

## Exercise 7

### 1 Lazy Revocation in a Cryptographic Filesystem

In a cryptographic filesystem, where every file is encrypted with a separate key, one form of access control can be implemented by handing out the key only to authorized parties. But every party can read all the encrypted data blocks of all files. When a party is revoked access to a file, a fresh file-key must be chosen, and the all data blocks of the file have to be re-encrypted with the fresh key.

The idea of *lazy revocation* is that re-encryption does not occur immediately, but is deferred to the time when the file is updated next. The intuition is that this does not weaken the security because the revoked user could have stored all file data in the past.

- a) Discuss a possible implementation of this concept. What do you think about the security of lazy revocation?
- b) Suppose the file-data blocks are encrypted using a symmetric cryptosystem (e.g., a block cipher). Describe a scheme in which a party that receives the current file-encryption key can derive all previous file-encryption keys on its own, but receives no information about future file-encryption keys.