Exercise 5

On-card Cryptography: Message Digests, Symmetric Cryptography
OO: Optimizations
JCOP Off-card API

In this exercise, we will revisit the password vault applet from Exercise 4. If you do not have your own solution to Exercise 4, you may use the example solution from the web page.

Part 1:

The vault applet stores passwords in plain-text, which represents a security risk. Come up with a strategy for secure storage of passwords and implement it.

Part 2:

Rethink the strategy for associating URLs with passwords. Since the most frequently used action is usually the retrieval of stored passwords, you may want to optimize for this. Also think about other possible optimizations, and the tradeoffs they impose. Justify your decisions, if necessary with empirical data, and implement your ideas.

Part 3:

Design and implement an off-card application to retrieve, store and delete passwords from the vault, using the JCOP off-card API. Note that your application should communicate through the APDU interface, not RMI. You may use Swing, SWT, or plain old command line.

We will be revisiting and extending this applet a few more times during the remainder of the course. This off-card application should make testing and usage easier than typing the plain APDUs in the JCOP Shell.