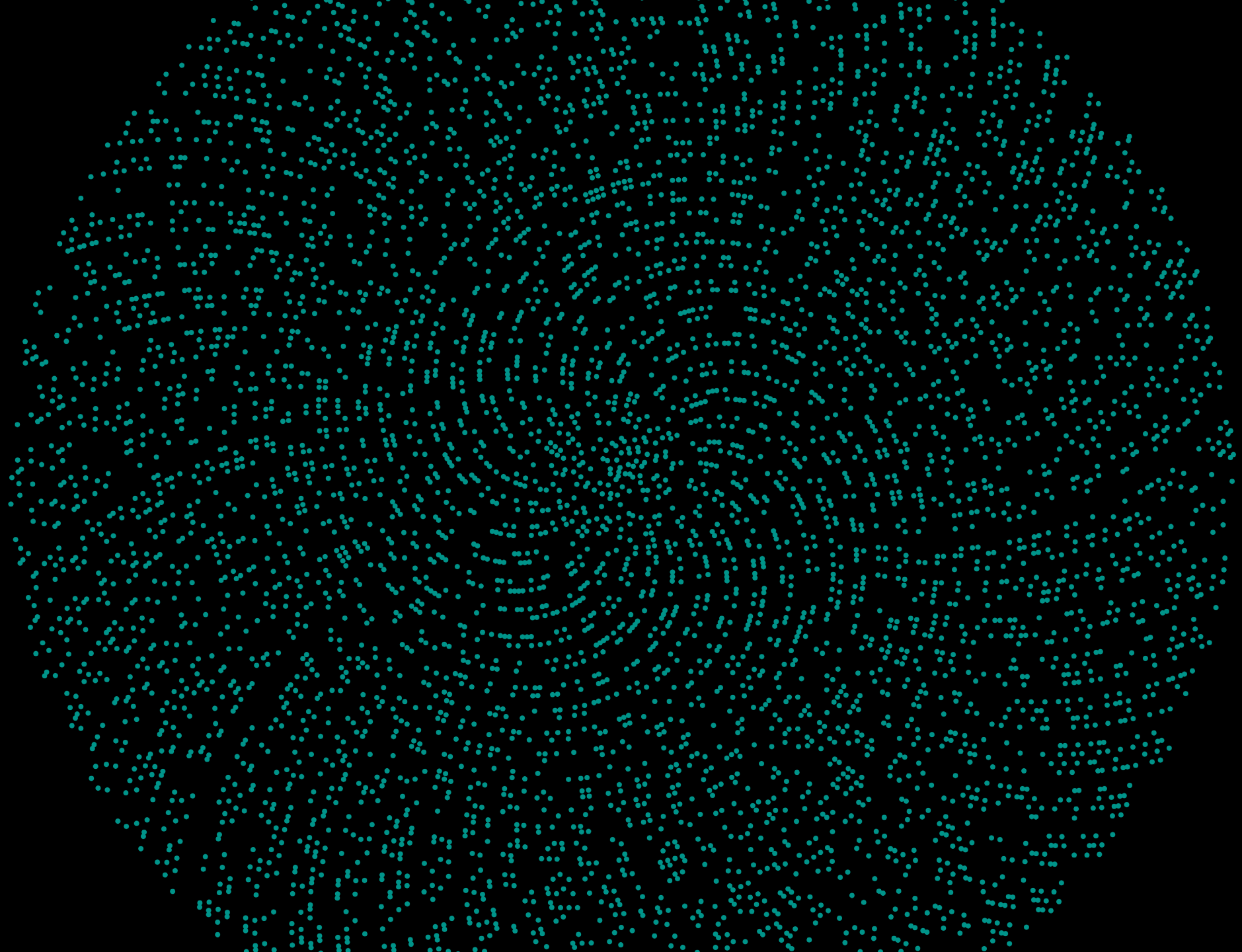
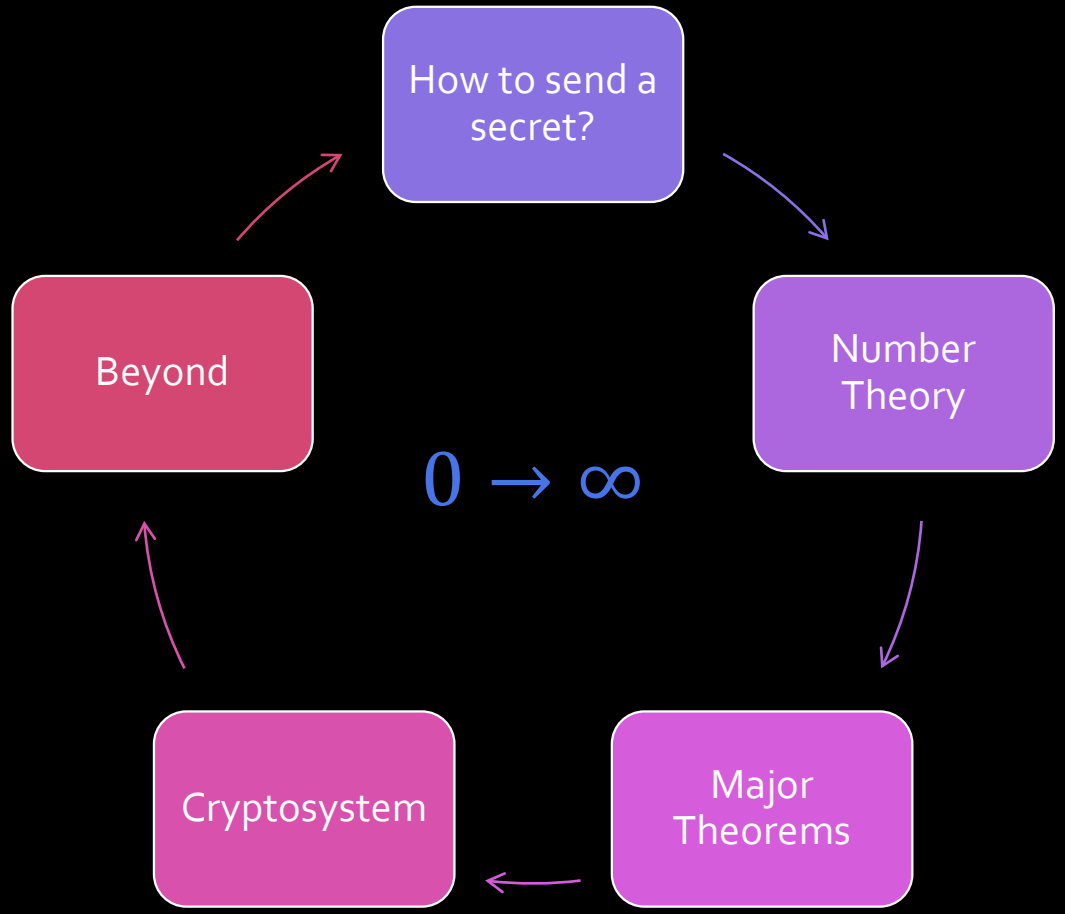
From Euler's Theorem to Elliptical Curves

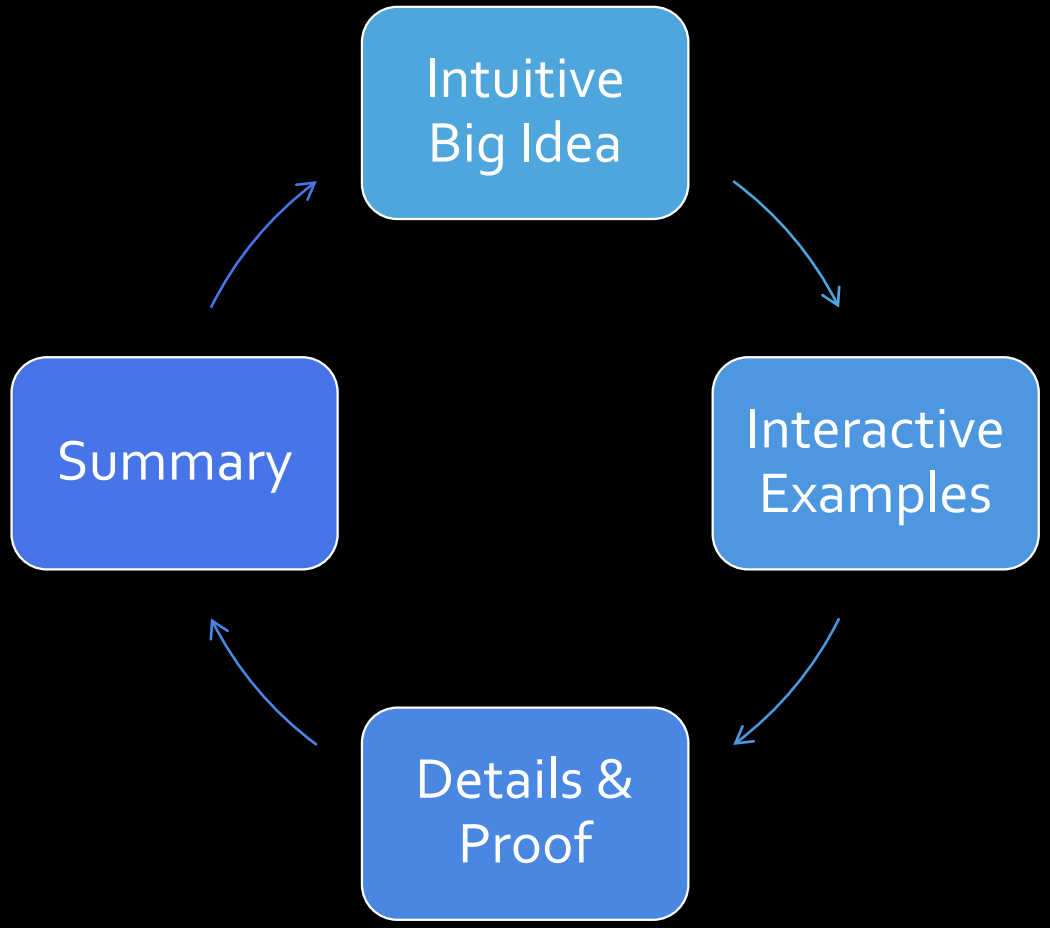
How to Hide Your Secrets with Number Theory



An Overview


How to send a secret?
Number Theory
Major Theorems
Cryptosystem
Beyond
$0 \to \infty$

What I wanna do



Sigma Terminal

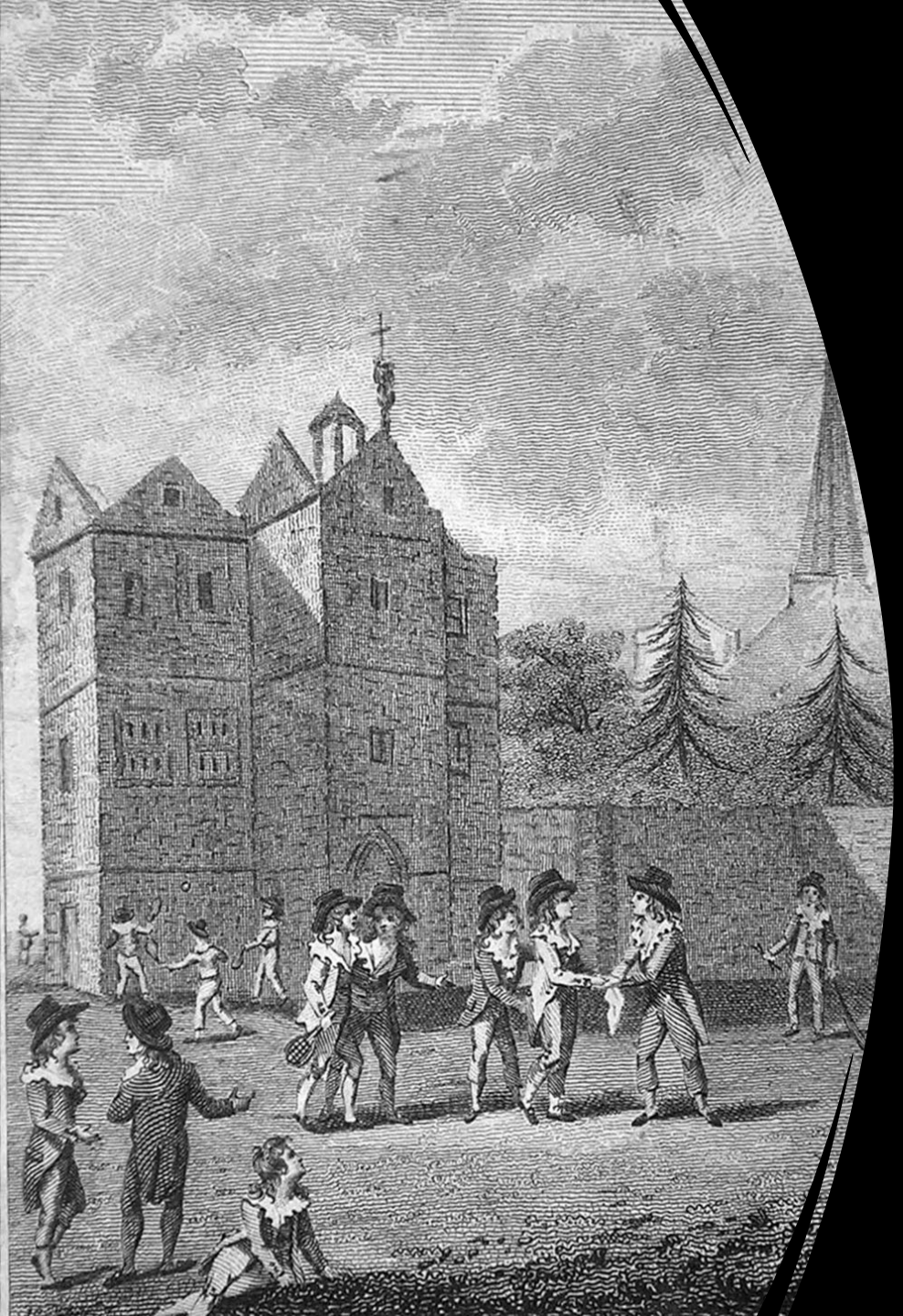
```
#Σ try me
```

https://sigma-terminal.glitch.me/

How do you hide secrets?

feat. King Alastair

Thought experiment



Suppose you're in the year 1572…

King Alastair needs to send a secret to King Byron

Both kings…

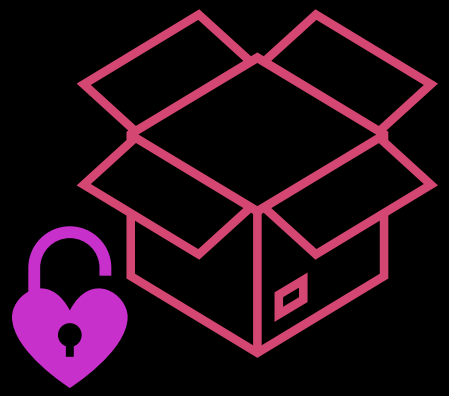
- can only send their secret via messengers
- have an unbreakable box, lock, and key
- have unforgable signatures

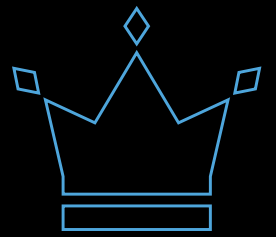
But the messengers are…

- all spies from King Churchill
- will read the secret whenever they can

How can you send a secret?

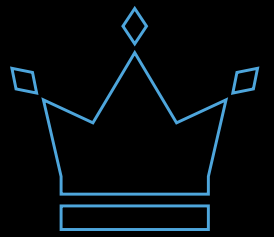
King Alastair



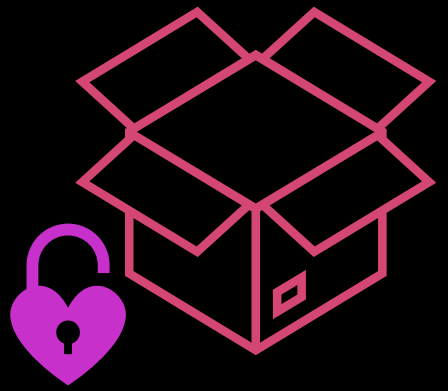


King Byron

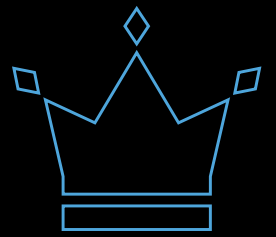
King Alastair



King Byron

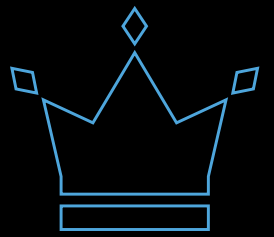


King Alastair



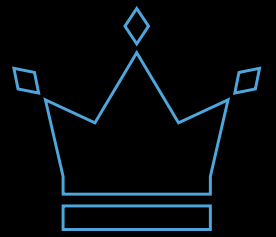
King Byron

King Alastair



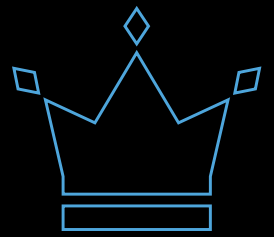
King Byron

King Alastair

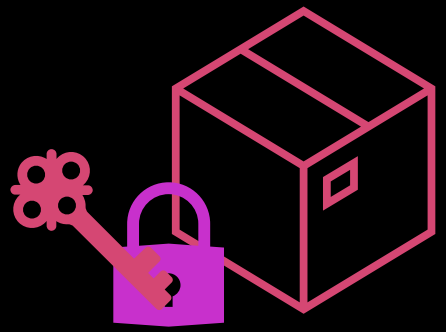


King Byron

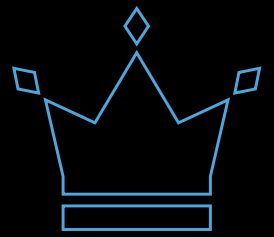
King Alastair



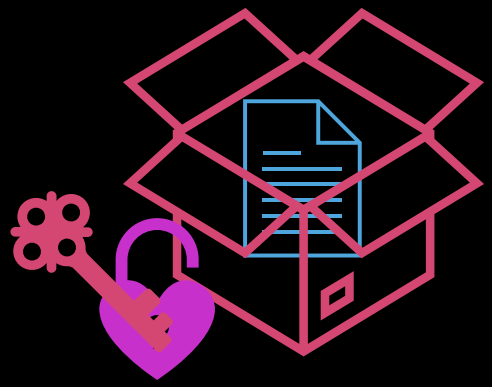
King Byron



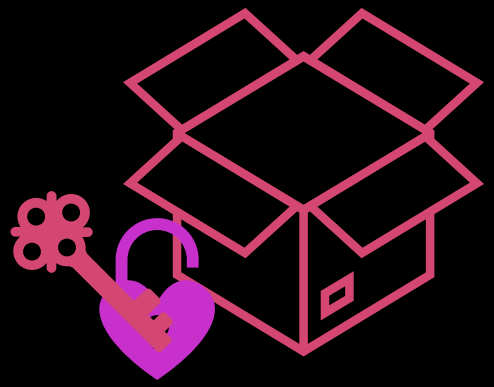
King Alastair

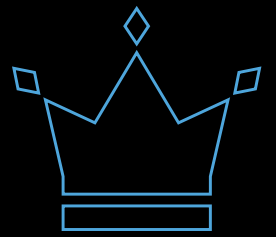


King Byron

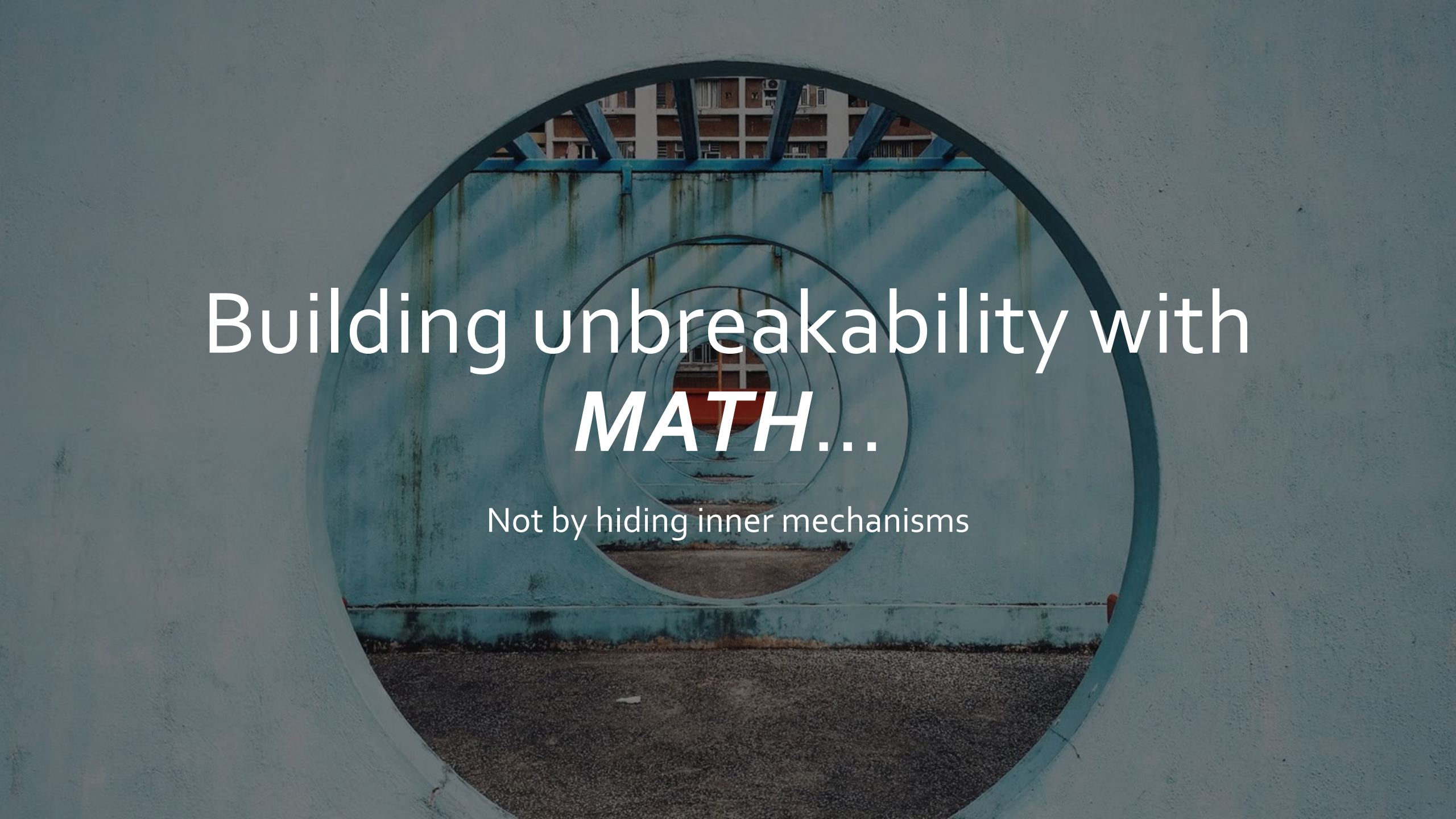


King Alastair





King Byron

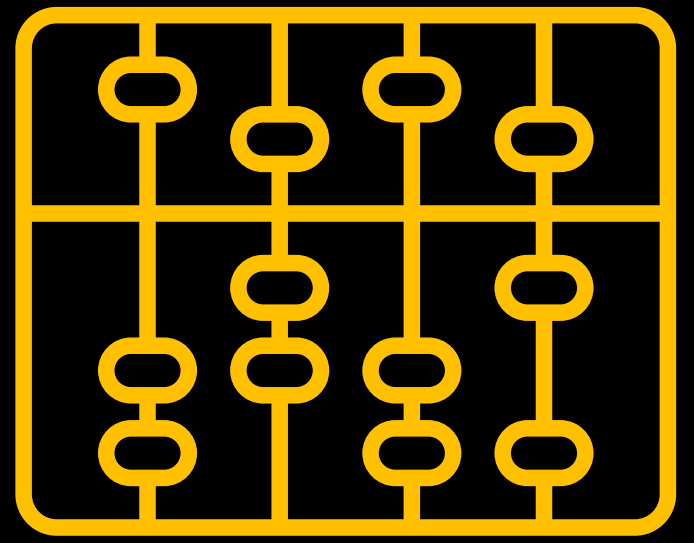


Building unbreakability with ***MATH***...

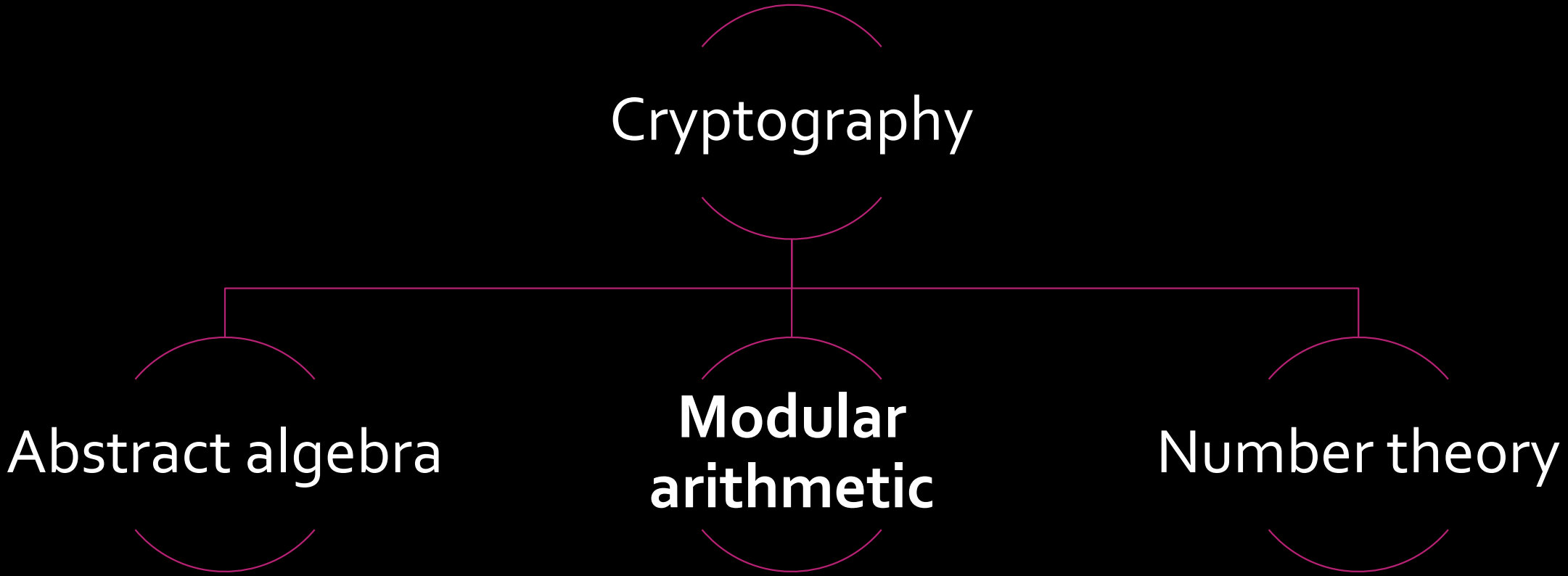
Not by hiding inner mechanisms

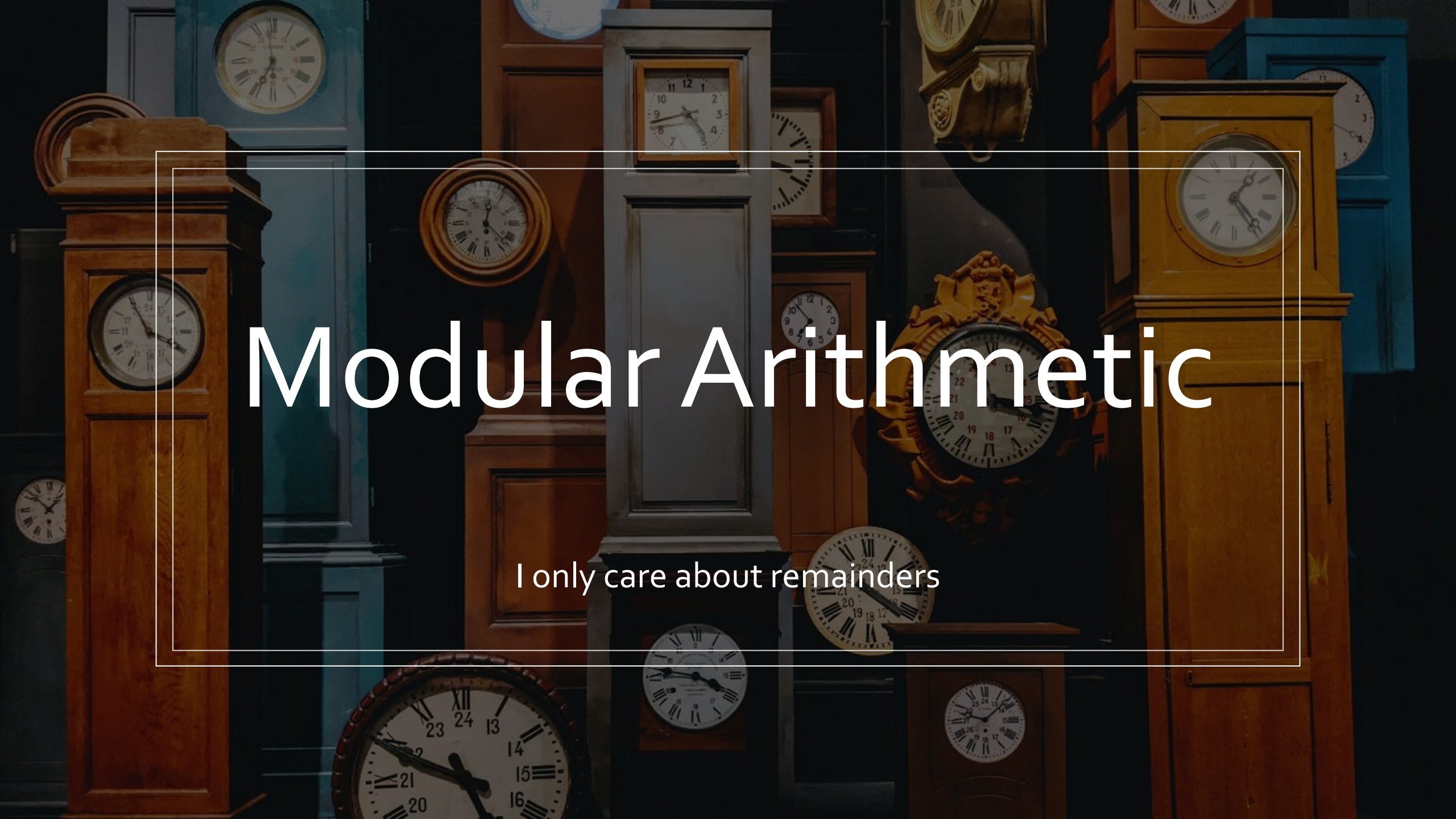
The Foundation of Cryptography

Number Theory



Math Time 😎


Cryptography
Abstract algebra
Modular arithmetic
Number theory



Modular Arithmetic

I only care about remainders

Modular Arithmetic

"$mod\ m$" means taking the remainder:

Math If $x = a \times m + r$ then $x \equiv r \ (mod\ m)$ (where $r < m$)

E.g. $17 = 5 \times \mathbf{3} + 2$ $\therefore 17 \equiv 2 \ (mod\ \mathbf{3})$

* When $a \equiv 0 \ (mod\ m)$, we say that "a is divisible by m", or "*m divides a*"

Greatest Common Divisor is the largest number that simultaneously divides two integers:

E.g. $GCD(10, 15) = 5$ $GCD(2, 4) = 2$ $GCD(42, 70) = 14$ **#Σ** `gcd(a,b)`

If a and b are coprime (or relatively prime), their *Greatest Common Divisor* is 1 :

E.g. $GCD(4, 9) = 1$ so 4 and 9 are coprime

The totient function $\phi(n)$ counts the number of integers that are coprime to n (from 1 to n):

E.g. $\phi(9) = 8$ because there are 8 integers coprime to 9: $\{1, 2, 4, 5, 7, 8\}$ **#Σ** `totient(n)`

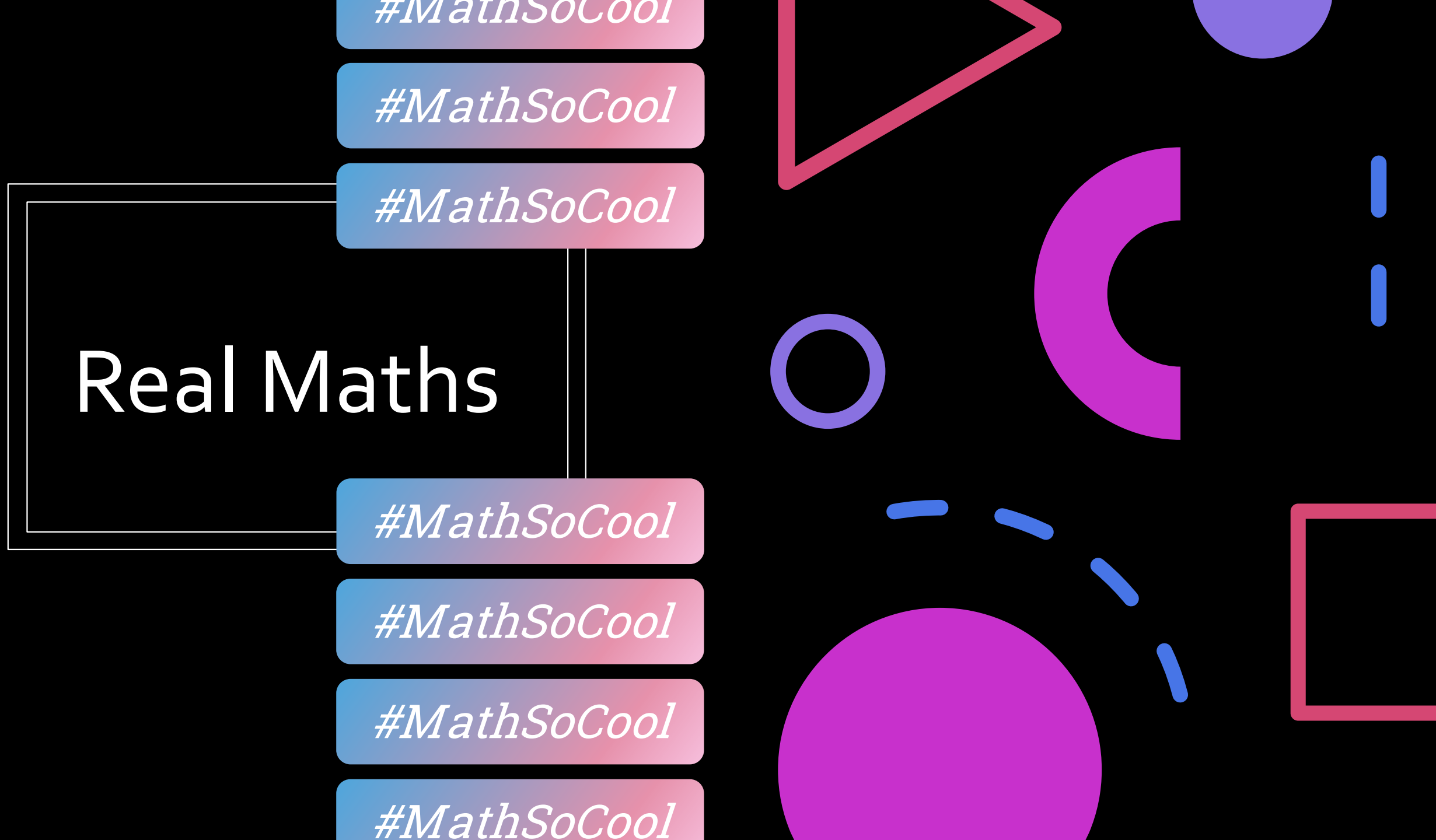
Inverses

#Σ inv(a,b)

- $\frac{1}{3}$ is the inverse of 3, because $\frac{1}{3} \times 3 = 1$ (the identity)
- What about in modular arithmetic?

$$2x \equiv 1 \ (mod\ 5)?$$

Must be coprime!


#MathSoCool
#MathSoCool
#MathSoCool
Real Maths
#MathSoCool
#MathSoCool
#MathSoCool
#MathSoCool

Fermat's Little Theorem

$$a^{p-1} \equiv 1 \pmod{p}$$

Let's prove it!

Euler's Theorem

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

for a and n that are coprime

Can you prove it?

Remainder Theorem

- Say I wanna find a number x
- $x \equiv 2\ (mod\ 3)$
- $x \equiv 1\ (mod\ 5)$
- What's x? Does it exist? Is it unique?
- Remainder theorem: Yes! It always exists, and is unique $mod\ 3 \times 5$!

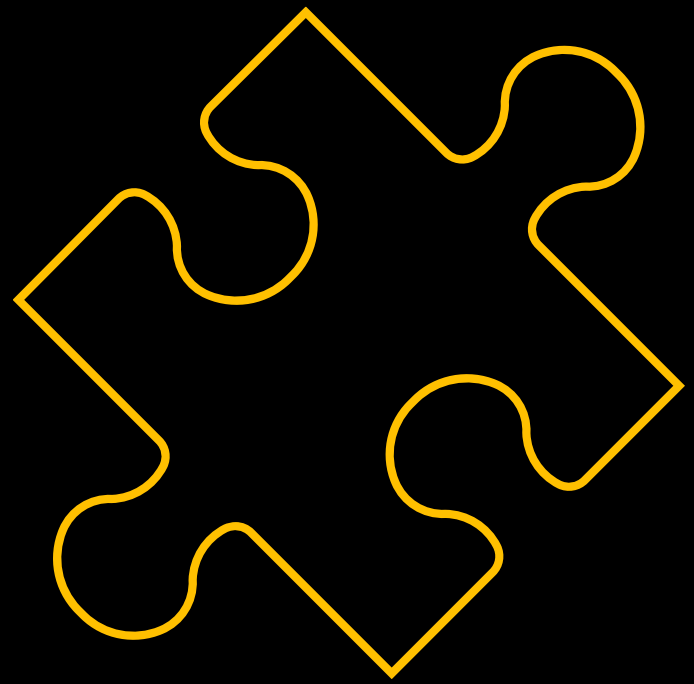
Chinese Remainder Theorem

Every system of congruences
over relatively prime moduli
have a unique solution
modulo the product of those moduli

Let's prove it!

Rivest–Shamir–Adleman, MIT is so cool

RSA Cryposystem





Ron Rivest | Adi Shamir | Leonard Adleman

1977


ExpressVPN


TLS

How does it work?

Factorise 97180163

#CRYPTO

#Σ

#CRYPTO

What next?

#Σ

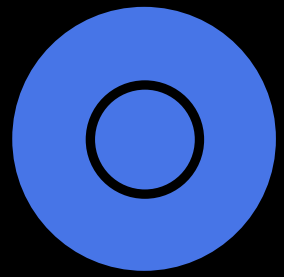
#CRYPTO

#Σ

Beyond RSA

RSA DIGITAL SIGNATURES

DIFFIE-HELLMAN KEY EXCHANGE



ZERO-KNOWLEDGE PROOFS

ELLIPTICAL CURVE CRYPTOSYSTEMS

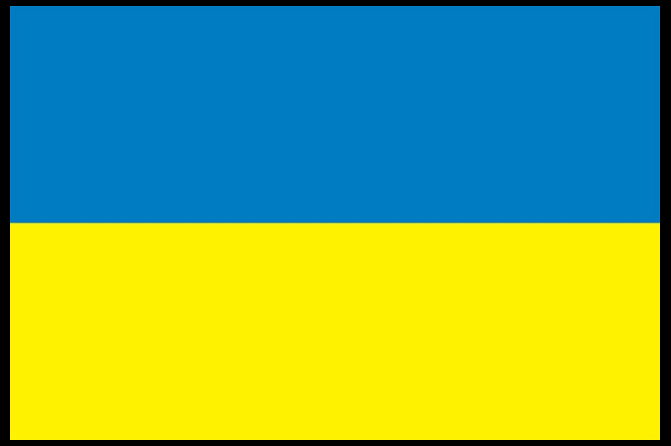
How do you hide secrets?

In the future?

Is it really… just about maths?

- Government agencies
- Technological leaps
- Bugs in implementation
- Irresponsible corporations
- Social engineering
- Cyber warfare

Just maths?

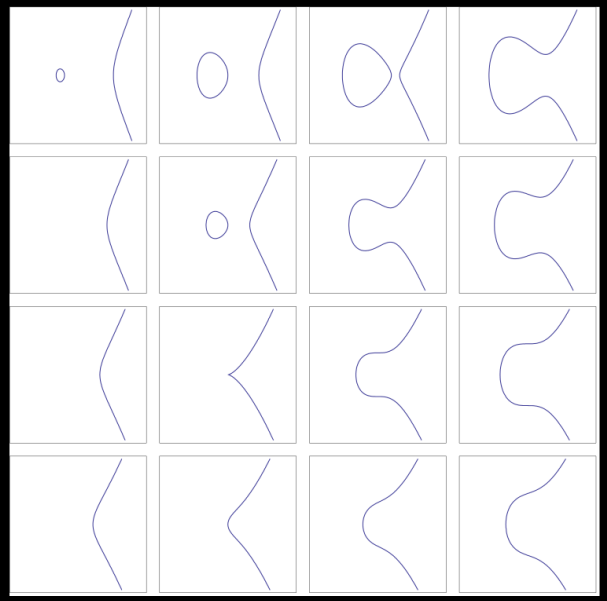


How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer

06/01/2014

Nick Sullivan

There has been a lot of news lately about nefarious-sounding backdoors being inserted into cryptographic standards and toolkits. One algorithm, a pseudo-random bit generator, Dual_EC_DRBG, was ratified by the National Institute of Standards and Technology (NIST) in 2007 and is attracting a lot of attention for having a potential backdoor. This is the algorithm into which the NSA allegedly inserted a backdoor and then paid RSA to use.



Jonathan Greig

April 23, 2022

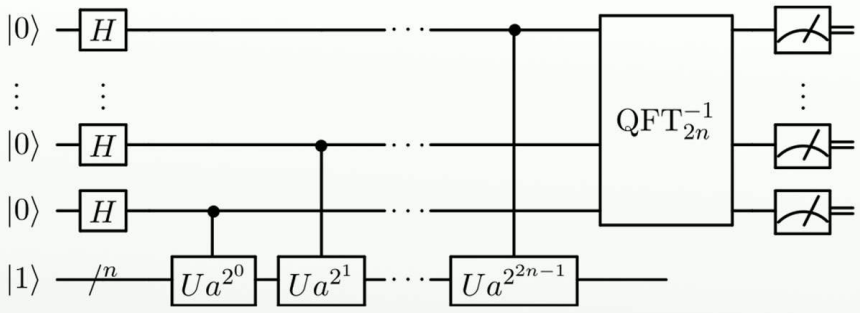
Briefs

Experts warn of need to patch critical cryptographic Java bug

Cybersecurity experts urged administrators to push through a patch for CVE-2022-21449 – a vulnerability affecting those using the Elliptic Curve Digital Signature Algorithm (ECDSA) signatures in Java 15, Java 16, Java 17, or Java 18.

This new Java vulnerability originates in an improper implementation of the ECDSA signature verification algorithm and essentially allows an attacker to potentially intercept communication and messages that should have otherwise been encrypted, such as SSL communication, authentication processes, and more. It has a CVSS of

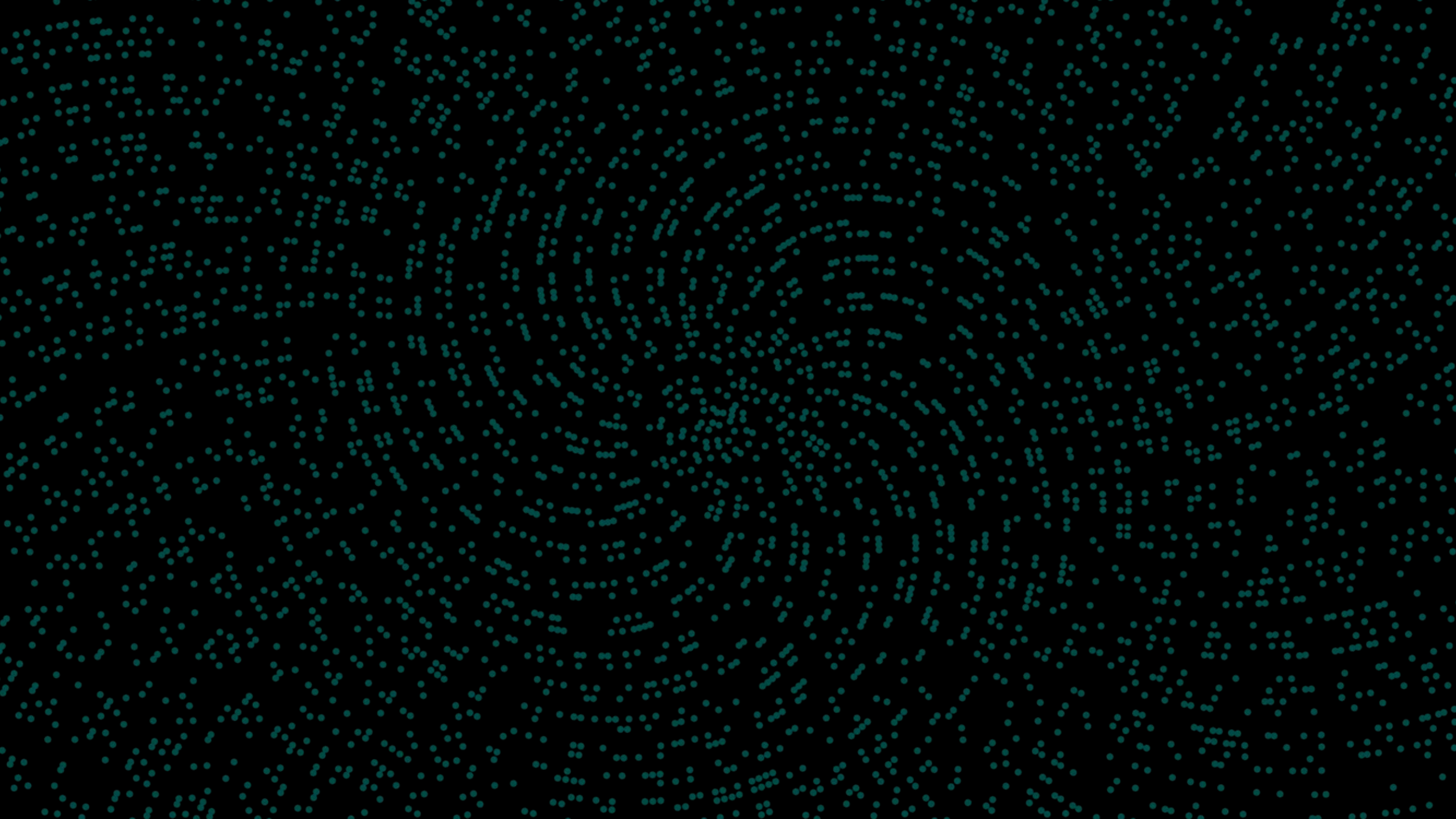
Shor's algorithm



https://en.wikipedia.org/wiki/File:Shor's_algorithm.svg

Math is clean, life is dirty

SKEPTICISM vs EFFICIENCY



THANK YOU