

# User Manual

## Necessary Python Packages

```
coverage==7.6.9  
sympy==1.13.3
```

## General Testing Report

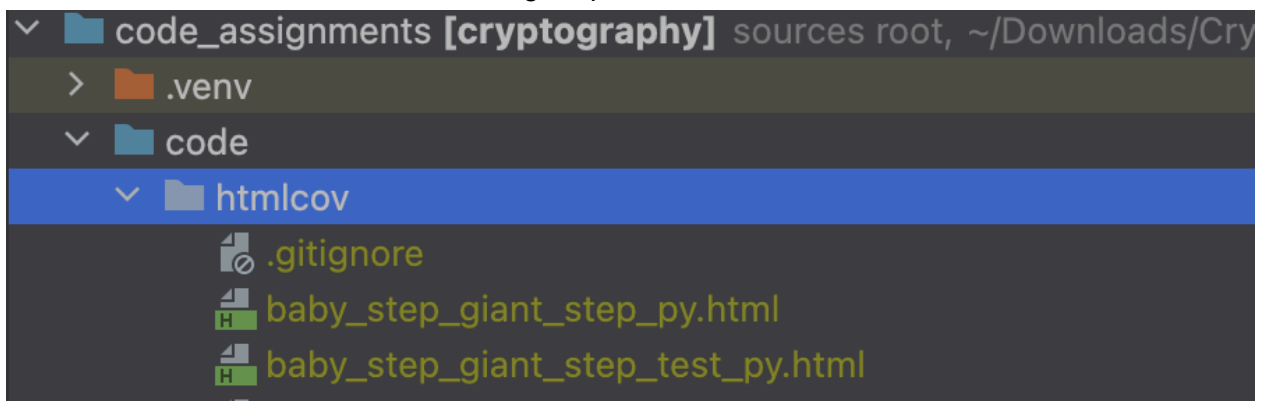
Open test\_coverage\_report.pdf to find out the line coverage report of all the tests.

## Run All the Tests at Once

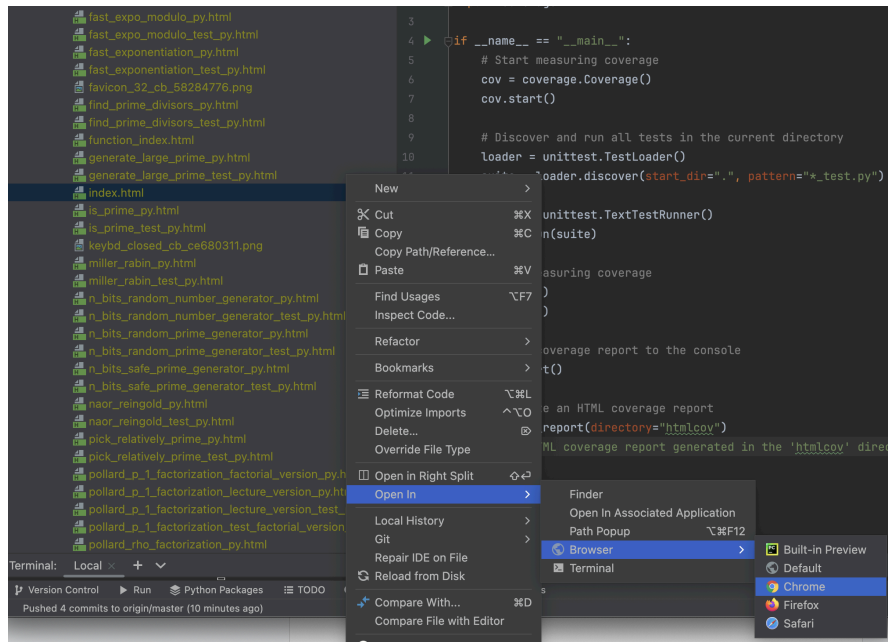
1 To run all the test modules in the project, run the following module.



2 After that, a more detailed test coverage report can be found in **htmlcov** folder.



3 follow the following path to open the test coverage report **index.html**.



## RSA Related

Encrypt: use `rsa_decrypt(private_key, ciphertext) :` in `rsa_without_padding.py`

Decrypt: use `rsa_encrypt(public_key, plaintext)` in `rsa_without_padding.py`

Break: use `break_rsa_with_pollard_rho(public_key, ciphertext) :` in `break_rsa.py`

All necessary helper functions can be found in the same module.

## EL Gamal Related

Encrypt: use `el_gamal_encrypt(message, b_to_power_of_l, r, prime)` in `el_gamal.py`

Decrypt: use `el_gamal_decrypt(cipher_text, brl_inverse, prime) :`  
in `el_gamal.py`

Break: use `break_el_gamal(cipher_text, p, b, b_to_power_of_r, b_to_power_of_l) :`  
in `break_el_gamal.py`

All necessary helper functions can be found in the same module.