

Exercise 9

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 files in encrypted form. When a party is revoked access to a file, a fresh file-key must be chosen; this is known as *lazy revocation*.

- a) Discuss possible implementations of this concept and their security implications.
- b) Suppose the files are encrypted using a symmetric cryptosystem (e.g., a block cipher). Describe a scheme in which a party that receives the current file-key can derive all previous file-keys on its own, but receives no information about future file-keys.