Examination Secure Data Management (211094)
- October 30th, 2009 -

Instruction:
1. **This is an open book examination.**
2. **The examination consists of 5 questions (each 20 marks).**
3. **Success!**

1. DRM (20 marks)

- Explain the fundamental difference between Device Based DRM and Person Based DRM. Describe one situation in which Device Based DRM is preferred and one situation in which person based DRM is preferred **(4 marks).**

- Which OMA v1 delivery mode was developed to support super distribution of content over mobile phones? Describe the steps needed to super distribute a piece of content between 2 mobile phones, starting from the acquisition of the content on the first phone up to playing the content on the second phone **(5 marks).**

- Assume a DRM domain with domain key K. Assume further 3 devices in this domain: A, B, and C. These devices all have a domain key as well as a public-private key pair. Describe how content is encrypted that:
  - Can be used by all devices in the domain **(3 marks).**
  - Can only be used by device B in the domain **(3 marks).**

- Assume a piece of content C has been bought at a Coral compliant web-site indicating that it will be played on an OMA compliant device. Describe in detail the steps to be taken to play this content on a Marlin compliant device, i.e. to exchange the OMA licence for a Marlin licence **(5 marks).**

2. Access Control and XML Security (20 marks)

- There are mainly three types of access control systems, namely Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-Based Access Control (RBAC). Which of them should be used in the following scenarios, and why?
  - In a company, where there are many employees and many resources and access control decisions are based on job functionalities.
  - You have some files and want to share them with a couple of your friends.
  - In a military department, where there are strict hierarchies among resources and employees (**5 marks**).

- What is canonicalization? Why is canonicalization important in processing XML signatures? (**5 marks**)

- There exist three XML signature methods, namely enveloping signature, enveloped signature, and detached signature. Explain what the differences between them are (**5 marks**)

- Suppose Alice wants to send the following XML document to Bob over Internet.

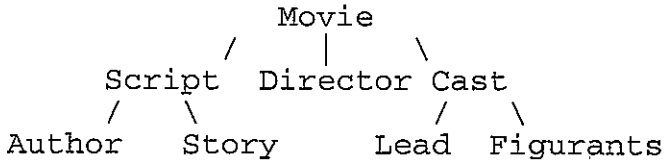
```
<?xml version="1.0"?>
<PurchaseInfo xmlns="http://example.org/info">

  <CustomerInfo >
    <Name>Alice</Name>
    <ContactNumber>123456789</ContactNumber>
    < Address>Emmastraat 101, Enschede, Netherlands</ Address >
  </ CustomerInfo >

  <PaymentInfo>
    <GoodsName>Perfume</ GoodsName >
    <Price>100</ Price >
    <CreditCardNum>088974321</ CreditCardNum >
   </ PaymentInfo >
</ PurchaseInfo >
```

If Alice wants to guarantee that
- Only Bob can read the CreditCardNum element
- Nobody can modify any element of the XML document

With the existing XML signature and encryption methods, what can Alice do to achieve her goals (explain which methods will be chosen and why) (**5 marks**).

3. Search in Encrypted Data (20 marks)

Consider the following XML tree:



Give a mapping function that maps the labels of the tree onto integers. **(2 marks)**

a. Give the complete polynomial representation of the XML tree using this mapping function **(5 marks).**
b. Split the polynomial in a client side and a server side polynomial **(3 marks).**
c. Represent the query /Story and /Lead **(2 marks).**
d. Describe in detail the steps that are taking to answer the query /Figurants the client and the server jointly **(8 marks).**

4. Statistical database security, Privacy-preserving data mining, privacy policies (20 marks)

- Enumerate the available technical methods for achieving statistical database security. For each method, try to use one or two sentences to explain how it works (**6 marks**).

- To achieve privacy in data mining, there exist two types of techniques: one type is crypto-based, and the other type is based on data modifications. Try to compare their performances from the following aspects: versatility, information disclosure risk, information loss, and the communication and computation cost (**6 marks**).

- When you interact with a website for some service, say using Google for searching, what are the potential privacy concerns in your opinion? (**2 marks**)

  Websites will normally provide lengthy literal privacy statements; do you think this method is helpful for protecting your privacy? (**3 marks**)
  P3P has been proposed for exchanging privacy preferences between users and websites (for example, the privacy finder service by Carnegie Mellon's Usable Privacy and Security Laboratory), do you think this method is more helpful than the above method (with literal privacy statements)? (**3 marks**)

5. Copy Protection (20 marks)

- Describe in detail the encryption and decryption steps of content in a two-layer key hierarchy that consists of a content key and a master key derived uniquely from a physical disk identifier. Describe where the decryption fails when trying to decrypt an illegal bit-wise copied disc **(6 marks).**

- What is the role of a media key block in a disc copy protection system and how is this achieved? Describe in detail which steps have to be added to your solution under (a) in order to include a media key block **(6 marks).**

- Consider the following media key block. In element XY indicates that the content key at that position can be accessed by devices X and Y.

```
FSL GHM BEN BTQ
CDL CEM BDO DER
DTN BHO BQO GIR
GXM GBO HIS HXR
```

  For each individual device give all combinations of other devices that need to be revoked to prevent access to the content key **(8 marks).**