Examination Secure Data Management (211094)
- October 31st, 2008 -

Instruction:

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

1. Copy Protection (20 marks)

- Explain how a Media Key Block works and give an example of a 3x3 media key block that supports 5 different devices (**5 marks**).
- Describe by means of a concrete example how, in the above media key block, it can happen that a device gets blocked from access to the content key, while the device itself was never revoked (**5 marks**).
- Describe how in a copy protection system relying on a physical disk identifier a decryption of a bit-wise copied disc will fail (**5 marks**).
- Consider the following media key block. In element XYZ indicates that the content key at that position can be accessed by devices X, Y and Z.

```
ABC CDE EFA
CAE BCD DEF
FBA ABC CDA
```

For each individual device give all combinations of other devices that need to be revoked to prevent access to the content key. Which device(s) needs the maximum and which the minimum? **(5 marks)**

2. Search in Encrypted Data (20 marks)

Consider a relational table STOCK PRICES with the attributes STOCK-CODE, PREVIOUS-PRICE, and CURRENT-PRICE. The values of the PRICE attributes range from 1 – 1000

- Give an example of an instantiation of this table containing 5 different stock entries. Give the encrypted representation of this table based on the approach of *H. Hacigumus, B. Iyer, C. Li*, and *S. Mehrotra* Give the explicit representation of the mapping functions used. The mappings should have at least 5 buckets **(5 marks).**
- Give the SQL query that retrieves the STOCK-CODEs that have a value of minimally 800. Give the relational algebra representation of the query as well as its equivalent relational algebra representation on the encrypted table **(5 marks).**
- Give the SQL query that retrieves the STOCK-CODEs that have fallen more that 10%. Give the relational algebra representation of the query as well as its equivalent relational algebra representation on the encrypted table **(5 marks).**

- Describe how the choice of the mapping functions influences the security and the performance **(5 marks).**

3. Access Control and Privacy (20 marks)

Given the following access matrix, answer the questions below.

	File$_1$	**File$_2$**	**File$_3$**
User$_1$	Read		Read
User$_2$	Read Write	Write	Read Write
User$_3$	Write		Write
User$_4$		Update	
User$_5$		Read	
User$_6$	Read Write	Read, Write	Read Write
User$_7$	Update		Write Update

- With respect to Role-Based Access Control (RBAC), define a set of roles for this matrix, describe the user assignment to these roles, draw the hierarchy graphs for these roles (**6 marks**).

- Give both the access control list and the capability list corresponding to the above access matrix, describe your observations on the performance differences from the above RBAC implementation (**4 marks**).

- Design an XACML policy to present the authorization rules about **User$_2$** and **User$_6$** (**5 marks**).

Given the following table, answer the question below.

Zip code	**Age**	**Nationality**	**Disease**
13053	28	Russian	Heart Disease
13068	29	American	Heart Disease
13053	21	Japanese	Viral infection
13068	23	American	Viral infection
13053	31	American	Cancer
13053	37	Indian	Cancer
13068	36	Japanese	Cancer
13068	35	American	Cancer

- Let {Zip code, Age, Nationality} be the quasi-identifier, create a new table to achieve 4-anonymity (definition is on page 171 of the textbook). Hint: try to use the global recording and Suppression techniques (**5 marks**).

4. XML Security and Privacy Policies (20 marks)

Consider the following XML fragment, answer the following three questions.

```
<?xml version="1.0"?>
<DoctorVisitInfo xmlns="http://example.org/info">
  <Name>Alice</Name>
  <RegisteredDoctor >
    <Number>5539</Number>
    <Hospital>Children's Hospital</ Hospital >
    < Address>Emmastraat 101, Enschede, Netherlands</ Address >
  </RegisteredDoctor >
  <Symptom name="Fever">
    <Duration>10 days</ Duration >
    <Degree>40</Degree>
  </Symptom>
  <Symptom name="Eye Infection">
    <Duration>5 days</ Duration >
    <Degree>Serious</Degree>
  </Symptom>
</DoctorVisitInfo>
```

- Give the XML presentation of the above fragment with an enveloping signature for the Symptom elements (**5 marks**).

- Give the XML presentation of the above fragment with an enveloped signature for an encrypted RegisteredDoctor element and the Symptom elements (**5 marks**).

- Explain what kind of security properties has been achieved in each of the above two cases (**5 marks**).

Consider P3P and E-P3P

- Explain the main purposes of P3P and E-P3P, and point out what are the obstacles in their practical deployments (**5 marks**).

5. DRM (20 marks)

- Explain the fundamental difference between:
  - Digital Rights Management and Copy Protection **(2 marks)**
  - Digital Rights Management and Access Control **(2 marks)**
- The OMA v1 delivery modes have hardly any security. For each mode give a possible attack showing how an unauthorized user can get access to the content **(3 marks).**
- Assume an OMA v2 domain (with domain key K) contains 4 devices A, B, C, D. Each device posses a private-public key-pair.
  - Describe, using a 2-layer key hierarchy, how content will be encrypted that is:
    - Accessible to all domain members (**2 marks**)
    - Only accessible to device A in the domain (**2 marks**)
  - Using the same 2-layer key hierarchy, describe how content only accessible to device A can be transferred to device B. The transfer should guarantee that device B is in the domain and also that devices C and D have no access to the content although they are domain members **(4 marks).**
- Assume a piece of music has been bought at a Coral compliant iTunes website indicating that it will be played on an Apple 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).**