Homework

Homework – Password hashing

- Write 2 functions in C
  - To hash a password and store it in a hashed form
  - To verify supplied password against the stored password
- Notes
  - First read: http://www.codeproject.com/Articles/704865/Salted-Password-Hashing-Doing-it-Right
  - Use password salting
  - To generate the random salt use your code from the previous seminars (on random data)
  - Write both UNIX and Windows variants
  - In Unix use the crypt() function [use e.g. sha256]
  - In Windows implement yourself PBKDF2; use MS crypto API for hash functions