Privacy Engineering (70018)

Computing on Untrusted Servers - Questions

3.1 Exam 2018. Using proxy key encryption, outline in Python (or pseudo-code), a cryptographic scheme to perform encrypted keyword searches for encrypted documents held by a database running on an untrusted server.

In your solution assume Alice inserts a new document and its associated keywords while Bob searches for documents with a particular keyword. You can assume that keys have already been computed. Hint: Search on encrypted hashes of keywords and encrypt documents with a random symmetric key for better performance.

3.2 Exam 2018. In *functional encryption*, Alice has a public key pk and a special master secret key mk. Alice can use mk to compute secret function keys for functions, for example, Alice can compute fk for function f. Anyone given the private function key fk and the ciphertext c=$\mathrm{E}_{pk}(p)$ for some plaintext p can then compute $\mathrm{D}_{fk}(c)$= $f(p)$ without learning any other information about p. Explain how this could be used by an email service to privately filter spam encrypted emails sent to users.

3.3 This question is about the Longitude privacy-preserving location sharing scheme. Note: answers sometimes have many rewriting steps but they are very straightforward operations.

(a) Show that c_2 simplifies to $m \cdot e(g, g)^{r_a n}$ in step 5.

(b) Show that step 6 produces m.

(c) In order for Alice to revoke Bob's access to her location, Alice updates parts of her private (secret) key and public key and both elements of the re-encryption key for each of her remaining location-sharing friends:

(i) replaces x_a in her secret key (sk_a) to a new random value x_a'. Note x_a is not replaced in Z_a but Z_a' will cancel it.

(ii) updates Z_a in her public key (pk_a) to $Z_a' = Z_a^{xa'/\ xa}$

(iii) raises both elements of the re-encryption keys for each of her remaining location-sharing friends (not Bob) to the power $x_a'/\ x_a$

(iv) Show that Alice's location sharing friend Carol can still decrypt messages, but Bob can't.