

pyDH

Pure Python Implementation of Diffie-Hellman Key Exchange. Py2, Py3, PyPy compatible.

Example

To use as a library:

```
import pyDH
d1 = pyDH.DiffieHellman()
d2 = pyDH.DiffieHellman()
d1_pubkey = d1.gen_public_key()
d2_pubkey = d2.gen_public_key()
d1_sharedkey = d1.gen_shared_key(d2_pubkey)
d2_sharedkey = d2.gen_shared_key(d1_pubkey)
d1_sharedkey == d2_sharedkey
```

By default it uses the group 14 (2048 bit). To use another group (e.g., 15):

```
d1 = pyDH.DiffieHellman(15) #or pyDH.DiffieHellman(group=15)
```

Installation

To install pyDH, simply:

```
$ pip install pyDH
```