Examination Secure Data Management

192110940 (UT students)

192110941 (Kerckhoff students)

- November 2nd, 2012 -

Instruction:

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

1. **CLASSICAL ACCESS CONTROL (15 points)**
   a. Explain the difference between Identification and Authentication? **(3 points)**
   b. Explain what One-time password is and explain why one-time password is better than a normal password? **(3 points)**
   c. Explain synchronous and asynchronous one time passwords? Specify their drawbacks? **(3 points)**
   d. Explain why event logging is important and which events do you think should be logged (both in host computers and networks)? **(3 points)**
   e. Which access control model is more suitable for the military? Explain why? **(3 points)**

2. **COPY PROTECTION & DRM (20 points)**

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

b. Consider the following TWO media key blocks. In element XYZ indicates that the content key at that position can be accessed by devices X, Y and Z.

MEDIA KEY BLOCK 1

FRL	GHM	BEN
CDL	CEM	BDO
DFN	BHO	BDF

MEDIA KEY BLOCK 2

XRA	GSP	DET
CPA	CRT	XDO
DRS	BHO	QPR

i. Describe by means of a concrete example FOR EACH OF THE TWO above media key blocks, how it can happen that a device gets blocked from access to the content key, while the device itself was never revoked. **(2 points)**

ii. In MEDIA KEY BLOCK 2 which device(s) needs the least other devices to be revoked in order to be blocked from access to the content key? **(2 points)**

iii. Which of the two media key block is most vulnerable with respect to unintended blocking? **(2 points)**

c. 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. (**4 points**)

d. 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. (**4 points**)

e. Describe how in a copy protection system relying on a physical disk identifier a decryption of a bit-wise copied disc will fail. (**2 points**)

3. SECURE BUILDING BLOCKS AND PUBLIC KEY ENCRYPTION WITH DELEGATED SEARCH (15 points)

a. Explain similarities and differences between traditional public-key encryption (e.g. RSA) and Identity-Based Encryption? **(5 points)**

b. Explain how to create a Search on Encrypted Data scheme (e.g. PEKS) from an Identity-Based Encryption (IBE) scheme? Demonstrate it with an example? **(5 points)**

c. Explain what is a cryptographic assumption (e.g. Discrete log problem) and explain why is used in cryptography? **(5 points)**

4. **SEARCHING IN ENCRYPTED DATA (15 points)**

Consider the following XML tree.

```
         A

    /    |    \

   B     C     D

 /   \   |   / |  \

 E   F   G  H  F   E
```

a. Give a mapping function that maps the labels of the tree onto integers. **(2 points)**
b. Give the complete polynomial *factorial* representation of the XML tree using this mapping function (i.e. *no need to compute the coefficients*). **(2 points)**
c. What is the order of the polynomial representing node A? How can this order be *reduced* by 3 without losing the ability to use the polynomial for effective query answering? **(2 points)**
d. Represent the *reduced* polynomial representing node A in coefficient representation and split the polynomial in a server and client part. **(3 points)**
e. Represent the queries "/C" and "/E". **(2 points)**
f. Describe in detail the steps that are taking to answer both the queries "/C" and "/E" by the client and the server jointly. **(4 points)**

5. **ACCESS MANAGEMENT IN OPEN ENVIRONMENTS (20 points)**

a. Explain what is secret-sharing scheme and show how to create a (t,n) scheme for t=n, where t is the number of shares, and n is the number of participants? **(5 points)**
b. Explain how secret sharing scheme is used in Cipher text-Policy Attribute-Based Encryption (CP-ABE) and Key-Policy Attribute Based Encryption (KP-ABE)? **(5 points)**
c. Show how to use secret sharing scheme in CP-ABE to encrypt a message M according to the following access policy P= (UT AND Student) OR Professor. **(5 points)**
d. Explain why CP-ABE is more suitable than a traditional public-key encryption (e.g. RSA) when enforcing P? **(5 points)**

6. **RELATIONAL ENCRYPTION (15 points)**

Consider a relational table ELECTION RESULTS with the attributes PARTY, LEADER-PREV, LEADER-NEW, SEATS-PREV, and SEATS-NEW. The values of the SEATS-OLD and SEATS-NEW attributes range from 1 – 50.

a. Give an example of an instantiation of this table containing 5 different parties. **(2 points)**
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. Argue why you use a certain number of buckets. **(4 points)**
c. Give the SQL query that retrieves the PARTYs that have the same leader for the previous and new elections. Give the relational algebra representation of the query as well as its equivalent relational algebra representation on the encrypted table. **(3 points)**
d. Give the SQL query that retrieves the PARTYs that have at least 20% less seats after the current election than after the previous election. Give the relational algebra representation of the query as well as its equivalent relational algebra representation on the encrypted table. **(6 points)**