Criptografia Aplicada 2004/2005
Enunciado do Trabalho Prático

Manuel Bernardo Barbosa – mbb@di.uminho.pt

September 26, 2004

1 Introdução

As aulas práticas de criptografia aplicada serão preenchidas com a elaboração de pequenos projectos de software, por grupos de dois alunos.

O objectivo final das aulas práticas é a integração dos componentes desenvolvidos ao longo do semestre numa aplicação demonstrativa das tecnologias abordadas no âmbito da disciplina.

Os projectos serão implementados na linguagem JAVA, utilizando as seguintes APIs especializadas em funcionalidades de segurança:

- Java Cryptography Architecture (JCA) – API básica para integração de funcionalidade de segurança em aplicações JAVA.
- Java Cryptography Extension (JCE) – extensão à JCA que inclui técnicas criptográficas mais poderosas.
- APIs utilitárias para manipulação de estruturas de dados ASN.1.

A JCA é um componente básico da infraestrutura JAVA distribuida pela SUN (JDK). Esta infraestrutura inclui também a implementação da JCE da própria SUN. Conjuntamente, estas duas APIs fornecem implementações dos algoritmos criptográficos mais comuns. No entanto, recomenda-se a utilização da implementação JCE da IAIK que, para além de mais completa, está integrada de forma elegante com a API para manipulação de estruturas de dados ASN.1, do mesmo fabricante. A instalação básica do JDK apresenta uma limitação das políticas de utilização de algoritmos criptográficos que tem de ser desbloqueada substituindo os ficheiros correspondentes por versões mais liberais. Estes ficheiros podem ser descarregados do site da SUN.

2 Instalação do software em Linux

O software para Linux pode ser descarregado de
`http://www.di.uminho.pt/~glmf/ca/0203/softw`.

A instalação deve ser feita do seguinte modo:

1. Instalar o RPM do java

   ```
   rpm -i j2sdk-1_4_1-beta-linux-i586.rpm
   ```

2. Alterar o `.bash_profile` para incluir:

   ```
   PATH=$PATH:$HOME/bin:/usr/java/j2sdk1.4.1/bin
   JAVA_PATH=/usr/java/j2sdk1.4.1
   CLASS_PATH=$CLASS_PATH:
   export PATH JAVA_PATH CLASS_PATH
   ```

3. Alterar a politica de segurança:

   ```
   unzip jce_policy-1_4_1-beta.zip
   cp ./jce/* /usr/java/j2sdk1.4.1/jre/lib/security
   ```

4. Instalar o IAIK escolhendo a directoria `/usr/java`

   ```
   java iaikjce301ev
   ```

5. Copiar o IAIK completo para a directoria do IAIK e para as extensões do java

   ```
   cp iaik_jce_full.jar /usr/java/IAIK-JCE3.01eval/lib-signed
   cp iaik_jce_full.jar /usr/java/j2sdk1.4.1/jre/lib/ext
   ```

6. Instalar o provider IAIK inserindo a seguinte linha no ficheiro

   ```
   /usr/java/j2sdk1.4.1/jre/lib/security/java.security

   . . .
   security.provider.6=iaik.security.provider.IAIK
   . . .
   ```

3 Objectivos do Trabalho Prático

Os componentes de software desenvolvidos durante as aulas serão utilizados para implementar um protocolo de Anonymous Digital Cash (ADC). Este tipo de protocolos representam uma tentativa de reproduzir no mundo electrónico algo com propriedades semelhantes ao dinheiro físico.

Os sistemas de pagamento que não recorrem a dinheiro físico são cada vez mais comuns hoje em dia, incluindo cheques, cartões de débito, cartões de crédito, porta-moedas electrónicos, etc. No entanto, todos estes sistemas têm uma propriedade que pode ser vista como um problema: a auditabilidade. De facto, com dinheiro físico é possível implementar transacções monetárias no

completo anonimato. Se isto é uma vantagem ou uma desvantagem, depende do ponto de vista: os defensores do direito à privacidade vêem esta propriedade como uma vantagem; este ponto de vista é partilhado por aqueles envolvidos em transacções monetárias relacionadas com negócios ilegais.

As propriedades desejáveis para um protocolo de ADC são as seguintes:

- **Independência** A segurança não depende da localização física ou das condições de armazanamento e transferência.
- **Segurança** O ADC não pode ser falsificado ou reutilizado (gasto duas vezes).
- **Privacidade** A privacidade do utilizador está sempre protegida, i.e. ninguém consegue estabelecer uma relação entre o utilizador e as suas compras.
- **Pagamento off-line** Não deverá ser necessária uma ligação on-line a um agente de confiança (e.g. banco) na altura do pagamento.
- **Transferibilidade** O ADC deverá poder ser transferido a outros utilizadores.
- **Divisibilidade** Um item de ADC deverá poder ser dividido em itens de valor inferior (obviamente mantendo o valor total).

A solução de referência no contexto desta disciplina é a desenvolvida por Chaum e descrita em detalhe na secção 6.4 do livro "Applied Cryptography" de Bruce Schneier.

Será fornecida uma biblioteca de classes JAVA contendo implementações das operações criptográficas mais obscuras necessárias à implementação deste protocolo.

Como opção de valorização do trabalho, sugere-se como alternativa o estudo e implementação de uma outra solução para este problema que esteja disponível na literatura.

Durante as aulas teórico-práticas será discutida uma arquitectura para a aplicação a desenvolver. A identificação dos requisitos de segurança inerentes às interacções entre os intervenientes nas transacções relacionadas com o ADC, bem como a sua correcta implementação, serão também discutidas nas aulas da disciplina. Serão o factor central na avaliação dos trabalhos práticos.

4 Avaliação

A avaliação do trabalho prático basear-se-á num relatório do trabalho efectuado, a entregar no final do semestre. Na altura da entrega do relatório terá lugar uma apresentação/demonstração da aplicação desenvolvida, sujeita também a avaliação.