LAB

Excercise

- Hashing in Linux and Windows

Crypt in Linux

```
#define _XOPEN_SOURCE
#include <unistd.h>
char *crypt(const char *key, const char *salt);
char *crypt_r(const char *key, const char *salt, struct crypt_data *data);
Link with -lcrypt.
```

```
If  salt is a character string starting with the characters "$id$" fol-
      lowed by a string terminated by "$":

            $id$salt$encrypted

      then instead of using the DES machine,  id  identifies  the  encryption
      method  used  and  this  then  determines  how the rest of the password
      string is interpreted.  The following  values  of id are supported:

            ID   | Method
            ---------------------------------------------------------
            1    | MD5
            2a   | Blowfish (not in mainline glibc; added in some
                 | Linux distributions)
            5    | SHA-256 (since glibc 2.7)
            6    | SHA-512 (since glibc 2.7)
```

Hashing in Windows

- MS Crypto API
  - CryptAcquireContext()
  - CryptReleaseContext()

  - CryptCreateHash()
  - CryptHashData()
  - CryptGetHashParam()
  - CryptDestroyHash()