
AdafruitRSA Library Documentation

Release 1.0

Brent Rubell

Jan 14, 2020

Contents

1	Dependencies	3
2	Installing from PyPI	5
3	Usage Example	7
4	Contributing	9
5	Documentation	11
6	Table of Contents	13
6.1	Simple test	13
6.2	Adafruit CircuitPython RSA API	14
7	Indices and tables	15
	Python Module Index	17
	Index	19

RSA implementation based on [Sybren A. Stüvel's python-rsa](#) pure-python RSA implementation.

CHAPTER 1

Dependencies

This driver depends on:

- [Adafruit CircuitPython](#)
- [Adafruit CircuitPython Logger Module](#)

Please ensure all dependencies are available on the CircuitPython filesystem. This is easily achieved by downloading the [Adafruit library and driver bundle](#).

CHAPTER 2

Installing from PyPI

On supported GNU/Linux systems like the Raspberry Pi, you can install the driver locally [from PyPI](#). To install for current user:

```
pip3 install adafruit-circuitpython-rsa
```

To install system-wide (this may be required in some cases):

```
sudo pip3 install adafruit-circuitpython-rsa
```

To install in a virtual environment in your current project:

```
mkdir project-name && cd project-name  
python3 -m venv .env  
source .env/bin/activate  
pip3 install adafruit-circuitpython-rsa
```


CHAPTER 3

Usage Example

Examples for this library are available in the examples/ folder.

CHAPTER 4

Contributing

Contributions are welcome! Please read our [Code of Conduct](#) before contributing to help this project stay welcoming.

CHAPTER 5

Documentation

For information on building library documentation, please check out [this guide](#).

6.1 Simple test

Ensure your device works with this simple test.

Listing 1: examples/rsa_simpletest.py

```
1 # Adafruit_CircuitPython_RSA Encryption/Decryption
2 import adafruit_rsa
3
4 # Create a keypair
5 print("Generating keypair...")
6 (public_key, private_key) = adafruit_rsa.newkeys(512)
7
8 # Message to send
9 message = "hello blinka"
10
11 # Encode the string as bytes (Adafruit_RSA only operates on bytes!)
12 message = message.encode("utf-8")
13
14 # Encrypt the message using the public key
15 print("Encrypting message...")
16 encrypted_message = adafruit_rsa.encrypt(message, public_key)
17
18 # Decrypt the encrypted message using a private key
19 print("Decrypting message...")
20 decrypted_message = adafruit_rsa.decrypt(encrypted_message, private_key)
21
22 # Print out the decrypted message
23 print("Decrypted Message: ", decrypted_message.decode("utf-8"))
```

6.2 Adafruit CircuitPython RSA API

RSA module

Module for calculating large primes, and RSA encryption, decryption, signing and verification. Includes generating public and private keys.

WARNING: this implementation does not use compression of the cleartext input to prevent repetitions, or other common security improvements. Use with care.

CHAPTER 7

Indices and tables

- `genindex`
- `modindex`
- `search`

a

adafruit_rsa, 14

A

adafruit_rsa (*module*), 14