HACKING RFIDs UNDER 2000INR

-Jayesh Singh Chauhan

About Me

- Sr. Security Engineer at PwC SDC
- OWASP SKANDA and CSRF POC generator
- OSCP
- Epitome of laziness

Topics

- RFID history
- History of RFID
- Death of the Technology
- Resurrection
- The Future
- Delve deeper
- Types of RFID

How it Began

- World War II, and the Germans rolled.
  - To distinguish the planes from that of the enemies'
- Commercialization of RFID
  - Tracking utility
  - Trucks, cows, carriages

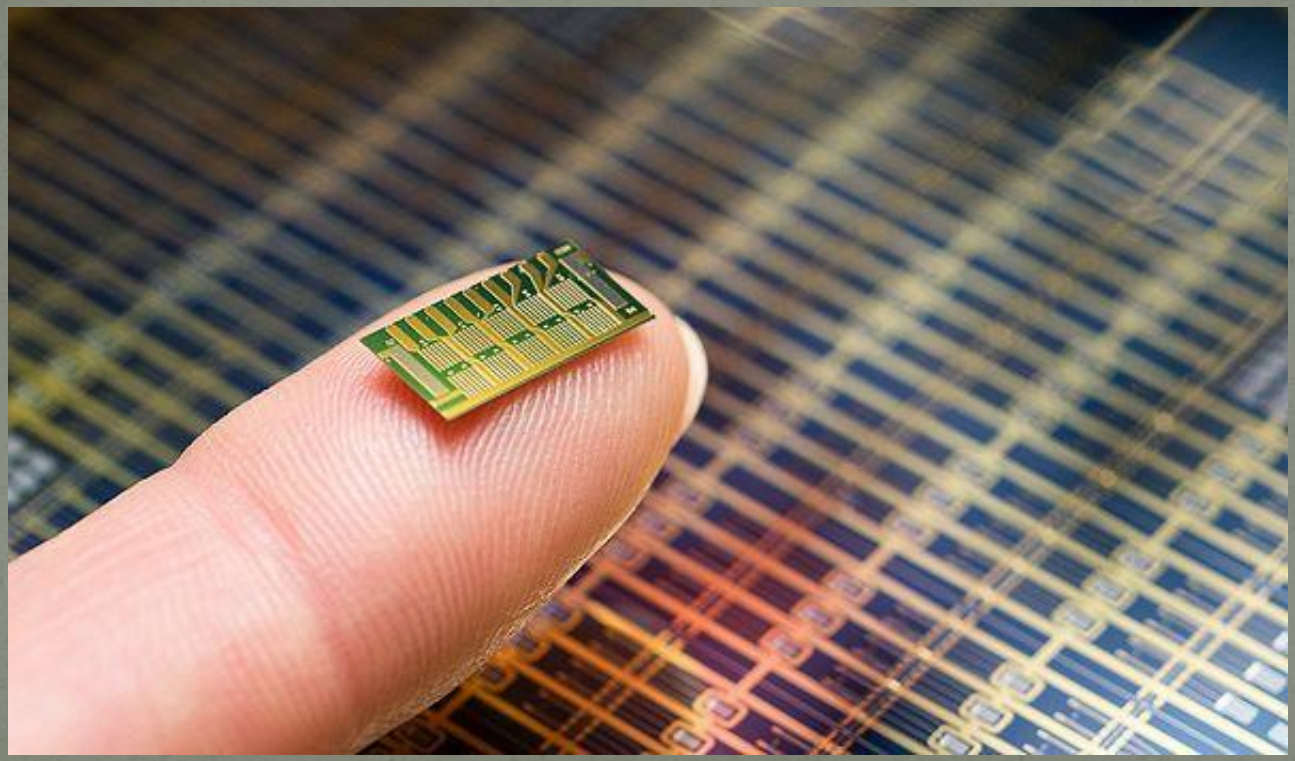
Technology Death

- 2 reasons
  - The impractical size of the RFID system
  - Cost of Production

- Early face of RFID tags
  - Inductively coupled RFID tags
  - Capacitively couple RFID tags

Resurrection of RFID

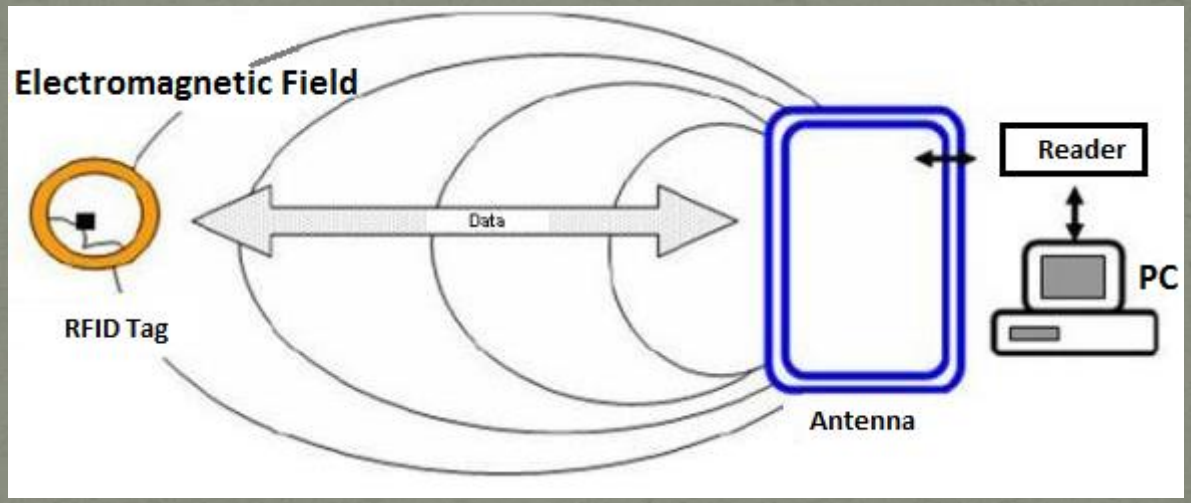
- The change – Introduction of Microchips



Where the Future lies

- Tracking and identification
- Payment and stored-value systems
- Access control
- Anti-Counterfeiting

Delving into the Technology



Types of RFID (Frequency based)

- Low Frequency
  - 30kHz to 300kHz
  - Typical: 125kHz
- High Frequency
  - 3 to 30 MHz
  - Typical: 13.56MHz
- Ultra High Frequency
  - 300MHz to 3GHz
  - Typical: 900 to 915Mhz

Types of RFID (design based)

- Active
  - Battery powers the system
- Semi-Passive
  - This too has a battery
- Passive
  - No battery

More on Active Tags

- Two types of Active Tags:
  - Transponders
  - Beacons

Types of RFID (based on usability)

- Read-only
- Read-Write
- WORM – Write Once Read Many

Important Blocks

- Block 0:

byte															byte
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Serial number				CB	manufacturer data										

CB: "serial number check byte" CB = byte 0 ^ byte 1 ^ byte 2 ^ byte 3 (^ ... XOR)

- Block 3 in each sector is the Sector Trailer

default coding:

byte															byte
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
transport key A						FF	07	80	xx	transport key B					

(blocks 3 / 7 / 11 / 15 / 19 / 23 / 27 / 31 / 35 / 39 / 43 / 47 / 51 / 55 / 59 / 63)
Byte 9 of all sector trailers is not defined. Its memory contents after IC test can vary.

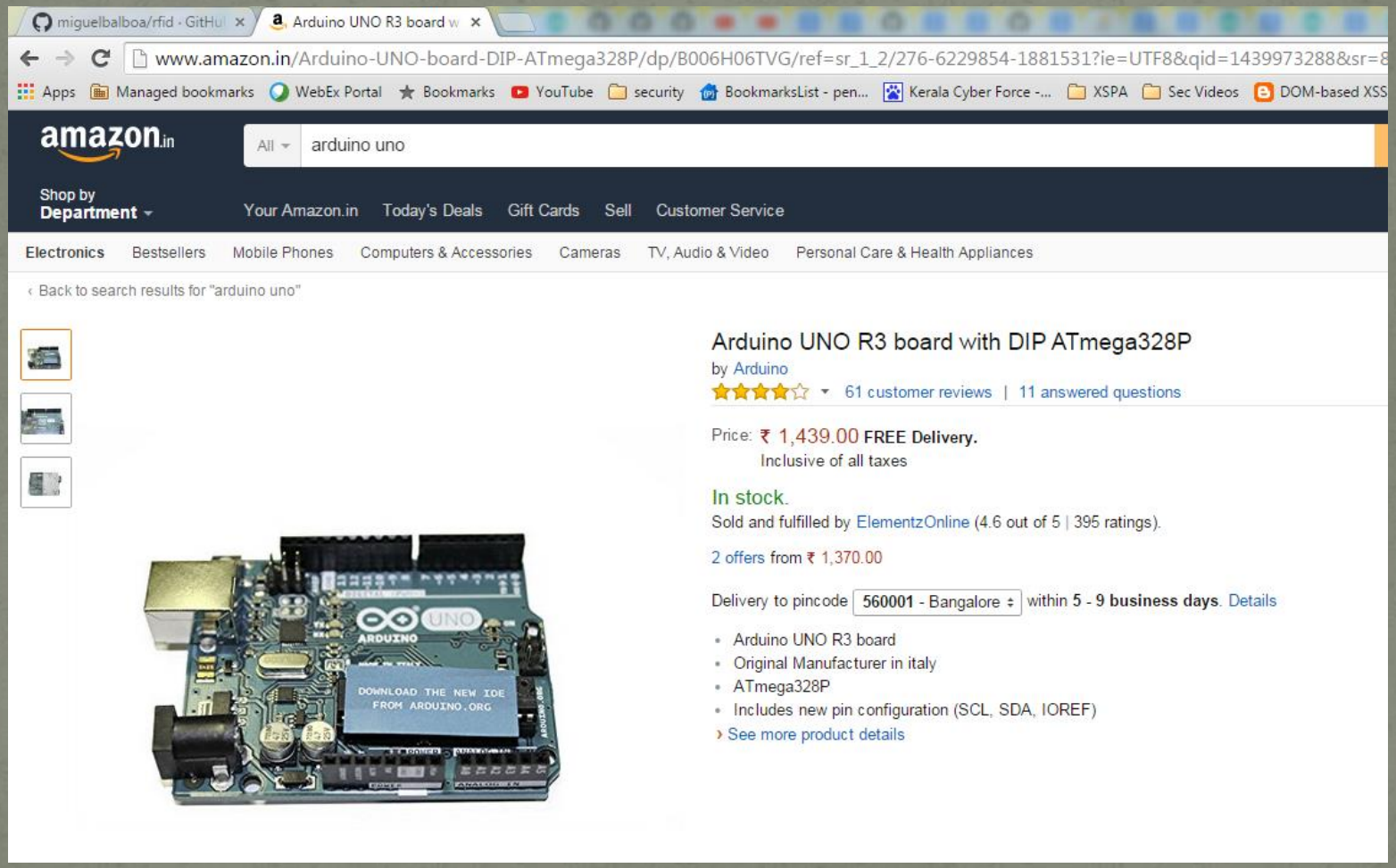
Data space in MIFARE Classic (1 KB)

- (16 sectors/card x 3 data blocks/sector X 16 bytes/block) – 16 bytes (first block) = 752 bytes/card

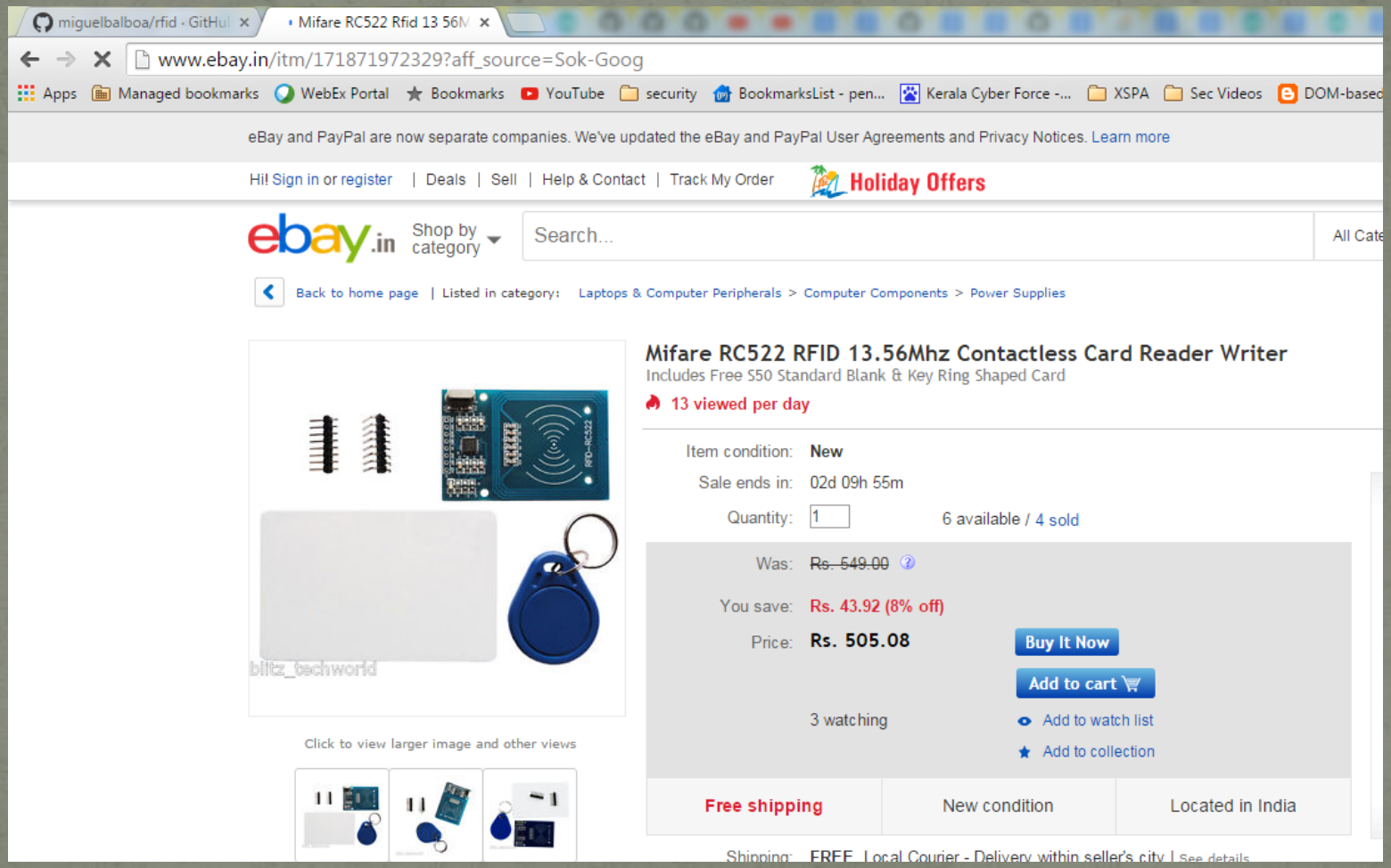
Setup

- Arduino Uno
- MFRC522
- MIFARE Classic Card/Tags – 13.56 Mhz
- Jumper Wires
- MFRC522.h Library

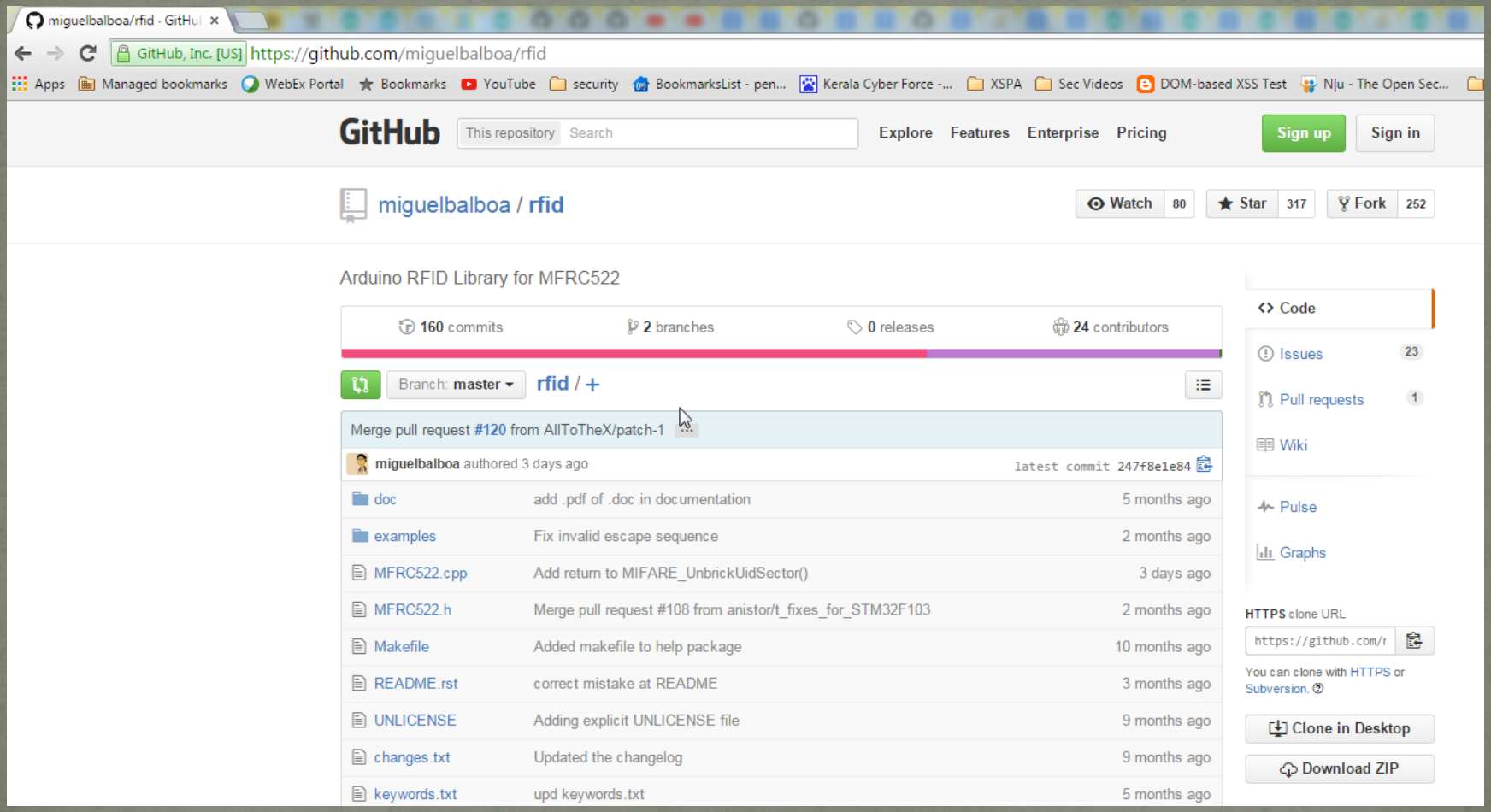
Arduino Uno


miguelbalboa/rfid - GitHu
Arduino UNO R3 board w
www.amazon.in/Arduino-UNO-board-DIP-ATmega328P/dp/B006H06TVG/ref=sr_1_2/276-6229854-1881531?ie=UTF8&qid=1439973288&sr=8
Apps
Managed bookmarks
WebEx Portal
Bookmarks
YouTube
security
BookmarksList - pen...
Kerala Cyber Force -...
XSPA
Sec Videos
DOM-based XSS
amazon.in
All
arduino uno
Shop by Department
Your Amazon.in
Today's Deals
Gift Cards
Sell
Customer Service
Electronics
Bestsellers
Mobile Phones
Computers & Accessories
Cameras
TV, Audio & Video
Personal Care & Health Appliances
‹ Back to search results for "arduino uno"
Arduino UNO R3 board with DIP ATmega328P
by Arduino
61 customer reviews | 11 answered questions
Price: ₹ 1,439.00 FREE Delivery.
Inclusive of all taxes
In stock.
Sold and fulfilled by ElementzOnline (4.6 out of 5 | 395 ratings).
2 offers from ₹ 1,370.00
Delivery to pincode 560001 - Bangalore within 5 - 9 business days. Details
Arduino UNO R3 board
Original Manufacturer in italy
ATmega328P
Includes new pin configuration (SCL, SDA, IOREF)
› See more product details
UNO
ARDUINO
DOWNLOAD THE NEW IDE
FROM ARDUINO.ORG

MFRC522


miguelbalboa/rfid · GitHu
Mifare RC522 Rfid 13 56M
www.ebay.in/itm/171871972329?aff_source=Sok-Goog
Apps
Managed bookmarks
WebEx Portal
Bookmarks
YouTube
security
BookmarksList - pen...
Kerala Cyber Force -...
XSPA
Sec Videos
DOM-based
eBay and PayPal are now separate companies. We've updated the eBay and PayPal User Agreements and Privacy Notices. Learn more
Hi! Sign in or register | Deals | Sell | Help & Contact | Track My Order
Holiday Offers
ebay.in
Shop by category
Search...
All Cate
Back to home page | Listed in category: Laptops & Computer Peripherals > Computer Components > Power Supplies
Mifare RC522 RFID 13.56Mhz Contactless Card Reader Writer
Includes Free S50 Standard Blank & Key Ring Shaped Card
13 viewed per day
Item condition: New
Sale ends in: 02d 09h 55m
Quantity: 1
6 available / 4 sold
Was: Rs. 549.00
You save: Rs. 43.92 (8% off)
Price: Rs. 505.08
Buy It Now
Add to cart
3 watching
Add to watch list
Add to collection
Free shipping
New condition
Located in India
Click to view larger image and other views
blitz_techworld

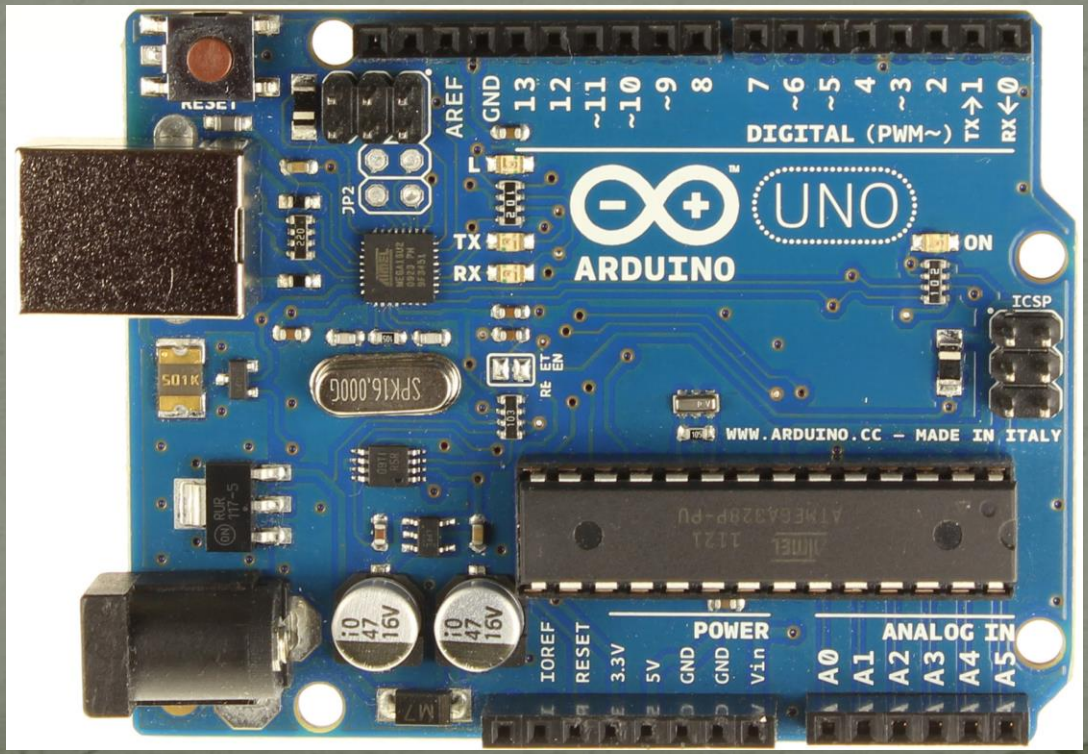
RFID Library



Important Hardware Involved

- Micro Controller: An Arduino
- PCD(Proximity Coupling Device):MFRC522
- PICC (Proximity Integrated Circuit Card): card
  - 16 sectors * 4 blocks/sector * 16 bytes/block = 1024 bytes

Demo


RESET
AREF
GND
13
12
~11
~10
~9
8
7
~6
~5
4
~3
2
TX→1
RX←0
DIGITAL (PWM~)
L
TX
RX
UNO
ARDUINO
ON
ICSP
JP2
WWW.ARDUINO.CC – MADE IN ITALY
POWER
ANALOG IN
IOREF
RESET
3.3V
5V
GND
GND
Vin
A0
A1
A2
A3
A4
A5

Cloners - Out of the box

- Proxmark3
- BishopFox

Q & A ?

Credits

- Yashin Mehaboobe
- Miguel Balboa

Contact

- @jayeshsch