Examination Secure Data Management

192110940 (UT students)

192110941 (Kerckhoff students)

- November 4th, 2011 -

Instruction:

- **This is an open book examination.**
- **The examination consists of SIX questions.**
- **Success!**

1. **HOMOMORPHIC ENCRYPTION (16 marks)**
   Paillier is a popular homomorphic encryption scheme.
   a. Generate a public private key pair, by following the 5 steps as mentioned on page 340 of the reader. Choose small numbers so that you can calculate everything by hand. (**6 marks**)
   b. With the keys generated in the previous question, encrypt the values 2 and 5 (**6 marks**)
   c. Illustrate the homomorphic property by showing that E(2) * E(5) = E(2+5) (**4 marks**)

2. **SHAMIR SECRET SHARING (14 marks)**
   In a (k,n) Shamir secret sharing scheme a secret s is shared among n parties, such that any k (=n) parties can retrieve the secret.
   a. What is the minimal degree of the polynomial in case k=3 and n=4? (**3 marks**)
   b. Let k=3, n=4, choose a polynomial (of minimal degree) you can use to share the secret s=7 (**3 marks**)
   c. Give the shares using the polynomial from question (b) (**3 marks**)

   Now, consider a (3,3)-secret sharing scheme which uses the polynomial $f(x)=ax^2+bx+c$, with secret $s=f(0)=c$

   d. Given the 3 point f(1)=6, f(2)=14 and f(3)=26, recover the secret s (**5 marks**)

3. COPY PROTECTION & DRM (20 marks)

a. Explain the fundamental difference between:
   i. Digital Rights Management and Copy Protection (**2 marks**)
   ii. Digital Rights Management and Access Control (**2 marks**)

b. 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.

WAL	GSP	DET
CPL	CAT	WDO
DAS	BHO	QPA

   i. 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 (**2 marks**)
   ii. For the devices A, B, C, and D give all combinations of other devices that need to be revoked to prevent access to the content key (**6 marks**)

c. 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 (**4 marks**)

d. Assume a piece of music has been bought at a Coral compliant iTunes web-site 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 (**4 marks**)

4. CP-ABE (16 marks)

a. Assume a multi-national company with foreign branches with employees and managers that exchange confidential information. Give a set of minimally 6 different attributes that allow identifying different employees and managers and different levels of confidentiality of documents (**4 marks**)

b. Give 2 different access policies to the confidential information, each of them should build on minimally 3 of the above attributes. For each of the policies explain in words its meaning (**2 marks**)

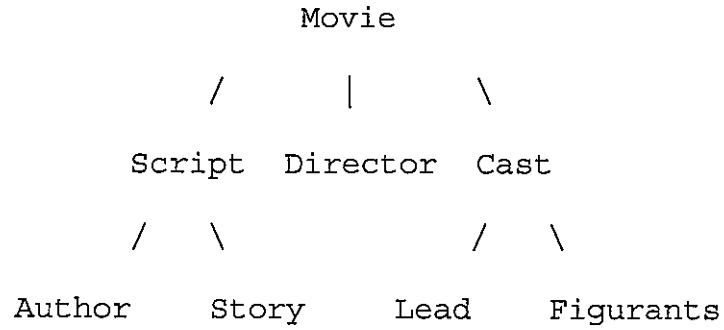
c. For one of the above policies give the details of the Key Generation and Encryption Steps in CP-ABE (**5 marks**)

d. For the other of the above policies give the details of the m-Decrypt step in Type-Based Proxy Re-encryption (**5 marks**)

↳ mCP-ABE?

5. SEARCHING IN ENCRYPTED DATA (20 marks)

Consider the following XML tree.



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

6. RELATIONAL ENCRYPTION (14 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 – 10.

a. Give an example of an instantiation of this table containing 5 different stock entries (**2 marks**)
b. 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 4 buckets (**4 marks**)
c. Give the SQL query that retrieves the STOCK-CODEs that have a value of less than 3. Give the relational algebra representation of the query as well as its equivalent relational algebra representation on the encrypted table (**3 marks**)
d. Give the SQL query that retrieves the STOCK-CODEs that have climbed more than 10%. Give the relational algebra representation of the query as well as its equivalent relational algebra representation on the encrypted table (**5 marks**)