sessão
13	Comparar hash(assinaturas) com hash criado	Criar hash do arquivo
14	se valido criar chave de sessão para arquivo	Decifrar hash com chave pública de Bob(certificado)
15	Criptografar arquivo com chave de sessão criada	Compara os hash
16	Criptografa chave de sessão com chave pública da Alice que está no certificado	Se verdadeiro grava no disco
17	Criar hash arquivo para enviar a Alice	Fecha conexão

18	Criptografa hash com chave privada de Bob	
19	Enviar para Alice arquivo+chave de sessão+hash+certificado de bob	
20	Fecha conexão	