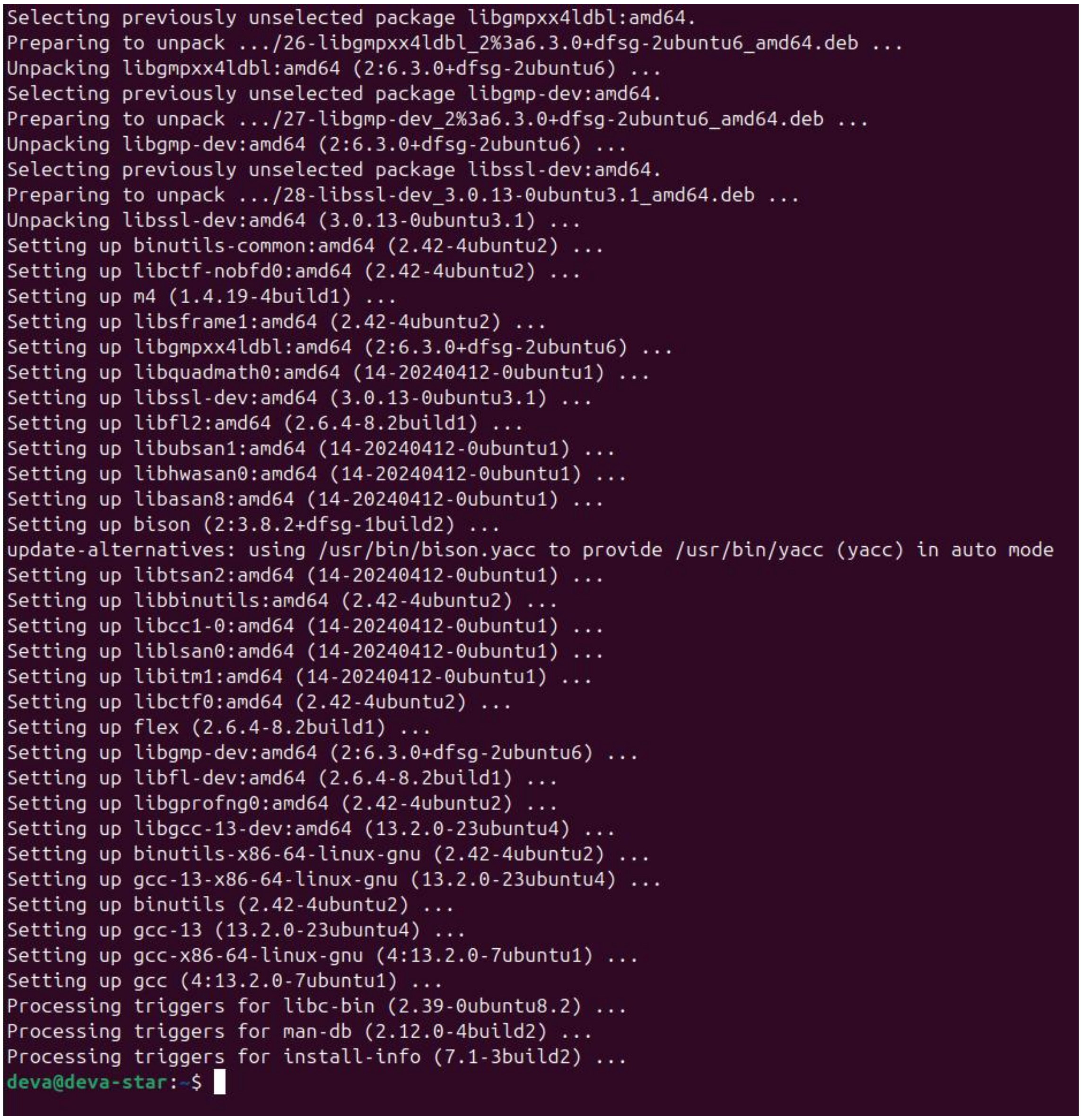
Installation of Charm-Crypto Library

❖ Charm library Installation Requirements:

- Charm does not work with Python3.8+ versions and so we will work on python3.7 environment (Until further update for python3.8+) .

❖ Installation of Pre-requisite Packages:

- sudo apt update
- sudo apt full-upgrade -y
- sudo apt autoremove
- sudo apt -y install flex bison libssl-dev libgmp-dev libgmp10
- sudo apt -y openssl



```
Selecting previously unselected package libgmpxx4ldbl:amd64.
Preparing to unpack .../26-libgmpxx4ldbl_2%3a6.3.0+dfsg-2ubuntu6_amd64.deb ...
Unpacking libgmpxx4ldbl:amd64 (2:6.3.0+dfsg-2ubuntu6) ...
Selecting previously unselected package libgmp-dev:amd64.
Preparing to unpack .../27-libgmp-dev_2%3a6.3.0+dfsg-2ubuntu6_amd64.deb ...
Unpacking libgmp-dev:amd64 (2:6.3.0+dfsg-2ubuntu6) ...
Selecting previously unselected package libssl-dev:amd64.
Preparing to unpack .../28-libssl-dev_3.0.13-0ubuntu3.1_amd64.deb ...
Unpacking libssl-dev:amd64 (3.0.13-0ubuntu3.1) ...
Setting up binutils-common:amd64 (2.42-4ubuntu2) ...
Setting up libctf-nobfd0:amd64 (2.42-4ubuntu2) ...
Setting up m4 (1.4.19-4build1) ...
Setting up libsframe1:amd64 (2.42-4ubuntu2) ...
Setting up libgmpxx4ldbl:amd64 (2:6.3.0+dfsg-2ubuntu6) ...
Setting up libquadmath0:amd64 (14-20240412-0ubuntu1) ...
Setting up libssl-dev:amd64 (3.0.13-0ubuntu3.1) ...
Setting up libfl2:amd64 (2.6.4-8.2build1) ...
Setting up libubsan1:amd64 (14-20240412-0ubuntu1) ...
Setting up libhwasan0:amd64 (14-20240412-0ubuntu1) ...
Setting up libasan8:amd64 (14-20240412-0ubuntu1) ...
Setting up bison (2:3.8.2+dfsg-1build2) ...
update-alternatives: using /usr/bin/bison.yacc to provide /usr/bin/yacc (yacc) in auto mode
Setting up libtsan2:amd64 (14-20240412-0ubuntu1) ...
Setting up libbinutils:amd64 (2.42-4ubuntu2) ...
Setting up libcc1-0:amd64 (14-20240412-0ubuntu1) ...
Setting up liblsan0:amd64 (14-20240412-0ubuntu1) ...
Setting up libitm1:amd64 (14-20240412-0ubuntu1) ...
Setting up libctf0:amd64 (2.42-4ubuntu2) ...
Setting up flex (2.6.4-8.2build1) ...
Setting up libgmp-dev:amd64 (2:6.3.0+dfsg-2ubuntu6) ...
Setting up libfl-dev:amd64 (2.6.4-8.2build1) ...
Setting up libgprofng0:amd64 (2.42-4ubuntu2) ...
Setting up libgcc-13-dev:amd64 (13.2.0-23ubuntu4) ...
Setting up binutils-x86-64-linux-gnu (2.42-4ubuntu2) ...
Setting up gcc-13-x86-64-linux-gnu (13.2.0-23ubuntu4) ...
Setting up binutils (2.42-4ubuntu2) ...
Setting up gcc-13 (13.2.0-23ubuntu4) ...
Setting up gcc-x86-64-linux-gnu (4:13.2.0-7ubuntu1) ...
Setting up gcc (4:13.2.0-7ubuntu1) ...
Processing triggers for libc-bin (2.39-0ubuntu8.2) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for install-info (7.1-3build2) ...
deva@deva-star:~$ 
```

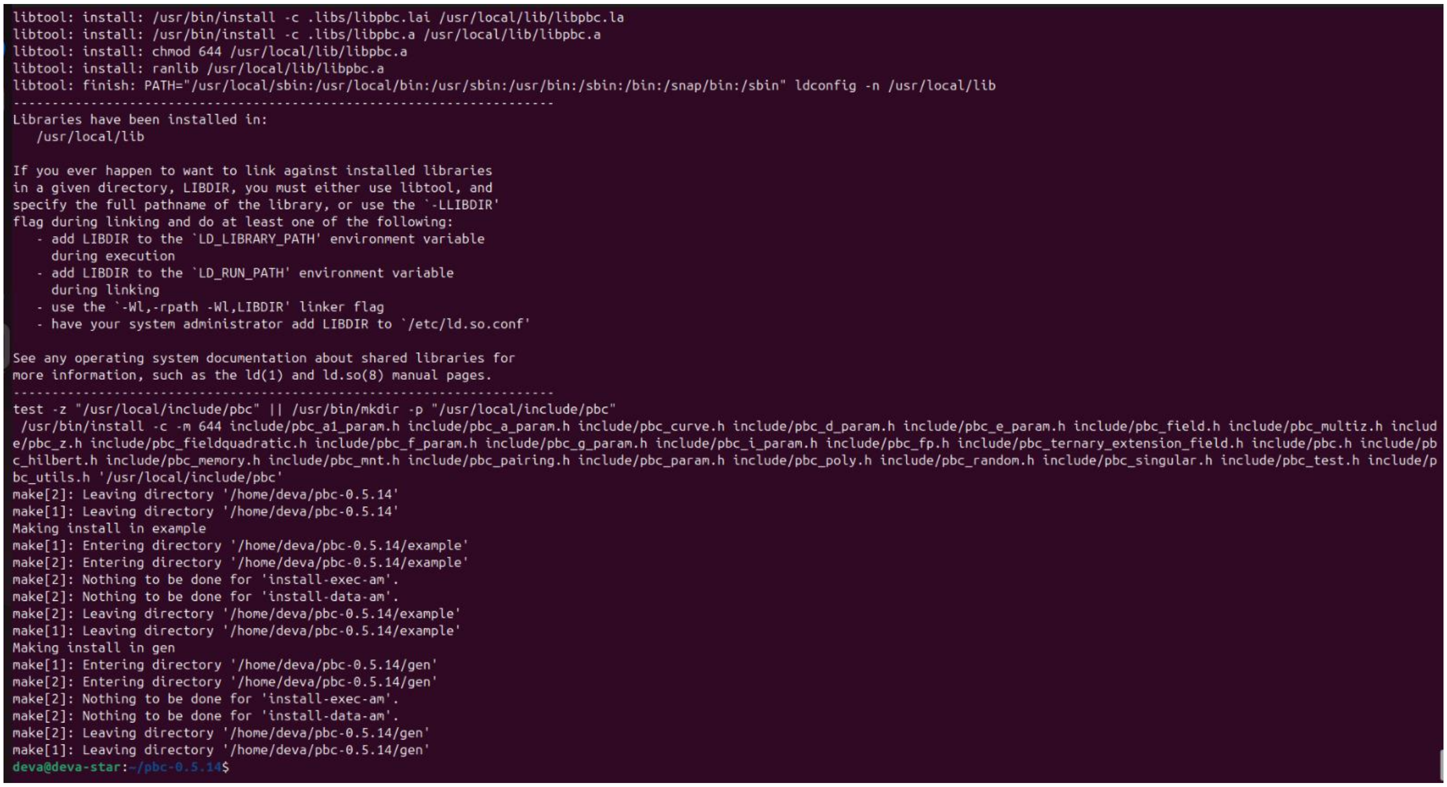
- sudo add-apt-repository ppa:deadsnakes/ppa

- sudo apt update
- sudo apt install python3.7 python3.7-dev python3.7-venv python3-setuptools pip libpython3.7-dev

❖ <u>Installation of Stanford PBC library:</u>

- wget http://crypto.stanford.edu/pbc/files/pbc-0.5.14.tar.gz
- Tar xf pbc-0.5.14.tar.gz
- cd pbc-0.5.14
- sudo ./configure
- sudo make
- sudo make install

Output for successful installation of PBC library:



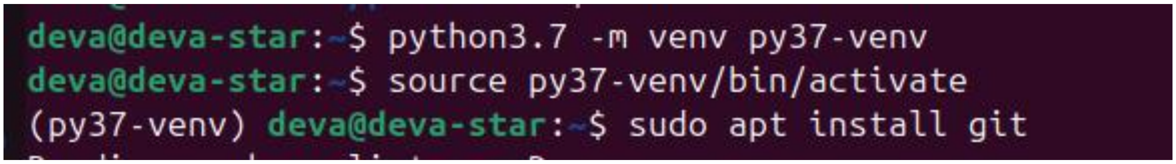
```
libtool: install: /usr/bin/install -c .libs/libpbc.lai /usr/local/lib/libpbc.la
libtool: install: /usr/bin/install -c .libs/libpbc.a /usr/local/lib/libpbc.a
libtool: install: chmod 644 /usr/local/lib/libpbc.a
libtool: install: ranlib /usr/local/lib/libpbc.a
libtool: finish: PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin:/sbin" ldconfig -n /usr/local/lib
----------------------------------------------------------------------
Libraries have been installed in:
   /usr/local/lib

If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the `-LLIBDIR'
flag during linking and do at least one of the following:
   - add LIBDIR to the `LD_LIBRARY_PATH' environment variable
     during execution
   - add LIBDIR to the `LD_RUN_PATH' environment variable
     during linking
   - use the `-Wl,-rpath -Wl,LIBDIR' linker flag
   - have your system administrator add LIBDIR to `/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
----------------------------------------------------------------------
test -z "/usr/local/include/pbc" || /usr/bin/mkdir -p "/usr/local/include/pbc"
 /usr/bin/install -c -m 644 include/pbc_a1_param.h include/pbc_a_param.h include/pbc_curve.h include/pbc_d_param.h include/pbc_e_param.h include/pbc_field.h include/pbc_multiz.h includ
e/pbc_z.h include/pbc_fieldquadratic.h include/pbc_f_param.h include/pbc_g_param.h include/pbc_i_param.h include/pbc_fp.h include/pbc_ternary_extension_field.h include/pbc.h include/pb
c_hilbert.h include/pbc_memory.h include/pbc_mnt.h include/pbc_pairing.h include/pbc_param.h include/pbc_poly.h include/pbc_random.h include/pbc_singular.h include/pbc_test.h include/p
bc_utils.h '/usr/local/include/pbc'
make[2]: Leaving directory '/home/deva/pbc-0.5.14'
make[1]: Leaving directory '/home/deva/pbc-0.5.14'
Making install in example
make[1]: Entering directory '/home/deva/pbc-0.5.14/example'
make[2]: Entering directory '/home/deva/pbc-0.5.14/example'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/deva/pbc-0.5.14/example'
make[1]: Leaving directory '/home/deva/pbc-0.5.14/example'
Making install in gen
make[1]: Entering directory '/home/deva/pbc-0.5.14/gen'
make[2]: Entering directory '/home/deva/pbc-0.5.14/gen'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/deva/pbc-0.5.14/gen'
make[1]: Leaving directory '/home/deva/pbc-0.5.14/gen'
deva@deva-star:~/pbc-0.5.14$
```

❖ <u>Creation of virtual environment for Python non-Debian packages using venv</u>

- python3.7 -m venv py37-venv

(py37-venv => Name of the virtual Environment)

- source py37-venv/bin/activate



```
deva@deva-star:~$ python3.7 -m venv py37-venv
deva@deva-star:~$ source py37-venv/bin/activate
(py37-venv) deva@deva-star:~$ sudo apt install git
```

(To deactivate : deactivate)

- ❖ <u>Installation of the Charm-Crypto Library (or Charm Library)</u>

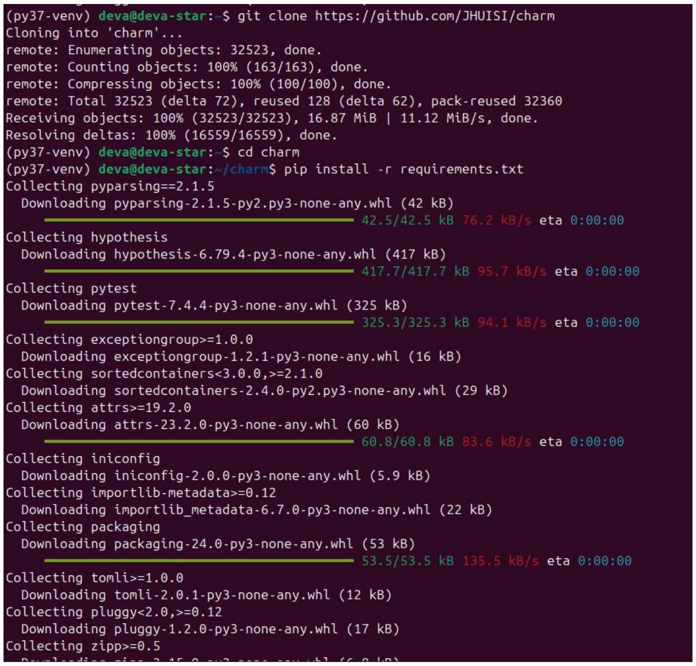
After installing PBC , come out from that PBC directory (cd ..) .

Clone the Charm GitHub repository in your desired installation folder.

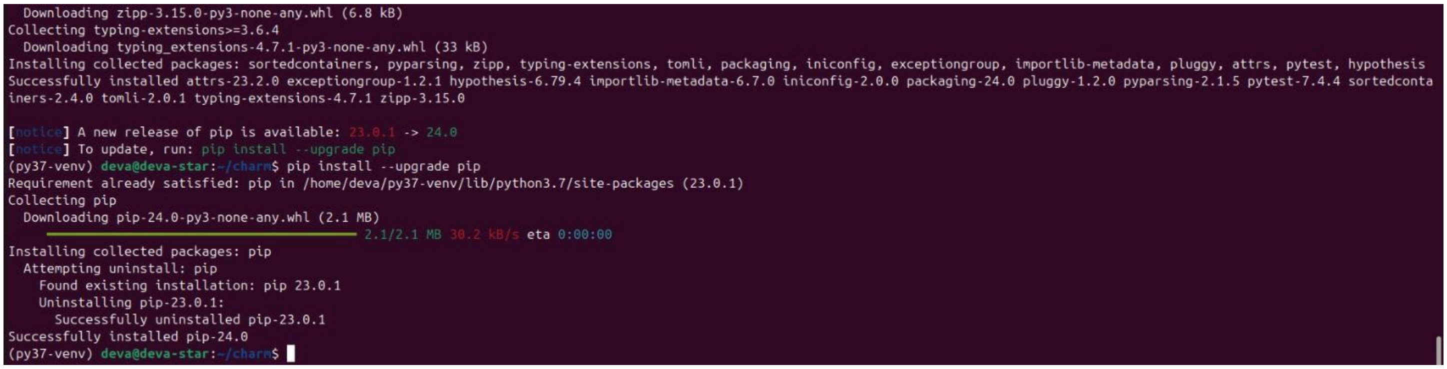
If git not installed : sudo apt install git

- ➢ git clone https://github.com/JHUISI/charm

Output of successful download of charm folder :



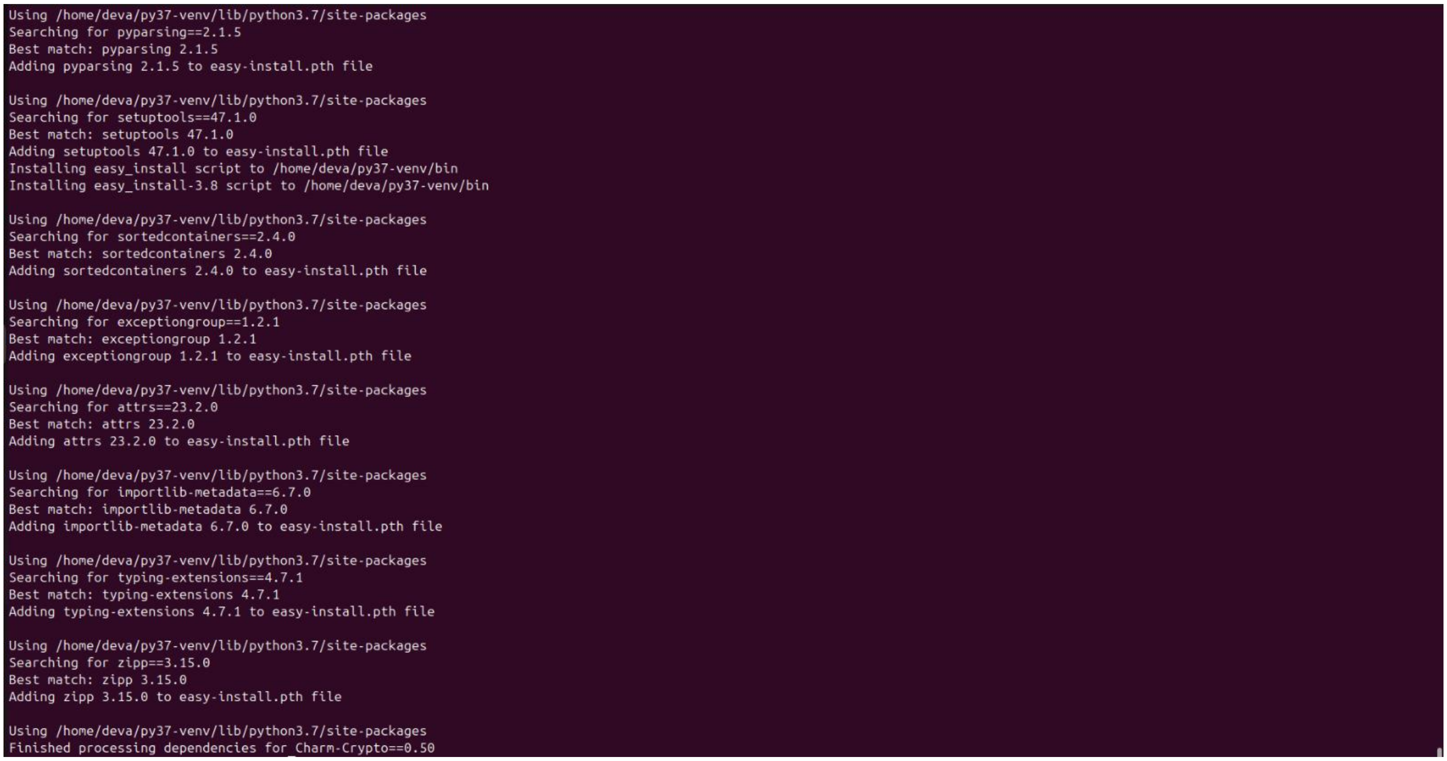
```
(py37-venv) deva@deva-star:~$ git clone https://github.com/JHUISI/charm
Cloning into 'charm'...
remote: Enumerating objects: 32523, done.
remote: Counting objects: 100% (163/163), done.
remote: Compressing objects: 100% (100/100), done.
remote: Total 32523 (delta 72), reused 128 (delta 62), pack-reused 32360
Receiving objects: 100% (32523/32523), 16.87 MiB | 11.12 MiB/s, done.
Resolving deltas: 100% (16559/16559), done.
(py37-venv) deva@deva-star:~$ cd charm
(py37-venv) deva@deva-star:~/charm$ pip install -r requirements.txt
Collecting pyparsing==2.1.5
  Downloading pyparsing-2.1.5-py2.py3-none-any.whl (42 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 42.5/42.5 kB 76.2 kB/s eta 0:00:00
Collecting hypothesis
  Downloading hypothesis-6.79.4-py3-none-any.whl (417 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 417.7/417.7 kB 95.7 kB/s eta 0:00:00
Collecting pytest
  Downloading pytest-7.4.4-py3-none-any.whl (325 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 325.3/325.3 kB 94.1 kB/s eta 0:00:00
Collecting exceptiongroup>=1.0.0
  Downloading exceptiongroup-1.2.1-py3-none-any.whl (16 kB)
Collecting sortedcontainers<3.0.0,>=2.1.0
  Downloading sortedcontainers-2.4.0-py2.py3-none-any.whl (29 kB)
Collecting attrs>=19.2.0
  Downloading attrs-23.2.0-py3-none-any.whl (60 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 60.8/60.8 kB 83.6 kB/s eta 0:00:00
Collecting iniconfig
  Downloading iniconfig-2.0.0-py3-none-any.whl (5.9 kB)
Collecting importlib-metadata>=0.12
  Downloading importlib_metadata-6.7.0-py3-none-any.whl (22 kB)
Collecting packaging
  Downloading packaging-24.0-py3-none-any.whl (53 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 53.5/53.5 kB 135.5 kB/s eta 0:00:00
Collecting tomli>=1.0.0
  Downloading tomli-2.0.1-py3-none-any.whl (12 kB)
Collecting pluggy<2.0,>=0.12
  Downloading pluggy-1.2.0-py3-none-any.whl (17 kB)
Collecting zipp>=0.5
```



```
  Downloading zipp-3.15.0-py3-none-any.whl (6.8 kB)
Collecting typing-extensions>=3.6.4
  Downloading typing_extensions-4.7.1-py3-none-any.whl (33 kB)
Installing collected packages: sortedcontainers, pyparsing, zipp, typing-extensions, tomli, packaging, iniconfig, exceptiongroup, importlib-metadata, pluggy, attrs, pytest, hypothesis
Successfully installed attrs-23.2.0 exceptiongroup-1.2.1 hypothesis-6.79.4 importlib-metadata-6.7.0 iniconfig-2.0.0 packaging-24.0 pluggy-1.2.0 pyparsing-2.1.5 pytest-7.4.4 sortedconta
iners-2.4.0 tomli-2.0.1 typing-extensions-4.7.1 zipp-3.15.0

[notice] A new release of pip is available: 23.0.1 -> 24.0
[notice] To update, run: pip install --upgrade pip
(py37-venv) deva@deva-star:~/charm$ pip install --upgrade pip
Requirement already satisfied: pip in /home/deva/py37-venv/lib/python3.7/site-packages (23.0.1)
Collecting pip
  Downloading pip-24.0-py3-none-any.whl (2.1 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.1/2.1 MB 30.2 kB/s eta 0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 23.0.1
    Uninstalling pip-23.0.1:
      Successfully uninstalled pip-23.0.1
Successfully installed pip-24.0
(py37-venv) deva@deva-star:~/charm$ 
```

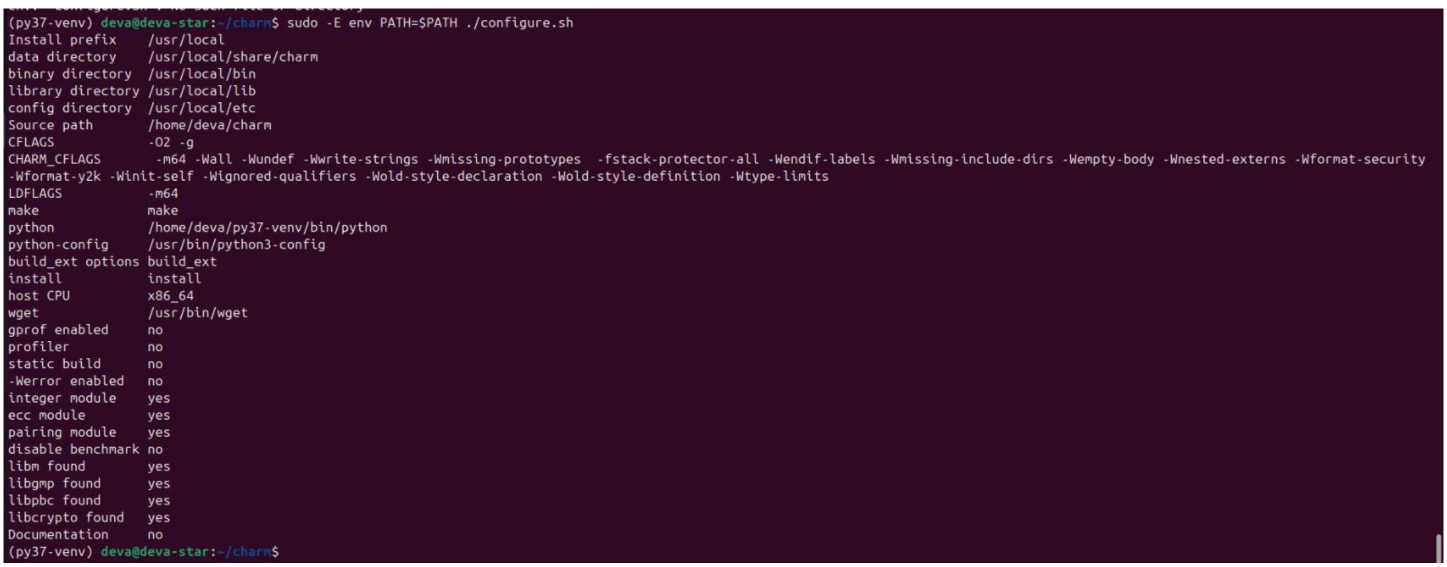
- ➢ cd charm
- ➢ pip install -r requirements.txt

Output of successful installation of dependencies:



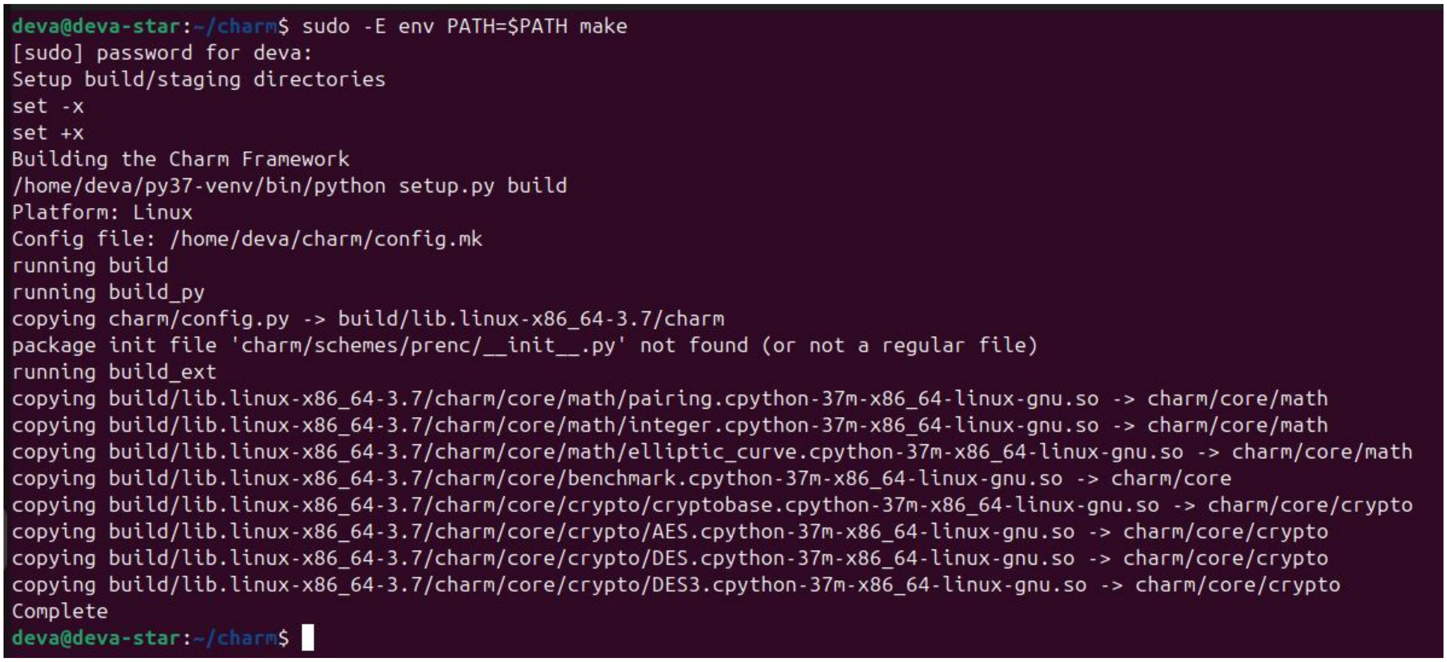
```
Using /home/deva/py37-venv/lib/python3.7/site-packages
Searching for pyparsing==2.1.5
Best match: pyparsing 2.1.5
Adding pyparsing 2.1.5 to easy-install.pth file

Using /home/deva/py37-venv/lib/python3.7/site-packages
Searching for setuptools==47.1.0
Best match: setuptools 47.1.0
Adding setuptools 47.1.0 to easy-install.pth file
Installing easy_install script to /home/deva/py37-venv/bin
Installing easy_install-3.8 script to /home/deva/py37-venv/bin

Using /home/deva/py37-venv/lib/python3.7/site-packages
Searching for sortedcontainers==2.4.0
Best match: sortedcontainers 2.4.0
Adding sortedcontainers 2.4.0 to easy-install.pth file

Using /home/deva/py37-venv/lib/python3.7/site-packages
Searching for exceptiongroup==1.2.1
Best match: exceptiongroup 1.2.1
Adding exceptiongroup 1.2.1 to easy-install.pth file

Using /home/deva/py37-venv/lib/python3.7/site-packages
Searching for attrs==23.2.0
Best match: attrs 23.2.0
Adding attrs 23.2.0 to easy-install.pth file

Using /home/deva/py37-venv/lib/python3.7/site-packages
Searching for importlib-metadata==6.7.0
Best match: importlib-metadata 6.7.0
Adding importlib-metadata 6.7.0 to easy-install.pth file

Using /home/deva/py37-venv/lib/python3.7/site-packages
Searching for typing-extensions==4.7.1
Best match: typing-extensions 4.7.1
Adding typing-extensions 4.7.1 to easy-install.pth file

Using /home/deva/py37-venv/lib/python3.7/site-packages
Searching for zipp==3.15.0
Best match: zipp 3.15.0
Adding zipp 3.15.0 to easy-install.pth file

Using /home/deva/py37-venv/lib/python3.7/site-packages
Finished processing dependencies for Charm-Crypto==0.50
```

- ➢ sudo -E env PATH=$PATH ./configure.sh



```
(py37-venv) deva@deva-star:~/charm$ sudo -E env PATH=$PATH ./configure.sh
Install prefix    /usr/local
data directory    /usr/local/share/charm
binary directory  /usr/local/bin
library directory /usr/local/lib
config directory  /usr/local/etc
Source path       /home/deva/charm
CFLAGS            -O2 -g
CHARM_CFLAGS       -m64 -Wall -Wundef -Wwrite-strings -Wmissing-prototypes  -fstack-protector-all -Wendif-labels -Wmissing-include-dirs -Wempty-body -Wnested-externs -Wformat-security
-Wformat-y2k -Winit-self -Wignored-qualifiers -Wold-style-declaration -Wold-style-definition -Wtype-limits
LDFLAGS           -m64
make              make
python            /home/deva/py37-venv/bin/python
python-config     /usr/bin/python3-config
build_ext options build_ext
install           install
host CPU          x86_64
wget              /usr/bin/wget
gprof enabled     no
profiler          no
static build      no
-Werror enabled   no
integer module    yes
ecc module        yes
pairing module    yes
disable benchmark no
libm found        yes
libgmp found      yes
libpbc found      yes
libcrypto found   yes
Documentation     no
(py37-venv) deva@deva-star:~/charm$
```

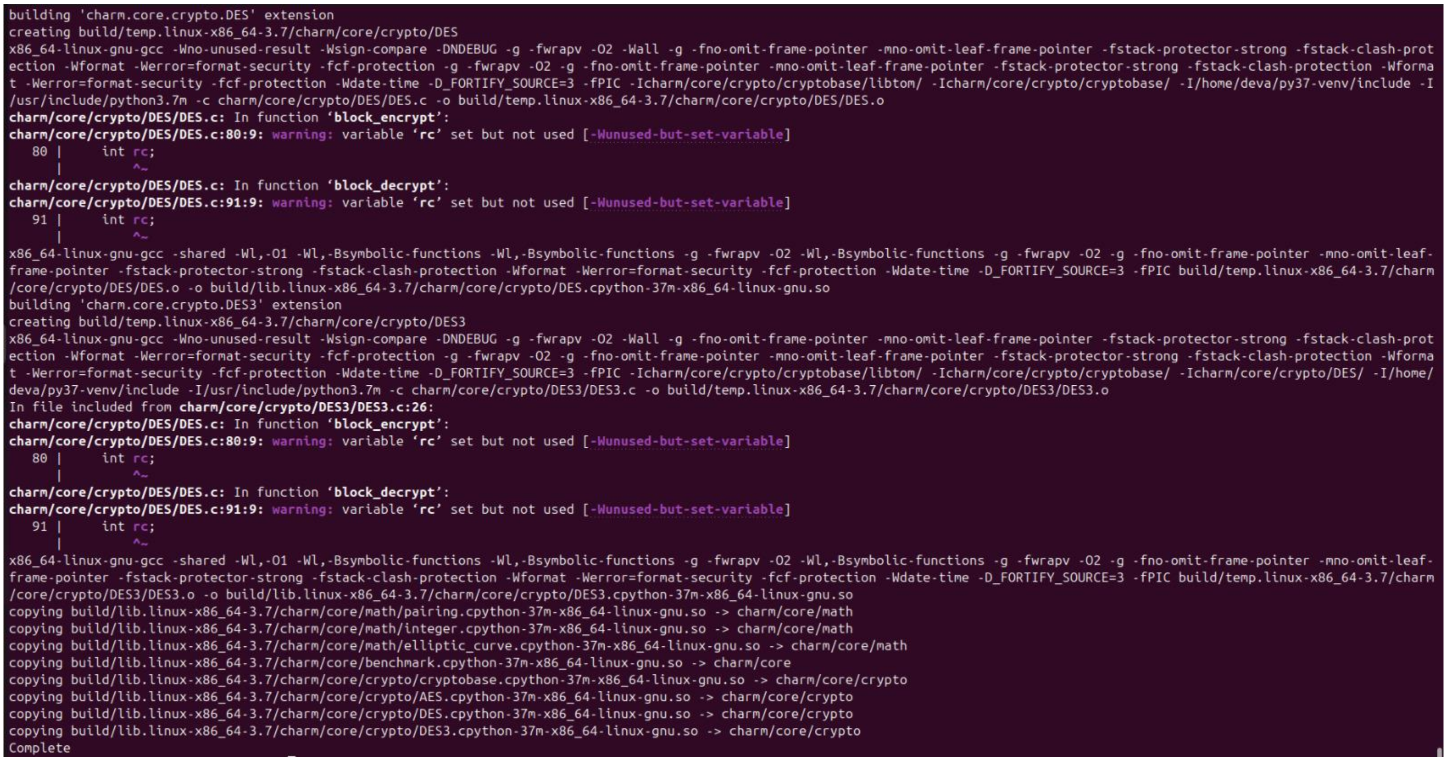
- ➢ sudo -E env PATH=$PATH make



```
deva@deva-star:~/charm$ sudo -E env PATH=$PATH make
[sudo] password for deva:
Setup build/staging directories
set -x
set +x
Building the Charm Framework
/home/deva/py37-venv/bin/python setup.py build
Platform: Linux
Config file: /home/deva/charm/config.mk
running build
running build_py
copying charm/config.py -> build/lib.linux-x86_64-3.7/charm
package init file 'charm/schemes/prenc/__init__.py' not found (or not a regular file)
running build_ext
copying build/lib.linux-x86_64-3.7/charm/core/math/pairing.cpython-37m-x86_64-linux-gnu.so -> charm/core/math
copying build/lib.linux-x86_64-3.7/charm/core/math/integer.cpython-37m-x86_64-linux-gnu.so -> charm/core/math
copying build/lib.linux-x86_64-3.7/charm/core/math/elliptic_curve.cpython-37m-x86_64-linux-gnu.so -> charm/core/math
copying build/lib.linux-x86_64-3.7/charm/core/benchmark.cpython-37m-x86_64-linux-gnu.so -> charm/core
copying build/lib.linux-x86_64-3.7/charm/core/crypto/cryptobase.cpython-37m-x86_64-linux-gnu.so -> charm/core/crypto
copying build/lib.linux-x86_64-3.7/charm/core/crypto/AES.cpython-37m-x86_64-linux-gnu.so -> charm/core/crypto
copying build/lib.linux-x86_64-3.7/charm/core/crypto/DES.cpython-37m-x86_64-linux-gnu.so -> charm/core/crypto
copying build/lib.linux-x86_64-3.7/charm/core/crypto/DES3.cpython-37m-x86_64-linux-gnu.so -> charm/core/crypto
Complete
deva@deva-star:~/charm$ 
```

- ➢ sudo -E env PATH=$PATH make install

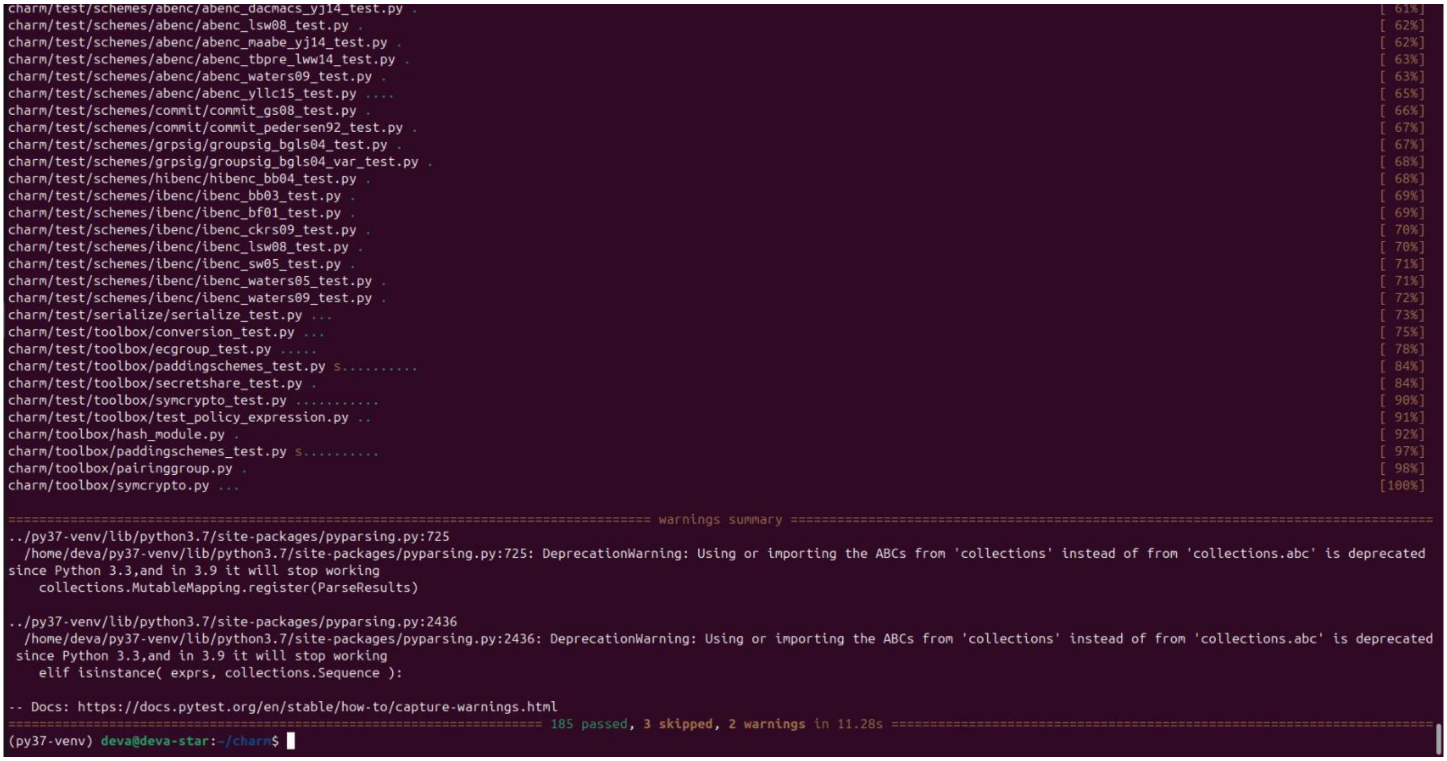
Output of successful installation of Charm Library:



```
building 'charm.core.crypto.DES' extension
creating build/temp.linux-x86_64-3.7/charm/core/crypto/DES
x86_64-linux-gnu-gcc -Wno-unused-result -Wsign-compare -DNDEBUG -g -fwrapv -O2 -Wall -g -fno-omit-frame-pointer -mno-omit-leaf-frame-pointer -fstack-protector-strong -fstack-clash-prot
ection -Wformat -Werror=format-security -fcf-protection -g -fwrapv -O2 -g -fno-omit-frame-pointer -mno-omit-leaf-frame-pointer -fstack-protector-strong -fstack-clash-protection -Wforma
t -Werror=format-security -fcf-protection -Wdate-time -D_FORTIFY_SOURCE=3 -fPIC -Icharm/core/crypto/cryptobase/libtom/ -Icharm/core/crypto/cryptobase/ -I/home/deva/py37-venv/include -I
/usr/include/python3.7m -c charm/core/crypto/DES/DES.c -o build/temp.linux-x86_64-3.7/charm/core/crypto/DES/DES.o
charm/core/crypto/DES/DES.c: In function ‘block_encrypt’:
charm/core/crypto/DES/DES.c:80:9: warning: variable ‘rc’ set but not used [-Wunused-but-set-variable]
   80 |     int rc;
      |         ^~
charm/core/crypto/DES/DES.c: In function ‘block_decrypt’:
charm/core/crypto/DES/DES.c:91:9: warning: variable ‘rc’ set but not used [-Wunused-but-set-variable]
   91 |     int rc;
      |         ^~
x86_64-linux-gnu-gcc -shared -Wl,-O1 -Wl,-Bsymbolic-functions -Wl,-Bsymbolic-functions -g -fwrapv -O2 -Wl,-Bsymbolic-functions -g -fwrapv -O2 -g -fno-omit-frame-pointer -mno-omit-leaf-
frame-pointer -fstack-protector-strong -fstack-clash-protection -Wformat -Werror=format-security -fcf-protection -Wdate-time -D_FORTIFY_SOURCE=3 -fPIC build/temp.linux-x86_64-3.7/charm
/core/crypto/DES/DES.o -o build/lib.linux-x86_64-3.7/charm/core/crypto/DES.cpython-37m-x86_64-linux-gnu.so
building 'charm.core.crypto.DES3' extension
creating build/temp.linux-x86_64-3.7/charm/core/crypto/DES3
x86_64-linux-gnu-gcc -Wno-unused-result -Wsign-compare -DNDEBUG -g -fwrapv -O2 -Wall -g -fno-omit-frame-pointer -mno-omit-leaf-frame-pointer -fstack-protector-strong -fstack-clash-prot
ection -Wformat -Werror=format-security -fcf-protection -g -fwrapv -O2 -g -fno-omit-frame-pointer -mno-omit-leaf-frame-pointer -fstack-protector-strong -fstack-clash-protection -Wforma
t -Werror=format-security -fcf-protection -Wdate-time -D_FORTIFY_SOURCE=3 -fPIC -Icharm/core/crypto/cryptobase/libtom/ -Icharm/core/crypto/cryptobase/ -Icharm/core/crypto/DES/ -I/home/
deva/py37-venv/include -I/usr/include/python3.7m -c charm/core/crypto/DES3/DES3.c -o build/temp.linux-x86_64-3.7/charm/core/crypto/DES3/DES3.o
In file included from charm/core/crypto/DES3/DES3.c:26:
charm/core/crypto/DES/DES.c: In function ‘block_encrypt’:
charm/core/crypto/DES/DES.c:80:9: warning: variable ‘rc’ set but not used [-Wunused-but-set-variable]
   80 |     int rc;
      |         ^~
charm/core/crypto/DES/DES.c: In function ‘block_decrypt’:
charm/core/crypto/DES/DES.c:91:9: warning: variable ‘rc’ set but not used [-Wunused-but-set-variable]
   91 |     int rc;
      |         ^~
x86_64-linux-gnu-gcc -shared -Wl,-O1 -Wl,-Bsymbolic-functions -Wl,-Bsymbolic-functions -g -fwrapv -O2 -Wl,-Bsymbolic-functions -g -fwrapv -O2 -g -fno-omit-frame-pointer -mno-omit-leaf-
frame-pointer -fstack-protector-strong -fstack-clash-protection -Wformat -Werror=format-security -fcf-protection -Wdate-time -D_FORTIFY_SOURCE=3 -fPIC build/temp.linux-x86_64-3.7/charm
/core/crypto/DES3/DES3.o -o build/lib.linux-x86_64-3.7/charm/core/crypto/DES3.cpython-37m-x86_64-linux-gnu.so
copying build/lib.linux-x86_64-3.7/charm/core/math/pairing.cpython-37m-x86_64-linux-gnu.so -> charm/core/math
copying build/lib.linux-x86_64-3.7/charm/core/math/integer.cpython-37m-x86_64-linux-gnu.so -> charm/core/math
copying build/lib.linux-x86_64-3.7/charm/core/math/elliptic_curve.cpython-37m-x86_64-linux-gnu.so -> charm/core/math
copying build/lib.linux-x86_64-3.7/charm/core/benchmark.cpython-37m-x86_64-linux-gnu.so -> charm/core
copying build/lib.linux-x86_64-3.7/charm/core/crypto/cryptobase.cpython-37m-x86_64-linux-gnu.so -> charm/core/crypto
copying build/lib.linux-x86_64-3.7/charm/core/crypto/AES.cpython-37m-x86_64-linux-gnu.so -> charm/core/crypto
copying build/lib.linux-x86_64-3.7/charm/core/crypto/DES.cpython-37m-x86_64-linux-gnu.so -> charm/core/crypto
copying build/lib.linux-x86_64-3.7/charm/core/crypto/DES3.cpython-37m-x86_64-linux-gnu.so -> charm/core/crypto
Complete
```

- ❖ Test the installation :
  - ➢ sudo -E env PATH=$PATH make test

Output of successful installation of Charm Library :



```
charm/test/schemes/abenc/abenc_dacmacs_yj14_test.py .                                                [ 61%]
charm/test/schemes/abenc/abenc_lsw08_test.py .                                                       [ 62%]
charm/test/schemes/abenc/abenc_maabe_yj14_test.py .                                                  [ 62%]
charm/test/schemes/abenc/abenc_tbpre_lww14_test.py .                                                 [ 63%]
charm/test/schemes/abenc/abenc_waters09_test.py .                                                    [ 63%]
charm/test/schemes/abenc/abenc_yllc15_test.py ....                                                   [ 65%]
charm/test/schemes/commit/commit_gs08_test.py .                                                      [ 66%]
charm/test/schemes/commit/commit_pedersen92_test.py .                                                [ 67%]
charm/test/schemes/grpsig/groupsig_bgls04_test.py .                                                  [ 67%]
charm/test/schemes/grpsig/groupsig_bgls04_var_test.py .                                              [ 68%]
charm/test/schemes/hibenc/hibenc_bb04_test.py .                                                      [ 68%]
charm/test/schemes/ibenc/ibenc_bb03_test.py .                                                        [ 69%]
charm/test/schemes/ibenc/ibenc_bf01_test.py .                                                        [ 69%]
charm/test/schemes/ibenc/ibenc_ckrs09_test.py .                                                      [ 70%]
charm/test/schemes/ibenc/ibenc_lsw08_test.py .                                                       [ 70%]
charm/test/schemes/ibenc/ibenc_sw05_test.py .                                                        [ 71%]
charm/test/schemes/ibenc/ibenc_waters05_test.py .                                                    [ 71%]
charm/test/schemes/ibenc/ibenc_waters09_test.py .                                                    [ 72%]
charm/test/serialize/serialize_test.py ...                                                           [ 73%]
charm/test/toolbox/conversion_test.py ...                                                            [ 75%]
charm/test/toolbox/ecgroup_test.py .....                                                             [ 78%]
charm/test/toolbox/paddingschemes_test.py s..........                                                [ 84%]
charm/test/toolbox/secretshare_test.py .                                                             [ 84%]
charm/test/toolbox/symcrypto_test.py ...........                                                     [ 90%]
charm/test/toolbox/test_policy_expression.py ..                                                      [ 91%]
charm/toolbox/hash_module.py .                                                                       [ 92%]
charm/toolbox/paddingschemes_test.py s.........                                                      [ 97%]
charm/toolbox/pairinggroup.py .                                                                      [ 98%]
charm/toolbox/symcrypto.py ...                                                                       [100%]

=================================================================================== warnings summary ===================================================================================
../py37-venv/lib/python3.7/site-packages/pyparsing.py:725
  /home/deva/py37-venv/lib/python3.7/site-packages/pyparsing.py:725: DeprecationWarning: Using or importing the ABCs from 'collections' instead of from 'collections.abc' is deprecated
since Python 3.3,and in 3.9 it will stop working
    collections.MutableMapping.register(ParseResults)

../py37-venv/lib/python3.7/site-packages/pyparsing.py:2436
  /home/deva/py37-venv/lib/python3.7/site-packages/pyparsing.py:2436: DeprecationWarning: Using or importing the ABCs from 'collections' instead of from 'collections.abc' is deprecated
 since Python 3.3,and in 3.9 it will stop working
    elif isinstance( exprs, collections.Sequence ):

-- Docs: https://docs.pytest.org/en/stable/how-to/capture-warnings.html
===================================================================== 185 passed, 3 skipped, 2 warnings in 11.28s =====================================================================
(py37-venv) deva@deva-star:~/charm$ 
```

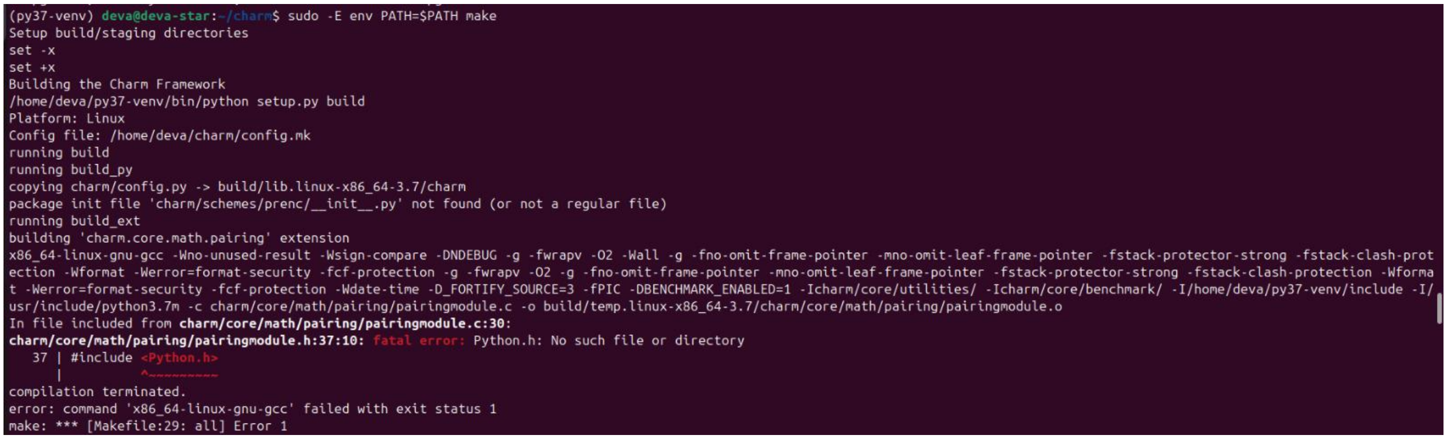
- ➢ To assess if installation is successful, we can run the test suite (command given above). If most (or all) Python tests pass then installation is successful.
- ➢ Alternatively, one can test by importing charm in a python file. If error is detected when the python file is run then there can be error in the installation.

❖ Working :

- ➢ Always work in the virtual environment .
- ➢ Caution : Do not use ' sudo ' command while working in the virtual environment.

- ❖ Error Detection :

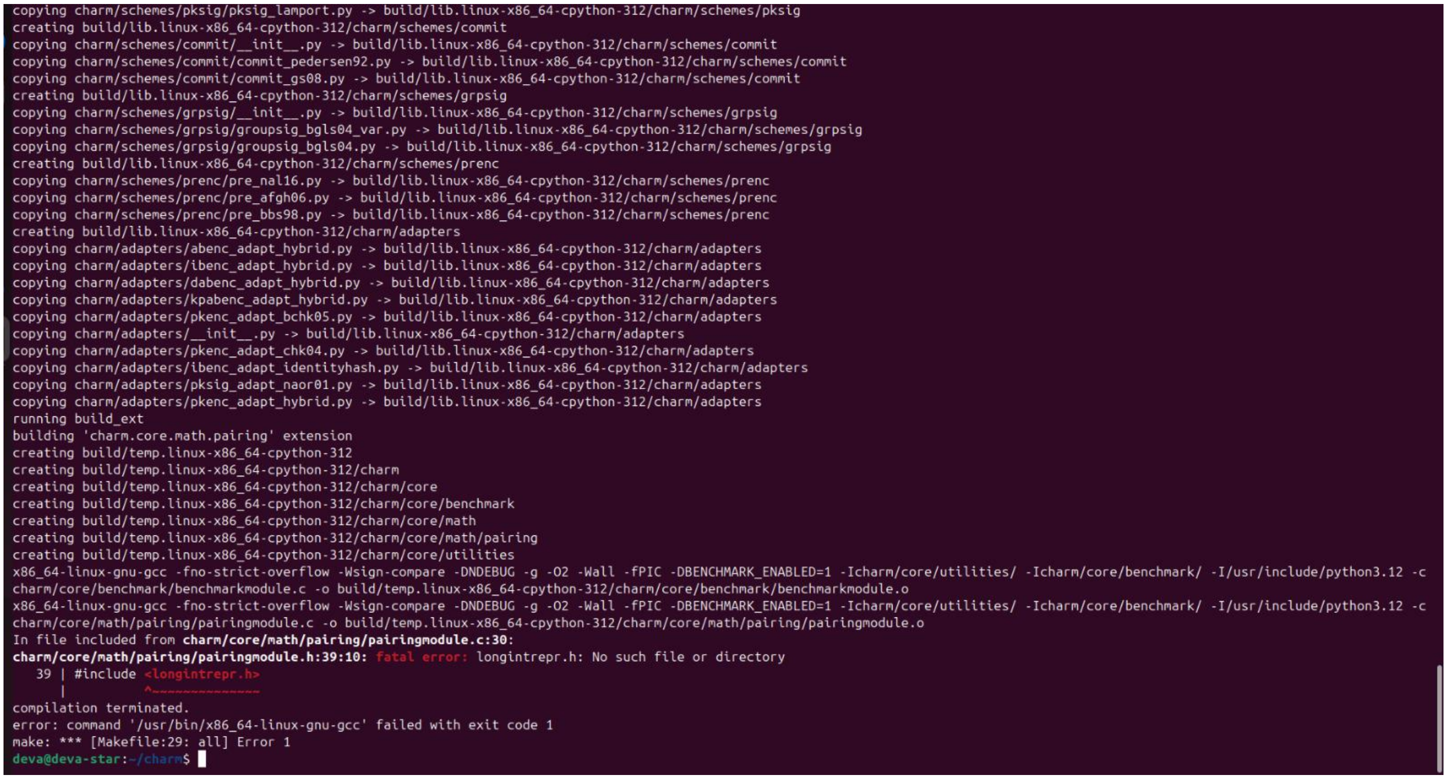
  - ➢ sudo apt install libpython3.7-dev



```
(py37-venv) deva@deva-star:~/charm$ sudo -E env PATH=$PATH make
Setup build/staging directories
set -x
set +x
Building the Charm Framework
/home/deva/py37-venv/bin/python setup.py build
Platform: Linux
Config file: /home/deva/charm/config.mk
running build
running build_py
copying charm/config.py -> build/lib.linux-x86_64-3.7/charm
package init file 'charm/schemes/prenc/__init__.py' not found (or not a regular file)
running build_ext
building 'charm.core.math.pairing' extension
x86_64-linux-gnu-gcc -Wno-unused-result -Wsign-compare -DNDEBUG -g -fwrapv -O2 -Wall -g -fno-omit-frame-pointer -mno-omit-leaf-frame-pointer -fstack-protector-strong -fstack-clash-prot
ection -Wformat -Werror=format-security -fcf-protection -g -fwrapv -O2 -g -fno-omit-frame-pointer -mno-omit-leaf-frame-pointer -fstack-protector-strong -fstack-clash-protection -Wforma
t -Werror=format-security -fcf-protection -Wdate-time -D_FORTIFY_SOURCE=3 -fPIC -DBENCHMARK_ENABLED=1 -Icharm/core/utilities/ -Icharm/core/benchmark/ -I/home/deva/py37-venv/include -I/
usr/include/python3.7m -c charm/core/math/pairing/pairingmodule.c -o build/temp.linux-x86_64-3.7/charm/core/math/pairing/pairingmodule.o
In file included from charm/core/math/pairing/pairingmodule.c:30:
charm/core/math/pairing/pairingmodule.h:37:10: fatal error: Python.h: No such file or directory
   37 | #include <Python.h>
      |          ^~~~~~~~~~
compilation terminated.
error: command 'x86_64-linux-gnu-gcc' failed with exit status 1
make: *** [Makefile:29: all] Error 1
```

  - ➢ Sudo –E env PATH=$PATH { command }

Caution : Do use python3.7 in virtual environment and avoiding root environment (contains the latest versions of python i.e. not supported by charm library) .



```
copying charm/schemes/pksig/pksig_lamport.py -> build/lib.linux-x86_64-cpython-312/charm/schemes/pksig
creating build/lib.linux-x86_64-cpython-312/charm/schemes/commit
copying charm/schemes/commit/__init__.py -> build/lib.linux-x86_64-cpython-312/charm/schemes/commit
copying charm/schemes/commit/commit_pedersen92.py -> build/lib.linux-x86_64-cpython-312/charm/schemes/commit
copying charm/schemes/commit/commit_gs08.py -> build/lib.linux-x86_64-cpython-312/charm/schemes/commit
creating build/lib.linux-x86_64-cpython-312/charm/schemes/grpsig
copying charm/schemes/grpsig/__init__.py -> build/lib.linux-x86_64-cpython-312/charm/schemes/grpsig
copying charm/schemes/grpsig/groupsig_bgls04_var.py -> build/lib.linux-x86_64-cpython-312/charm/schemes/grpsig
copying charm/schemes/grpsig/groupsig_bgls04.py -> build/lib.linux-x86_64-cpython-312/charm/schemes/grpsig
creating build/lib.linux-x86_64-cpython-312/charm/schemes/prenc
copying charm/schemes/prenc/pre_nal16.py -> build/lib.linux-x86_64-cpython-312/charm/schemes/prenc
copying charm/schemes/prenc/pre_afgh06.py -> build/lib.linux-x86_64-cpython-312/charm/schemes/prenc
copying charm/schemes/prenc/pre_bbs98.py -> build/lib.linux-x86_64-cpython-312/charm/schemes/prenc
creating build/lib.linux-x86_64-cpython-312/charm/adapters
copying charm/adapters/abenc_adapt_hybrid.py -> build/lib.linux-x86_64-cpython-312/charm/adapters
copying charm/adapters/ibenc_adapt_hybrid.py -> build/lib.linux-x86_64-cpython-312/charm/adapters
copying charm/adapters/dabenc_adapt_hybrid.py -> build/lib.linux-x86_64-cpython-312/charm/adapters
copying charm/adapters/kpabenc_adapt_hybrid.py -> build/lib.linux-x86_64-cpython-312/charm/adapters
copying charm/adapters/pkenc_adapt_bchk05.py -> build/lib.linux-x86_64-cpython-312/charm/adapters
copying charm/adapters/__init__.py -> build/lib.linux-x86_64-cpython-312/charm/adapters
copying charm/adapters/pkenc_adapt_chk04.py -> build/lib.linux-x86_64-cpython-312/charm/adapters
copying charm/adapters/ibenc_adapt_identityhash.py -> build/lib.linux-x86_64-cpython-312/charm/adapters
copying charm/adapters/pksig_adapt_naor01.py -> build/lib.linux-x86_64-cpython-312/charm/adapters
copying charm/adapters/pkenc_adapt_hybrid.py -> build/lib.linux-x86_64-cpython-312/charm/adapters
running build_ext
building 'charm.core.math.pairing' extension
creating build/temp.linux-x86_64-cpython-312
creating build/temp.linux-x86_64-cpython-312/charm
creating build/temp.linux-x86_64-cpython-312/charm/core
creating build/temp.linux-x86_64-cpython-312/charm/core/benchmark
creating build/temp.linux-x86_64-cpython-312/charm/core/math
creating build/temp.linux-x86_64-cpython-312/charm/core/math/pairing
creating build/temp.linux-x86_64-cpython-312/charm/core/utilities
x86_64-linux-gnu-gcc -fno-strict-overflow -Wsign-compare -DNDEBUG -g -O2 -Wall -fPIC -DBENCHMARK_ENABLED=1 -Icharm/core/utilities/ -Icharm/core/benchmark/ -I/usr/include/python3.12 -c
charm/core/benchmark/benchmarkmodule.c -o build/temp.linux-x86_64-cpython-312/charm/core/benchmark/benchmarkmodule.o
x86_64-linux-gnu-gcc -fno-strict-overflow -Wsign-compare -DNDEBUG -g -O2 -Wall -fPIC -DBENCHMARK_ENABLED=1 -Icharm/core/utilities/ -Icharm/core/benchmark/ -I/usr/include/python3.12 -c
charm/core/math/pairing/pairingmodule.c -o build/temp.linux-x86_64-cpython-312/charm/core/math/pairing/pairingmodule.o
In file included from charm/core/math/pairing/pairingmodule.c:30:
charm/core/math/pairing/pairingmodule.h:39:10: fatal error: longintrepr.h: No such file or directory
   39 | #include <longintrepr.h>
      |          ^~~~~~~~~~~~~~~
compilation terminated.
error: command '/usr/bin/x86_64-linux-gnu-gcc' failed with exit code 1
make: *** [Makefile:29: all] Error 1
deva@deva-star:~/charm$ 
```