# Setup:

* Install picloud client
* Install private\_dna.py with the paillier python library from the svn repository
* Change directory to the ***private\_dna.py*** parent directory and create a local folder for storing the database files: **dna-db\**
* Create a volume **dna-db:** on picloud to synchronize the local directory for storing the DNA database files

### Remarks:

* if you are on windows and don’t like cmd, try using Cygwin, add these 2 lines to your .bashrc:

export python="/cygdrive/c/Python27/"

export PATH=$python:$PATH

this allows Cygwin to use the Python installation of Windows

* add Cygwin directory to your windows path; C:\cygwin64 and C:\cygwin64\bin

this allows you to run Cygwin or Mintty from cmd

* add the noacl option to you Cygwin /etc/fstab file, this saves you from file permission problems

none /cygdrive cygdrive binary,noacl,posix=0,user 0 0

* Move to /cygdrive/c/your-eclipse-workspace/private-dna-parent/,if you prefer you can add this line to your bashrc file:

cd /cygdrive/c/ your-eclipse-workspace /DNA/

* finally use the python command to run your experiments:

python private-dna -h

# Tool help:

usage: private\_dna.py [-h] [-pi] [-gk bitlength] [-gd n m] [-ed {0,1}]

[-dd {0,1}] [-gq l m] [-eq {0,1}] [-v] [-s {0,1}]

Process counting queries over encrypted DNA database

optional arguments:

-h, --help show this help message and exit

-pi run on picloud

-gk bitlength generate key pair, store on pub.txt and priv.txt

-gd n m generate random database, n is number of sequences, m

is number of letters per sequence, store to

records.txt

-ed {0,1} encrypt database: (0) binary mode, store in

Erecords.txt (1) quaternary mode, store in

ErecordsQ.txt

-dd {0,1} decrypt database: (0) binary mode, decrypts from

Erecords.txt (1) quaternary mode, decrypts from

ErecordsQ.txt

-gq l m generate random query of l positions among m

-eq {0,1} execute query: (0) on binary mode, using Erecords.txt

(1) on quaternary mode, using ErecordsQ.txt

-v, --verify run query on plain-text database

-s {0,1}, --sync {0,1}

(0) synchronize cloud's folder to local folder and

exit; (1) synchronize local folder to cloud's folder and exit

# Paillier\_gmpy2

We took the pure python paillier library but it is slow so we have changed it to use the gmpy2 library (put links and explain)

# Experiments Log:

$ python private\_dna.py -gk 1024

running locally

generate\_keys function took 94.000 ms

Keys Generated

$ python private\_dna.py -gd 1 100

running locally

generate\_database function took 17.000 ms

records.txt

$ python private\_dna.py -ed 0

running locally

encrypt database using binary mode

encrypt\_database\_0 function took 3163.000 ms

Erecords.txt

$ python private\_dna.py -ed 1

running locally

encrypt database using quaternary mode

encrypt\_database\_1 function took 6220.000 ms

ErecordsQ.txt

$ python private\_dna.py -dd 0

running locally

decrypt database from binary mode

1 100

decrypt\_database\_0 function took 3088.000 ms

$ python private\_dna.py -dd 1

running locally

decrypt database from quaternary mode

1 100

decrypt\_database\_1 function took 3800.000 ms

$ python private\_dna.py -gq 20 100 -eq 0 -v

running locally

generate random query

query\_generator function took 0.000 ms

execute query on binary mode

1 100

decrypt\_query\_res\_0 function took 15.000 ms

handle\_query\_0 function took 945.000 ms

0

verification on clear database

1 100

handle\_query\_clear function took 1.000 ms

0

$ python private\_dna.py -gq 20 100 -eq 1 -v

running locally

generate random query

query\_generator function took 0.000 ms

execute query on quaternary mode

1 100

decrypt\_query\_res\_1 function took 15.000 ms

handle\_query\_1 function took 58.000 ms

0

verification on clear database

1 100

handle\_query\_clear function took 0.000 ms

0

# Experiment 1

python private\_dna.py -gk 256

running locally

generate\_keys function took 3.000 ms

Keys Generated

$ python private\_dna.py -gd 5000 300

running locally

generate\_database function took 2695.000 ms

records.txt

$ python private\_dna.py -ed 0

running locally

encrypt database using binary mode

encrypt\_database\_0 function took 1030526.000 ms

Erecords.txt

$ python private\_dna.py -ed 1

running locally

encrypt database using quaternary mode

encrypt\_database\_1 function took 2080692.000 ms

ErecordsQ.txt

$ python private\_dna.py -dd 1

running locally

decrypt database from quaternary mode

decrypt\_database\_1 function took 1305650.000 ms

$python private\_dna.py -dd 0

running locally

decrypt database from binary mode

decrypt\_database\_0 function took 1059826.000 ms