Week 03
Crypto II

Anakin, Hassam, Husnain, Nebu, Pranav

Meeting Flag

sigpwny{numbers_are_hard}

ALICE SENDS A MESSAGE TO BOB SAYING TO MEET HER SOMEWHERE.
UH HUH.
BUT EVE SEES IT, TOO, AND GOES TO THE PLACE.
WITH YOU SO FAR.
BOB IS DELAYED, AND ALICE AND EVE MEET.
YEAH?
I'VE DISCOVERED A WAY TO GET COMPUTER SCIENTISTS TO LISTEN TO ANY BORING STORY.

Announcements

Scoreboard should be properly reset (lmk if no)

Minecraft server (mc.sigpwny.club) VERIFY W Discord

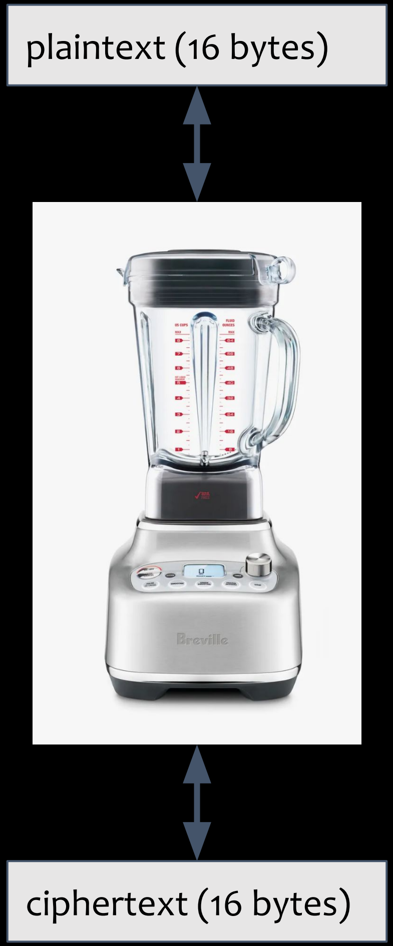
Thursday meeting changed (again)

CTFd Reskin (Open to any!)

Tools

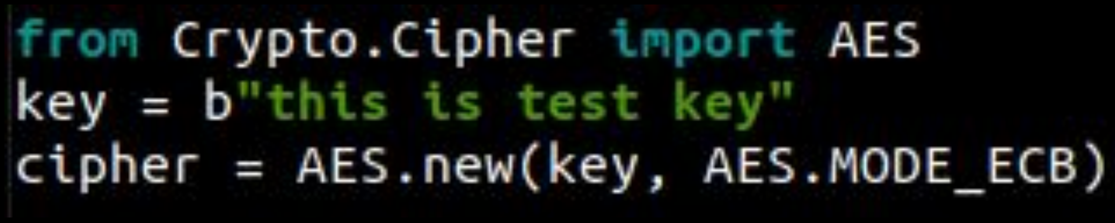
- Crypto often requires a lot of various tools that are difficult to install
- Instead of trying to install 6+ tools on three different OSs, use Docker!
- Check links in Discord
- https://docs.docker.com/get-docker/
- https://github.com/cryptohack/cryptohack-docker
  - `docker pull hyperreality/cryptohack:latest`
  - `docker run -p 127.0.0.1:8888:8888 -it hyperreality/cryptohack:latest`
- https://github.com/Ganapati/RsaCtfTool

AES

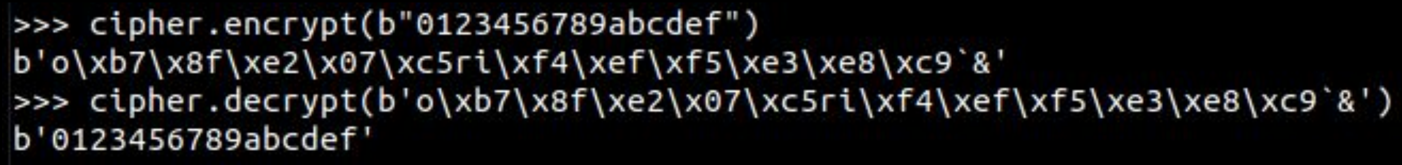


plaintext (16 bytes)

ciphertext (16 bytes)

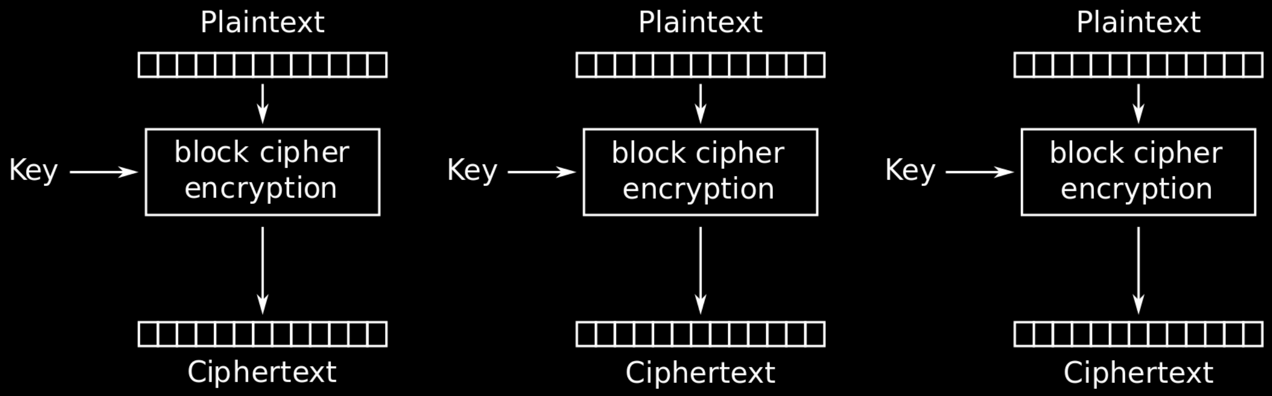


```python
from Crypto.Cipher import AES
key = b"this is test key"
cipher = AES.new(key, AES.MODE_ECB)
```

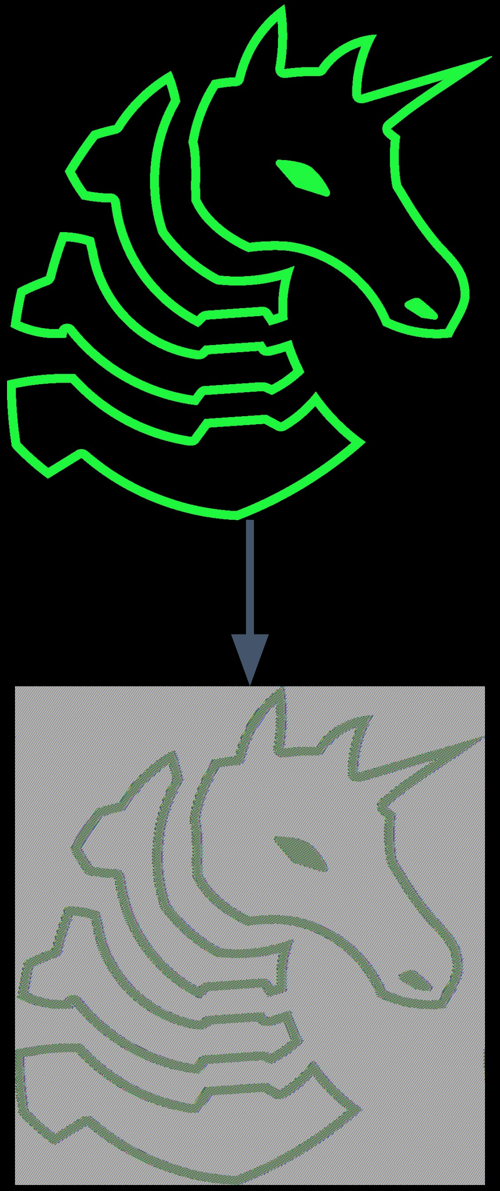


```
>>> cipher.encrypt(b"0123456789abcdef")
b'o\xb7\x8f\xe2\x07\xc5ri\xf4\xef\xf5\xe3\xe8\xc9`&'
>>> cipher.decrypt(b'o\xb7\x8f\xe2\x07\xc5ri\xf4\xef\xf5\xe3\xe8\xc9`&')
b'0123456789abcdef'
```

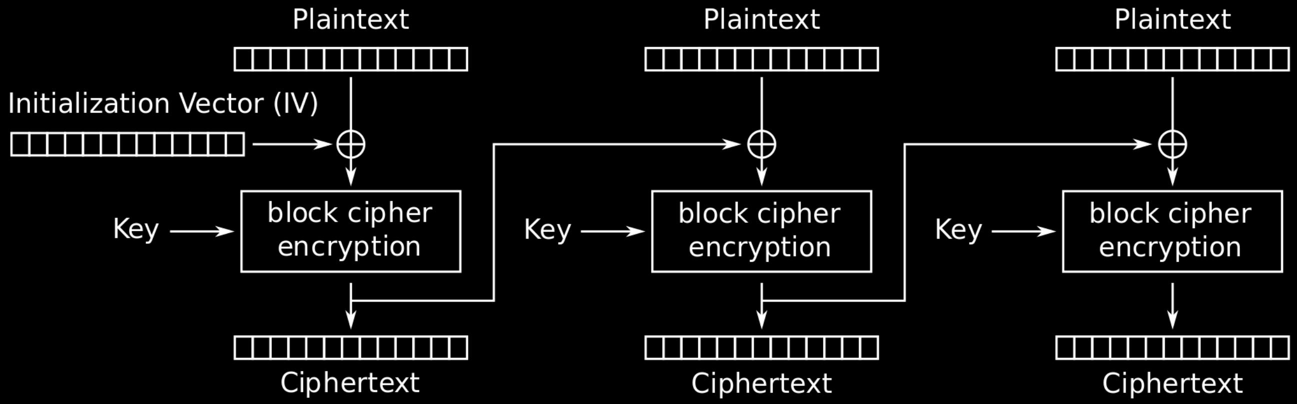
ECB Mode



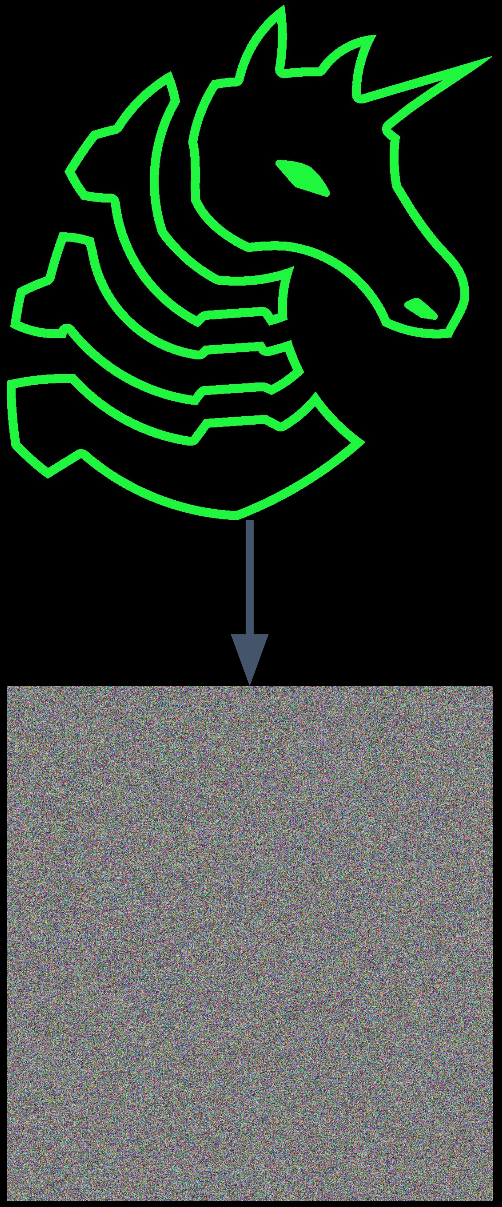
Electronic Codebook (ECB) mode encryption



CBC Mode



Cipher Block Chaining (CBC) mode encryption



RSA: In Some Detail

- Generate two primes p and q
- Multiply $n = pq$
- Compute $\lambda(n) = \mathrm{lcm}(p - 1, q - 1)$.
- Choose an integer e such that it is coprime $\lambda(n)$.
- $e = 65537$
- **The public key tuple is (n,e)**
- Compute $d \equiv e^{-1} \pmod{\lambda(n)}$
- **The tuple (d, p, q) is the private key.**

RSA

- Alice releases her public key tuple (n, e). To send her a message, Bob computes:
- $m^e \equiv c \pmod{n}$
- And sends her c.

- Alice on the other end simply computes:
- $c^d \equiv m \pmod{n}$
- And recovers m.

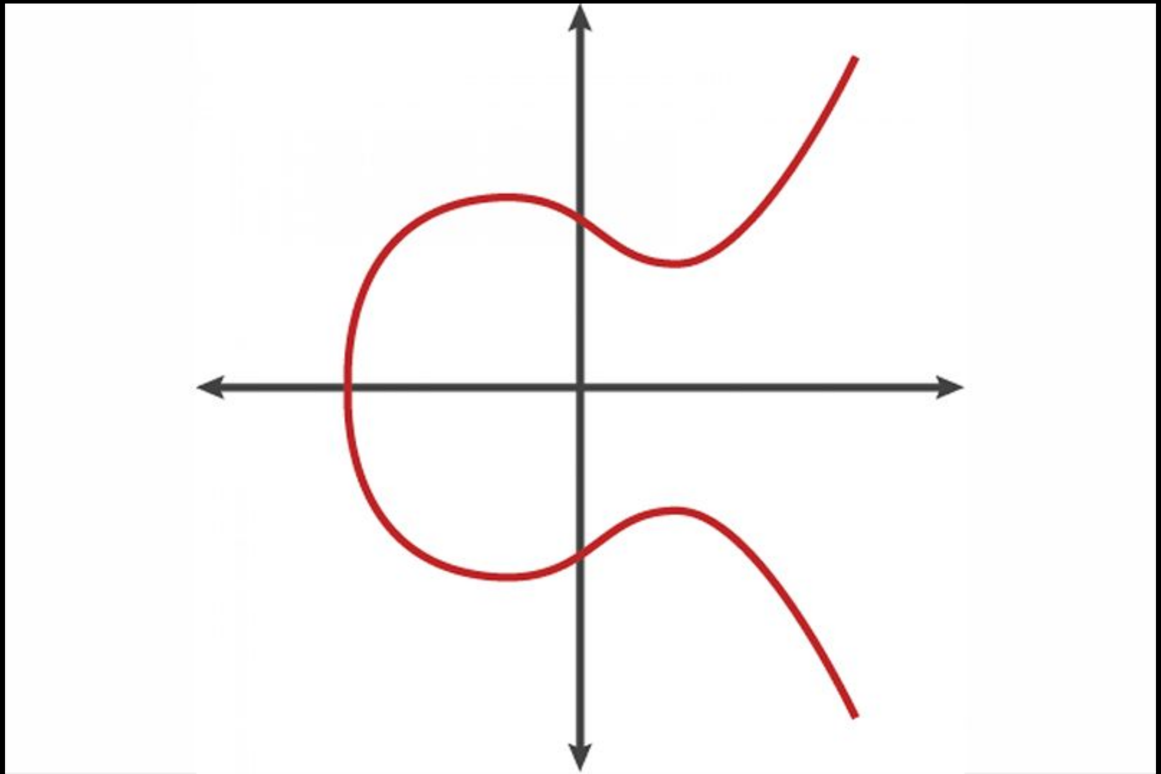
RSA Attacks

- n too small - just factor it! (gets unfeasible once n is larger than ~512 bits)
- d too small ⟶ Wiener’s attack
- e too small / partial key known ⟶ Coppersmith’s attack
- multiple moduli ⟶ Batch GCD
- faulty prime generation
- Something else ⟶ Google! (Or learn the math)

Discrete Log

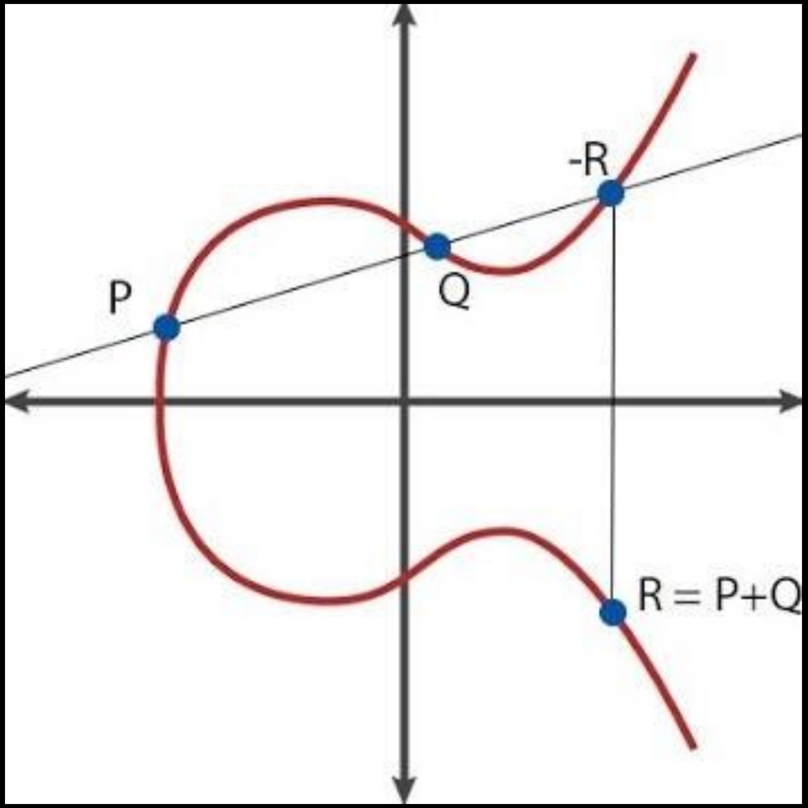
- Consider the integers mod some prime p:
  - {0, 1, 2, …, p - 1}
- We want integer solutions x given a, b such that a^x = b (mod p)
- "Trapdoor" function
  - Multiplying is computationally easy
  - Factoring / reversing is computationally difficult

Elliptic Curves



$y^2 = x^3 + ax + b$

Elliptic Curves



y^2 = x^3 + ax + b

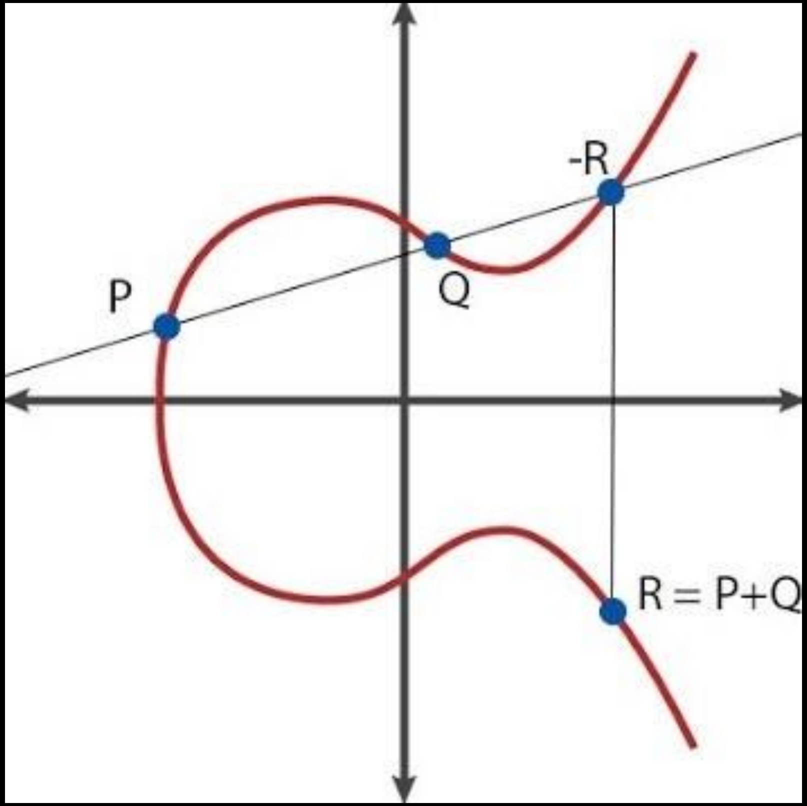
Elliptic Curves: Adding

P + Q = R

m = slope

x_R = m^2 - x_P - x_ Q

y_r = y_p + m(x_R - x_P)



y^2 = x^3 + ax + b

Elliptic Curves: Multiply

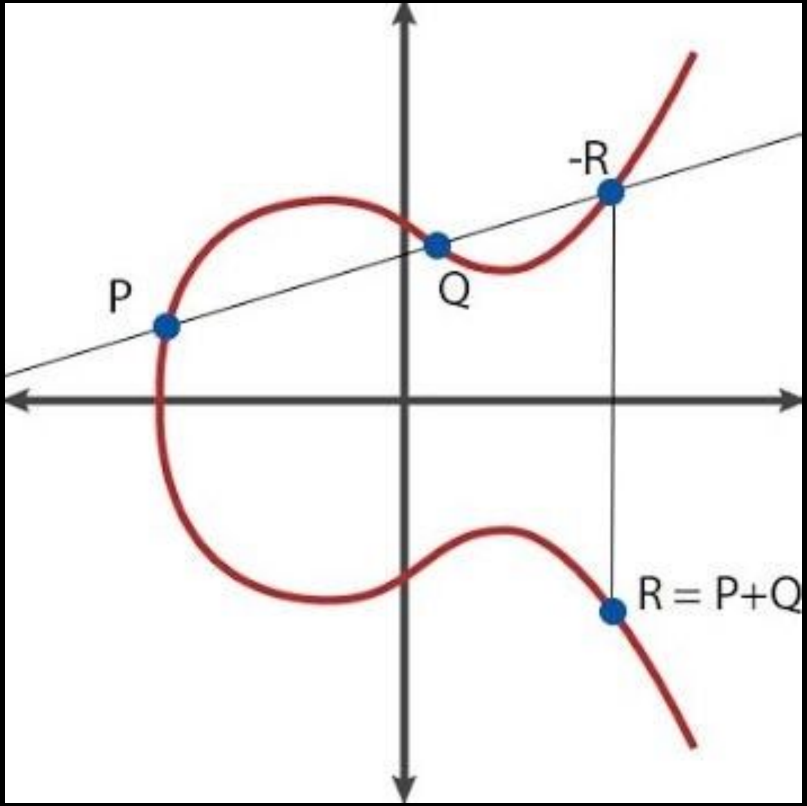
P + Q = R

m = slope

x_R = m^2 - x_P - x_ Q

y_r = y_p + m(x_R - x_P)

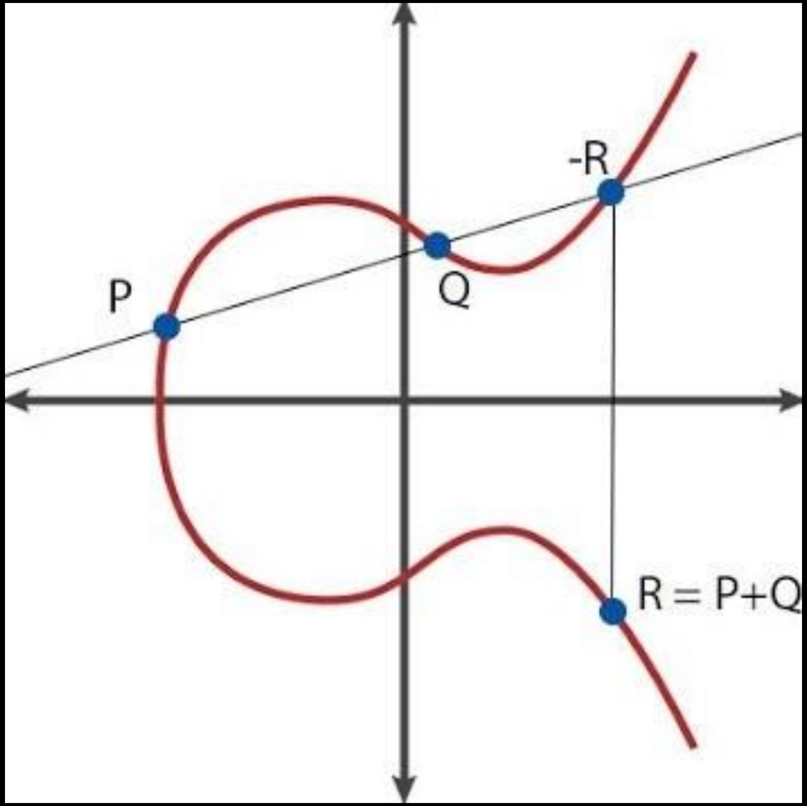
Just double and add!!



y^2 = x^3 + ax + b

Elliptic Curve Discrete Log Problem

Given points Q and P:
find k such that
Q = k*P

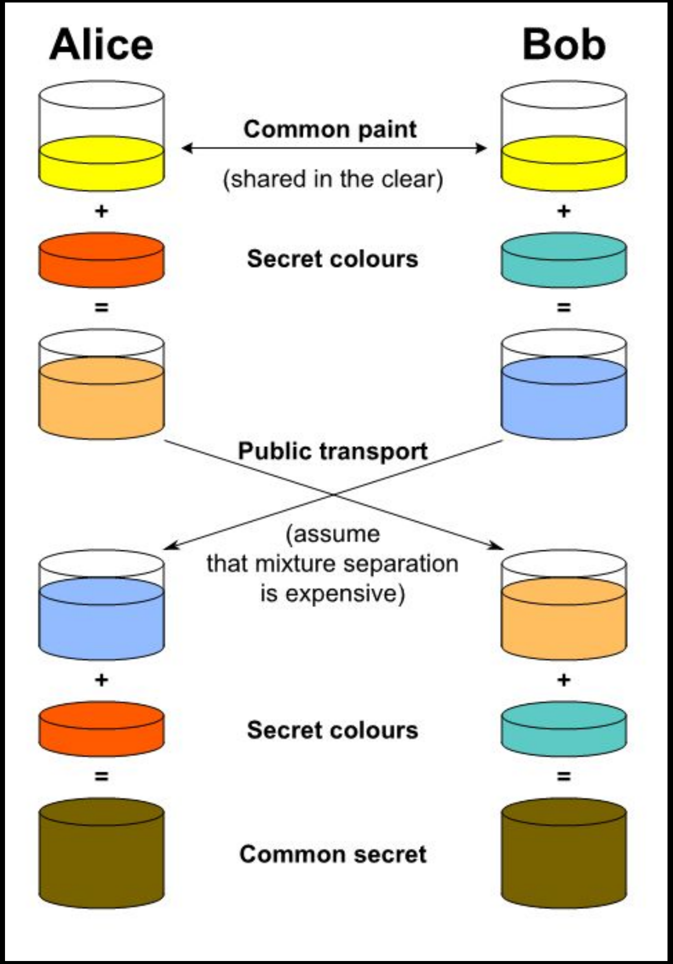


y^2 = x^3 + ax + b

Elliptic Curve Discrete Log Problem

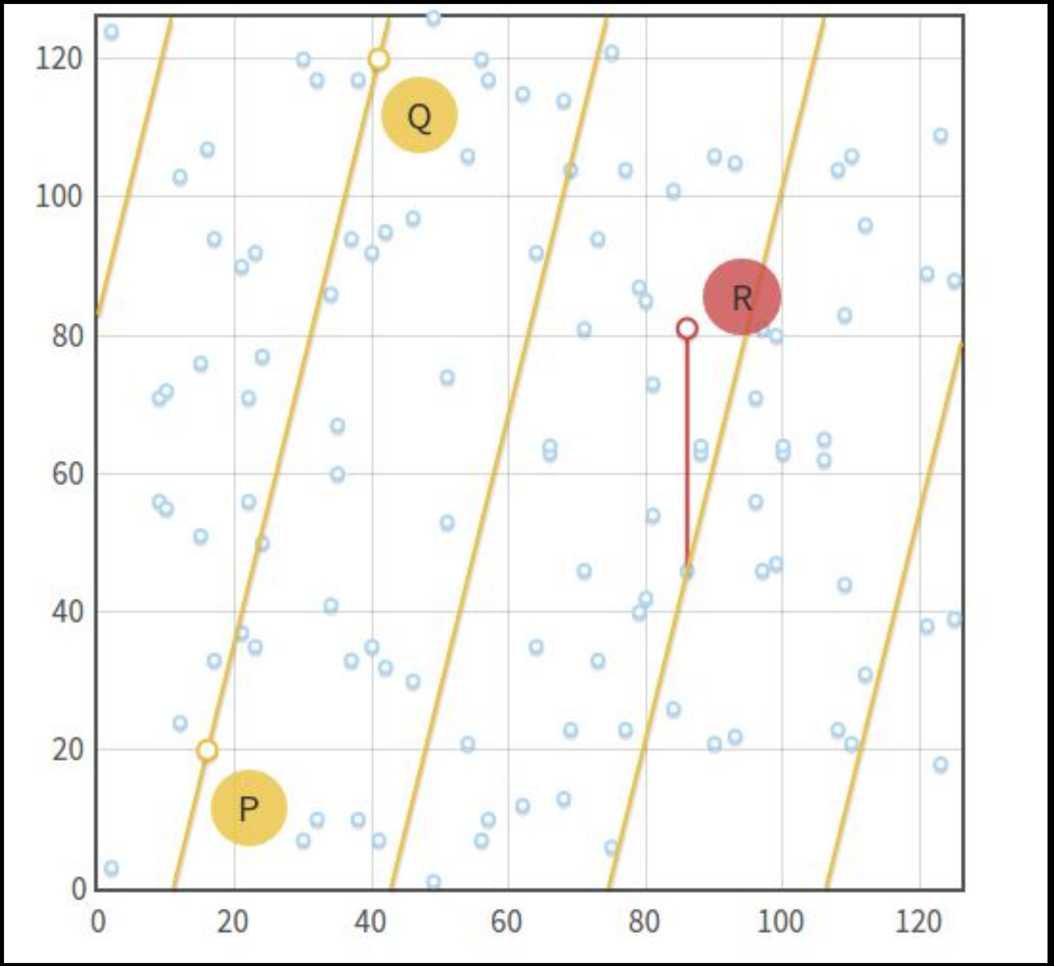
Old and Boring: DH

- Alice and Bob share g, large prime p
- Alice has secret a
  - Sends g^a (mod p)
- Bob has secret b
  - Sends g^b (mod p)
- Both now have g^a^b (mod p)



New and Cool: ECDH

- Alice and Bob share G, large prime p
- Alice has secret a
  - Sends G * a(mod p)
- Bob has secret b
  - Sends G * b (mod p)
- Both now have G * a *b (mod p)



What is the point?

RSA Key Size (bits)	ECC Key Size (bits)
1024	160
2048	244
3072	256
7680	384
15360	521

How to deal with ECC

- **Implement it yourself**

How to deal with ECC

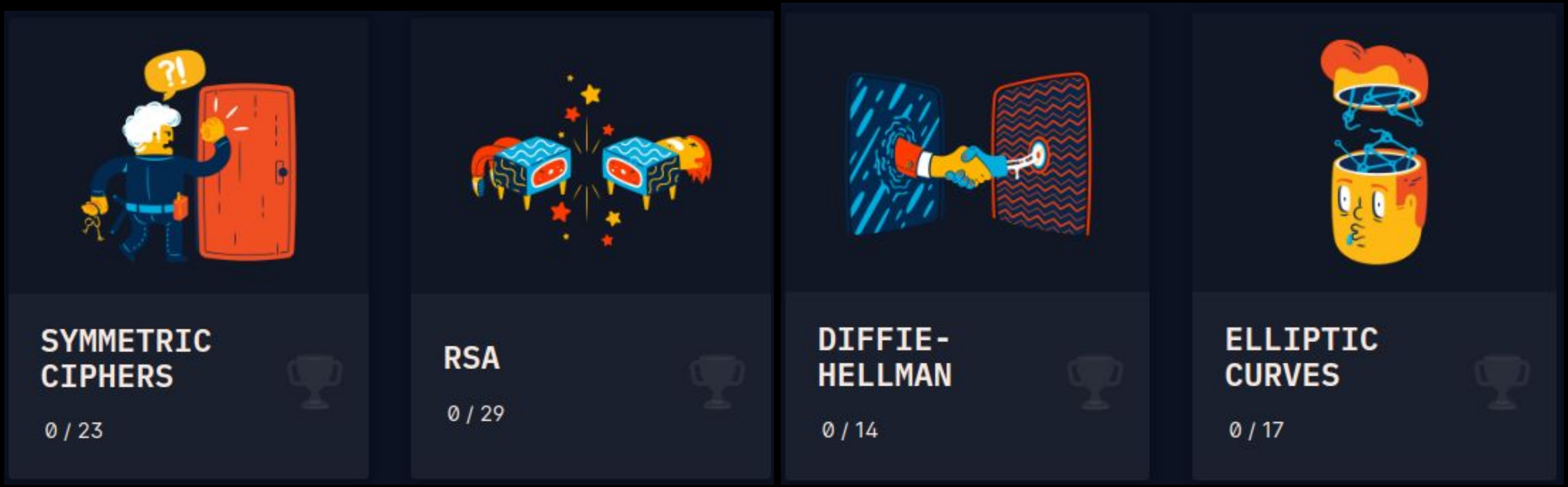
- ~~Implement it yourself~~
- Sagemath
  - Cryptohack Docker File!!!
  - TLDR
    - `docker pull hyperreality/cryptohack:latest`
    - `docker run -p 127.0.0.1:8888:8888 -it hyperreality/cryptohack:latest`
- Google algorithms and attacks
  - Curves do not live in a democracy
    - Some are better than others
  - Order of curve
  - Small primes (or not even using primes!!)
  - Singular Curves
  - Other patterns

How Do I practice?

this is cool!

Do CryptoHack!

https://discord.com/invite/h9E7cna5pV



SYMMETRIC CIPHERS

0 / 23

RSA

0 / 29

DIFFIE-HELLMAN

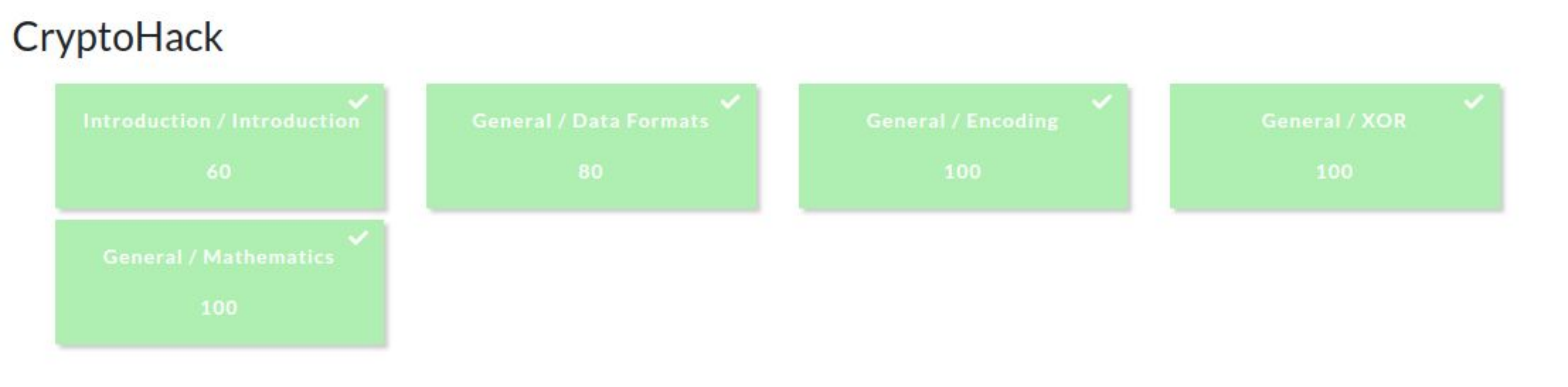
0 / 14

ELLIPTIC CURVES

0 / 17

Do CryptoHack!

https://discord.com/invite/h9E7cna5pV



CryptoHack

✓ Introduction / Introduction
60

✓ General / Data Formats
80

✓ General / Encoding
100

✓ General / XOR
100

✓ General / Mathematics
100

Next Meetings

Next Thursday: Opsec (Operational Security)

- Don’t get hacked!
- Don’t get embarrassed!
- Don’t get caught!
- VERY INTERACTIVE

Sunday Seminar: Crash Course on Law and Ethics

- Standard ethical models for security
- How to ethically report a vulnerability
- How NOT to get arrested