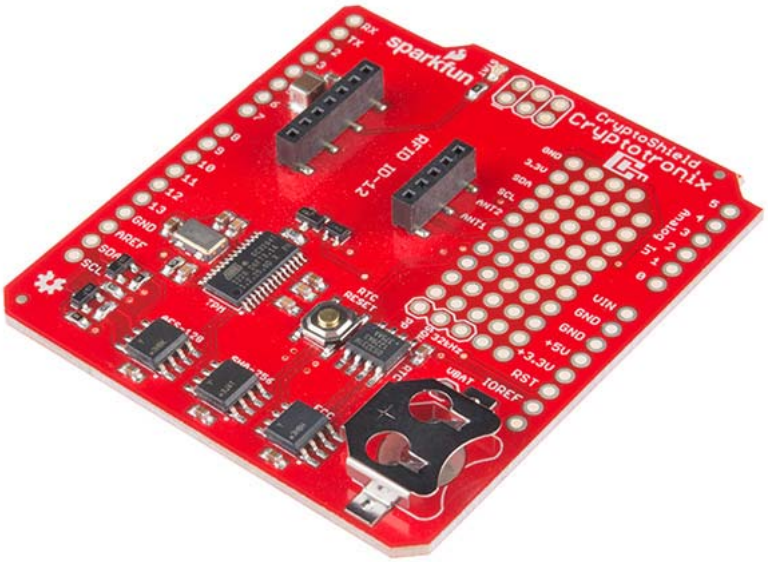
SparkFun CryptoShield

DEV-13183 ROHS



$59.95

Shipping outside of the US?
Click here for info

1	quantity
	22 in stock
$59.95	1+ units
$56.95	10+ units
$53.96	25+ units
$50.96	100+ units

Need larger quantities?
Check out our Volume Sales program

3D Download: Sketchup, STL, Blender

Description: The CryptoShield is a dedicated security peripheral for the Arduino and was made in collaboration with a previous Hacker In Residence, Josh Datko. This shield adds specialized ICs that perform various cryptographic operations which will allow you to add a hardware security layer to your Arduino project. It also is a nice device for those performing embedded security research. Needless to say this is a great product for those of you who are interested in computer security!

On board each CryptoShield is a slew of hardware fresh for your use: a real time clock (RTC) module to keep accurate time, a trusted platform module (TPM) for RSA encryption/decryption and signing in the hardware, an AES-128 encrypted EEPROM, an ATSHA204 authentication chip that performs SHA-256 and HMAC-256, and an ATECC108 that performs the Elliptic Curve Digital Signature Algorithm (ECDSA). Unlike its cousin, the CryptoCape, we've shrunk the prototyping area but added an RFID socket that works best with a ID-12LA module.

Each CryptoShield will need to have headers soldered on once you receive it. We prefer to give you the choice of soldering on stackable or non-stackable headers, whatever fits best for you project. The only other items you will need to get the CryptoCape fully functional are a dev board that supports the Arduino R3 form-factor and a CR1225 coin cell battery. All of these additional parts can be found in the *Recommended Products* section below.

Note: A portion of each sale is given back to Josh Datko for continued development of new and exciting Cryptographic tools.

SparkFun CryptoShield

Features:

- Encryption and Decryption Hardware Pre-Installed
- Encrypted EEPROM
- RSA Encryption/Decryption
- SHA-256 & HMAC-256
- Elliptic Curve Digital Signature Algorithm
- RFID Socket
- Prototyping Area

Documents:

- Schematic
- Eagle Files
- Hookup Guide
- Datasheets:
  - ATAES132 (AES-128)
  - DS3231MZ/V+ (RTC)
  - AT97SC3204T (TPM)
  - ATSHA204 (SHA-256)
  - ATECC108 (ECC)
- CCATS
- GitHub (Design Files)

Recommended Products

PAGE 1 OF 6

SPARKFUN RECOMMENDED
SparkFun RedBoard - Programmed with Arduino
DEV-12757
$19.95
4.5 stars 116

SPARKFUN RECOMMENDED
Arduino Uno - R3
DEV-11021
$24.95
4.5 stars 85

SPARKFUN RECOMMENDED
SparkFun RFID Starter Kit
KIT-13198
$49.95
4.5 stars 11

SPARKFUN RECOMMENDED
RFID Reader ID-12LA (125 kHz)
SEN-11827
$29.95
4.5 stars 7

COMMENTS 30 | REVIEWS 0 | **TUTORIALS 1**

Related Tutorials

Crypto Shield Hookup Guide
APRIL 23, 2015
How to start using the CryptoShield for Arduino, created in collaboration with Cryptronix.