Why do we care about primes?

Primes!

- 2,3,5,7,11 ……………….,7841,…………………… ………….,136395369829,…. 222334565193649

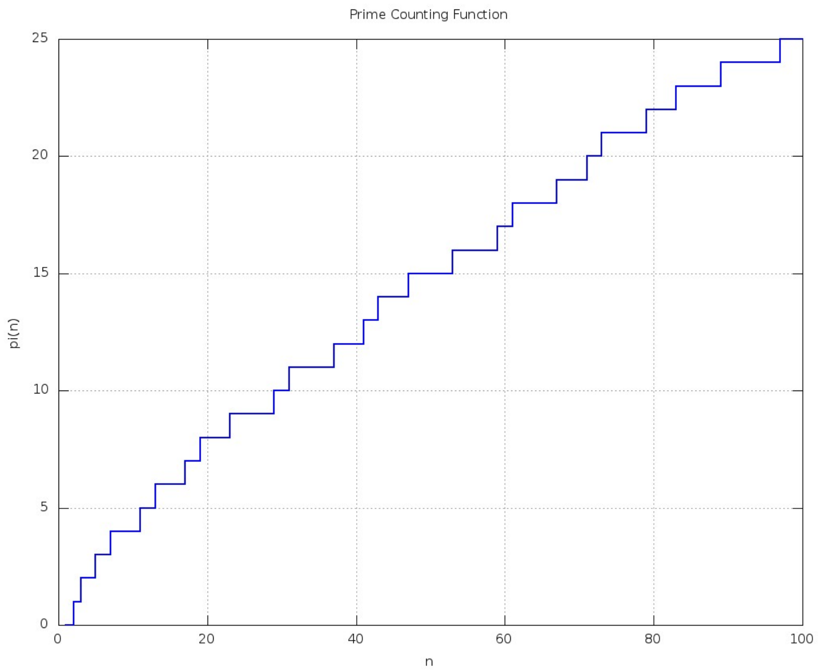
- The building block of the integers!
  - Fundamental Theorem of Arithmetic

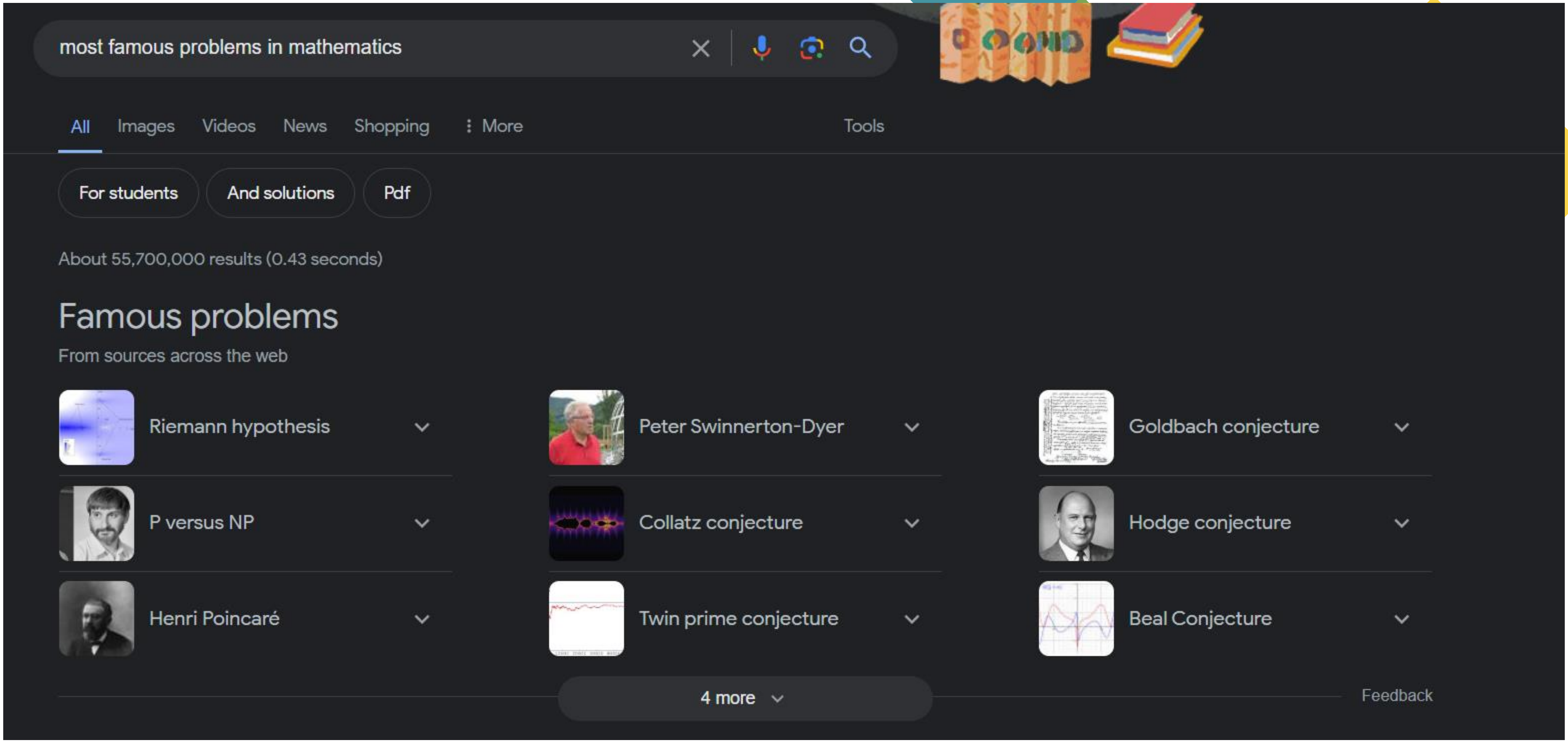
Quick Prime Facts

- There are infinitely many (Euclid)
- They become less common as numbers get larger
- Coprimes are numbers that share no common prime factors
- Determining a prime factorization can be difficult!
- You can win $150,000 if you discover a prime with over 100 million digits

A Quick History

- Euclid
    - A number which is measured by a unit alone
- Fermat
    - Little Theorem
- Gauss
    - Prime Number Theorem
- Riemann
    - Hypothesis




most famous problems in mathematics
All
Images
Videos
News
Shopping
More
Tools
For students
And solutions
Pdf
About 55,700,000 results (0.43 seconds)
Famous problems
From sources across the web
Riemann hypothesis
Peter Swinnerton-Dyer
Goldbach conjecture
P versus NP
Collatz conjecture
Hodge conjecture
Henri Poincaré
Twin prime conjecture
Beal Conjecture
4 more
Feedback

Prime Patterns

- Goldbach Conjecture
- Twin Prime Conjecture
- Riemann Hypothesis

- We want a way to generate primes!

Applications

- 1. Cryptography
- 2. Connections!

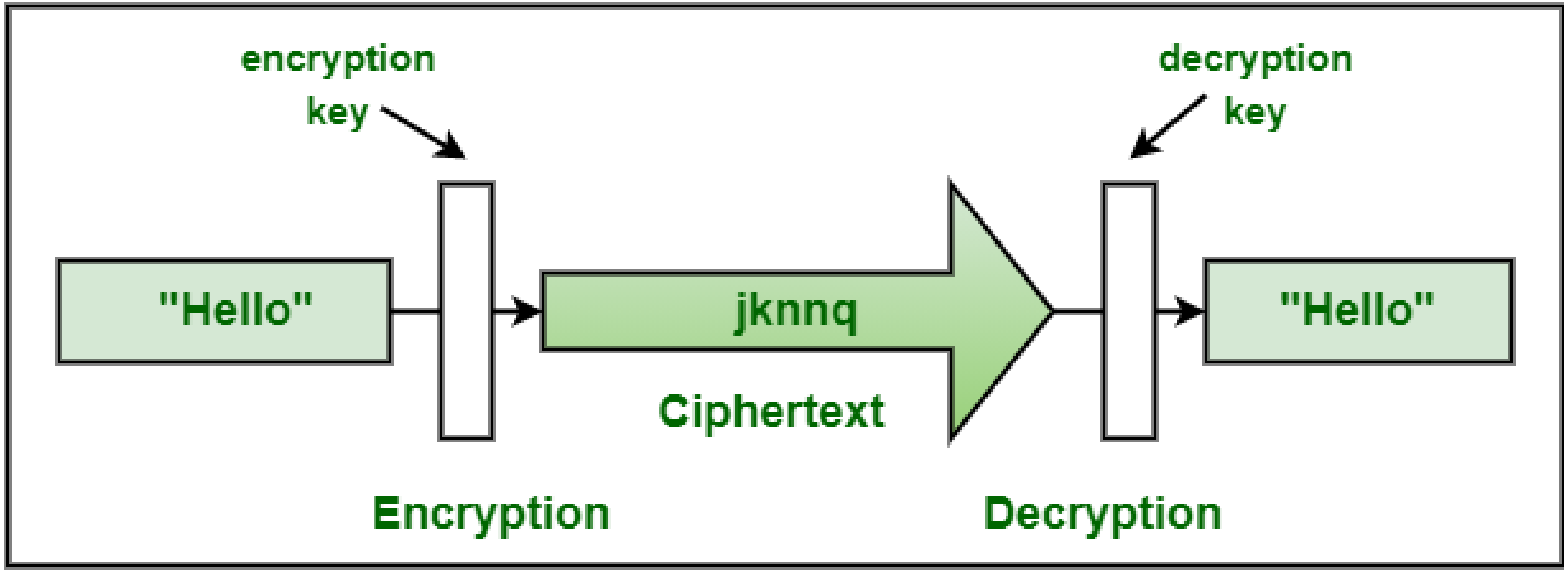
Cryptography

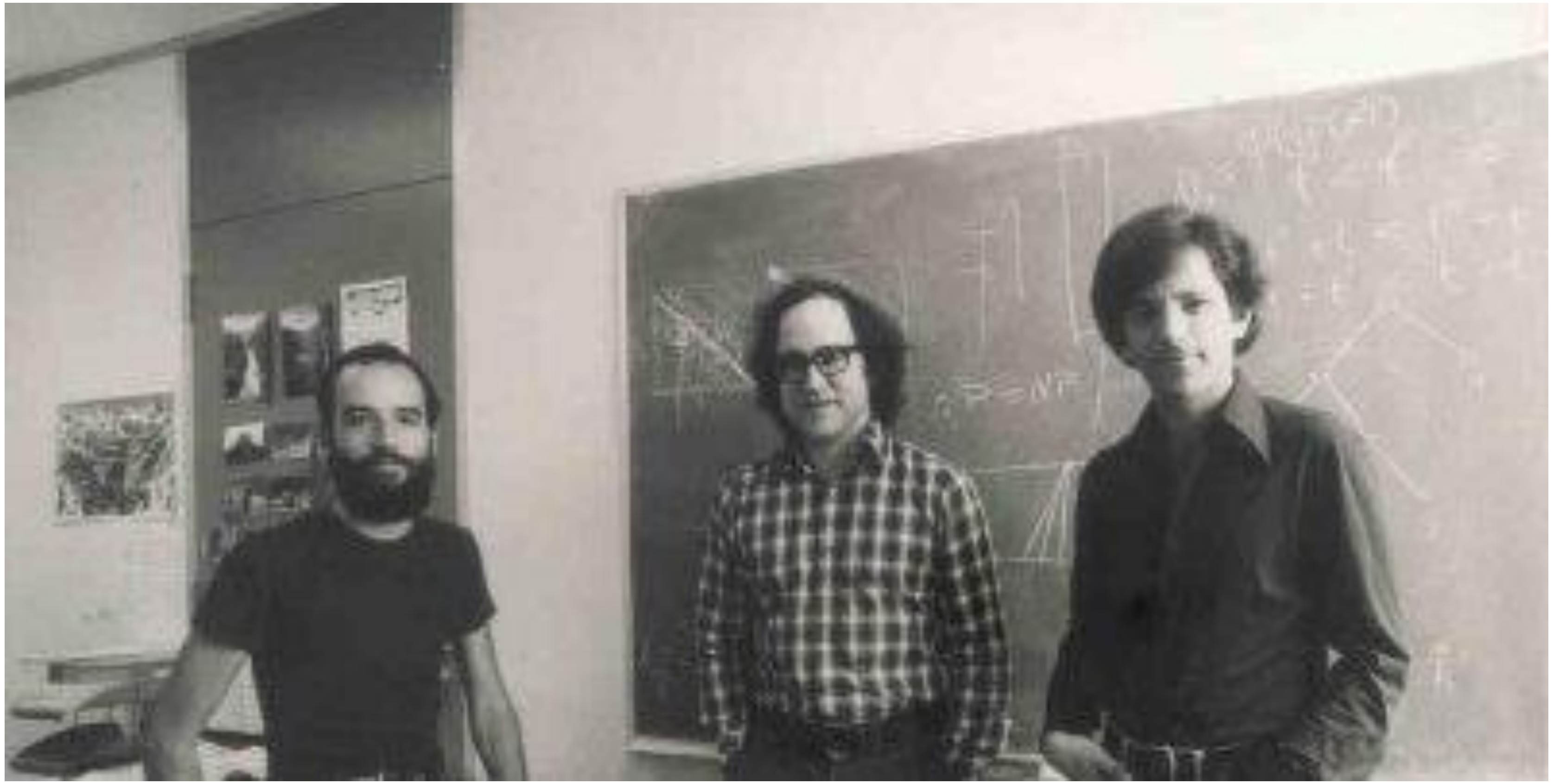
"The art of writing or solving codes"

Cybersecurity 101

- Pretty much everything you do on the internet is encrypted
- There are different algorithms to encrypt the data you transmit and receive
- Without encryption, anyone on your network can see your personal:
  - Messages
  - Passwords

Cryptography 101





RSA (Ron Rivest, Adi Shamir, Leonard Adleman)

RSA: Creating a Key Pair

- p, q are prime
- $n = pq$
- e: a number chosen to be coprime to $(p-1)(q-1)$
- (e, n) is our public key
- Find d such that $de \equiv 1 \; mod((p-1)(q-1))$
- (d, p, q) is our private key

RSA: Encryption

- p, q are prime
- $n = pq$
- e: a number chosen to be coprime to (p-1)(q-1)
- m: message to encrypt
- $c = m^e \, mod(n)$

RSA: Decryption

- p, q are prime
- $de \equiv 1\ mod((p-1)(q-1))$
- c: cipertext
- $m = c^d\ mod(n)$

RSA: Example

- $p = 7, q = 11$

RSA: Example

- $p = 7, q = 11$
- $n = 77$
- $(p-1)(q-1) = 6(10) = 60$
- Say $e = 7$
- Public Key: (7,77)
- $7d \ = \ 1\, mod(60)$
- $d \ = \ 43$
- Private Key: (43,7,11)

RSA: Proof it works

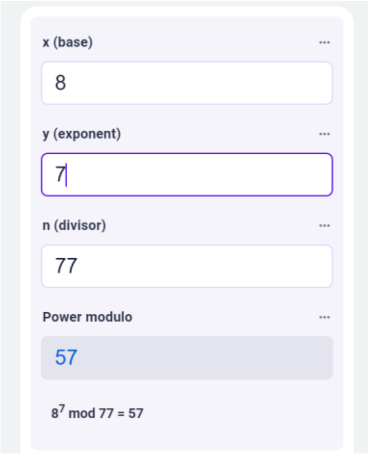
- $m = 8$

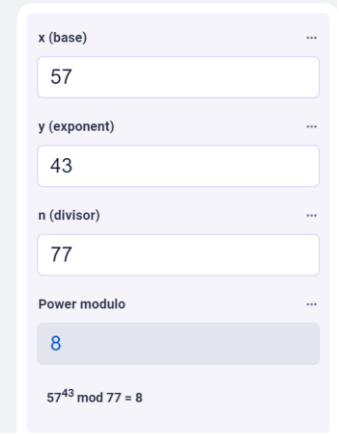
Encrypt, Public Key: (3,77)

- $8^7 \bmod(77) = 57$

Decrypt, Private Key: (43, 7, 11)

- $57^{43} \bmod(77) = 8$





RSA: Why does it work (Abstract Alg!)

- p, q are prime
- $n = pq$
- e: a number chosen to be coprime to $(p-1)(q-1)$
- Find d such that $de \equiv 1 \, mod((p-1)(q-1))$

Q: Why does d always exist?

A: Unit Groups!

RSA: Why does it work

- p, q are prime
- $n = pq$
- e: a number chosen to be coprime to $(p-1)(q-1)$
- Find d such that $de \equiv 1 \; mod((p-1)(q-1))$

- Claim: For integers m and c with $c = m^e \; mod(n)$,

  we have $m^{ed} \equiv c^d \equiv m \; mod(n)$

Claim: For integers m and c with $c = m^e \ mod(n)$, we have $m^{ed} \equiv c^d \equiv m \ mod(n)$

RSA: Why does it work

- p, q are prime
- $n = pq$
- e: a number chosen to be coprime to $(p-1)(q-1)$
- Find d such that $de \equiv 1 \ mod((p-1)(q-1))$

$de = 1 + k((p-1)(q-1))$ for some integer k

$$
\begin{aligned}
m^{ed} &= m^{1+k((p-1)(q-1))} \\
&= m * (m^{(p-1)})^{k(q-1)} \\
&\equiv m * (1)^{k(q-1)} \ mod(p) \\
&\equiv m \ mod(p)
\end{aligned}
$$

Similarly: $m^{ed} \equiv m \ mod(q)$

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

Claim: For integers m and c with $c = m^e \ mod(n)$, we have $m^{ed} \equiv c^d \equiv m \ mod(n)$

RSA: Why does it work

- p, q are prime
- $n = pq$
- e: a number chosen to be coprime to $(p-1)(q-1)$
- Find d such that $de \equiv 1 \ mod((p-1)(q-1))$

$$m^{ed} \equiv m \ mod(p)$$
$$m^{ed} \equiv m \ mod(q)$$

We also know:

$$m \equiv m \ mod(p)$$

$$m \equiv m \ mod(q)$$

So by the Chinese Remainder Theorem:

$$m^{ed} \equiv m \ mod(pq)$$

Which implies: $c^d \equiv m \ mod(n)$

Theorem: Let p, q be coprime. Then the system of equations

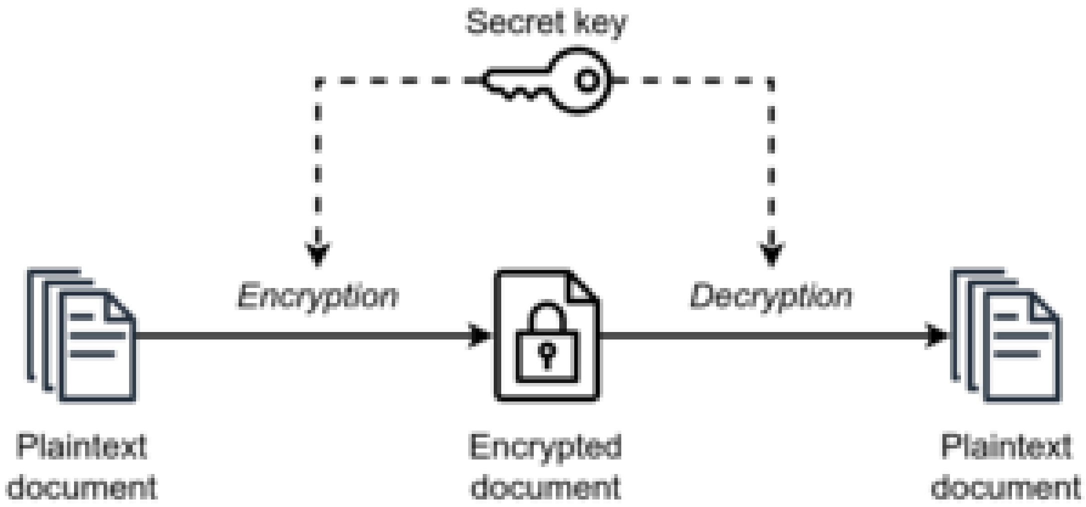
$$x = a \pmod{p}$$

$$x = b \pmod{q}$$

has a unique solution for x modulo pq.

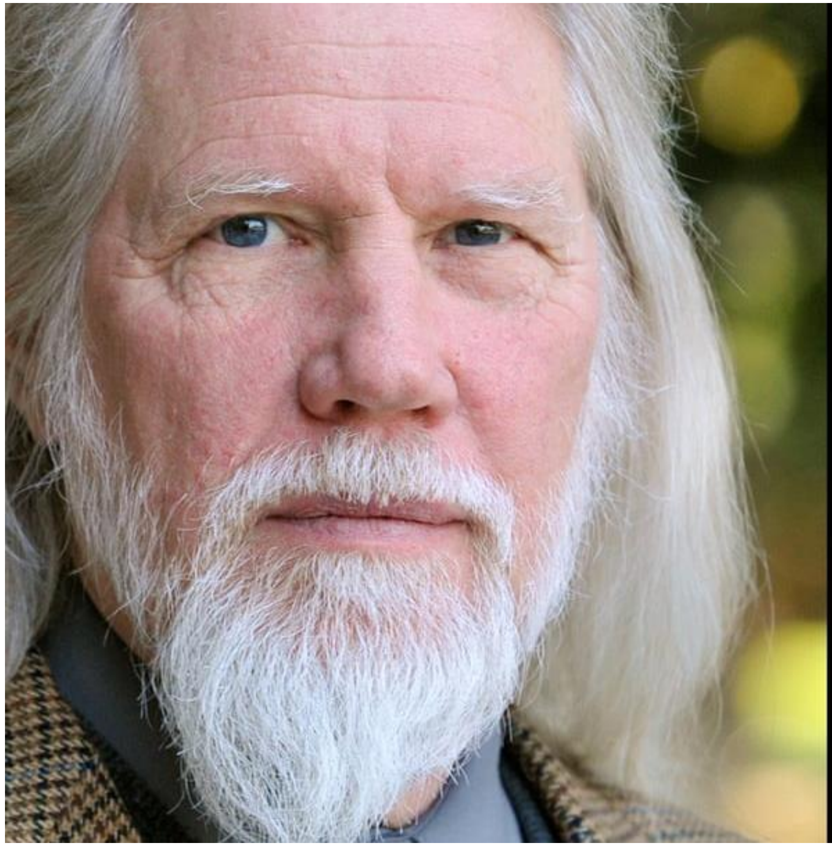
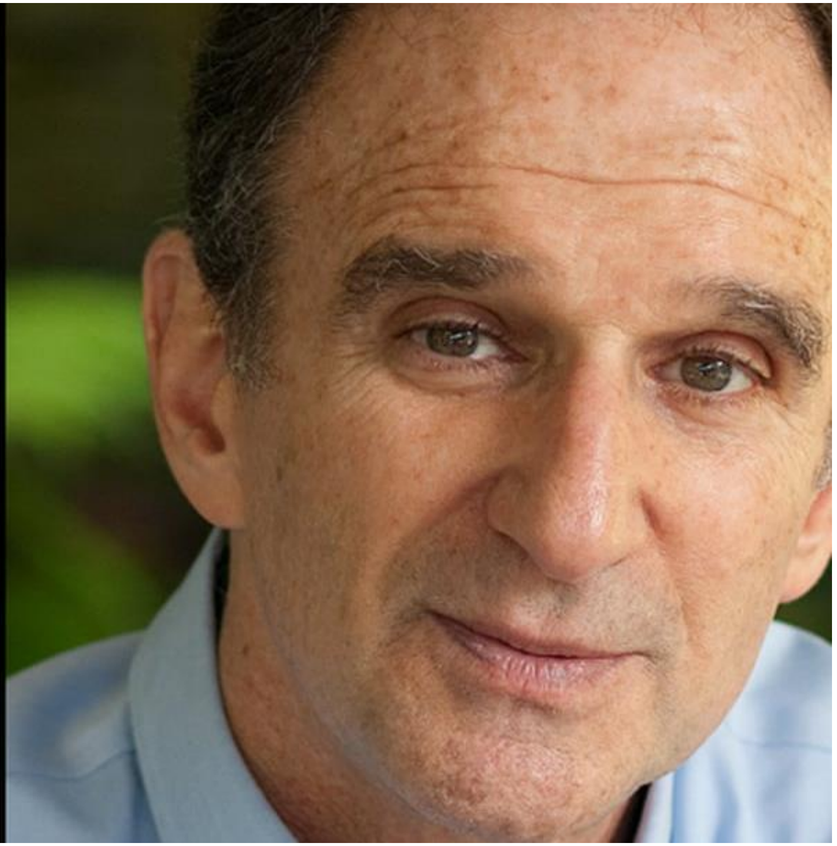
Symmetric Cryptography

- The same key is used for encryption and decryption
- Used to encrypt/decrypt larger pieces of information



Symmetric Cryptography

- How are both parties able to agree upon a key?

Diffie-Hellman

DH: The Algorithm

- Two participants (Alice and Bob) want to share a key
- They mutually decide upon a two numbers, a relatively small integer g and a large prime n
- Alice chooses an integer between 1 and n (private), say a
- Bob chooses an integer between 1 and n (private), say b
- Alice computes $g^a \ mod(n)$ and sends the result to Bob
- Bob computes $g^b \ mod(n)$ and sends the result to Alice
- Using the information they provide each other, Alice computes $(g^b)^a \ mod(n)$ and Bob computes $(g^a)^b \ mod(n)$
- $g^{ab} \ mod(n)$ is their secret key

DH: Discrete Logarithm Problem

- G is a multiplicative cyclic group and g is a generator of G, then from the definition of cyclic groups, we know every element h in G can be written as g^x for some x.
- The discrete logarithm to the base g of h in the group G is defined to be x
- We NEED n to be prime otherwise the group would not be cyclic and that would limit the number of options the key could be
- Safe primes: In the form 2q + 1
  - Avoids the Pohlig–Hellman Algorithm

Connections!

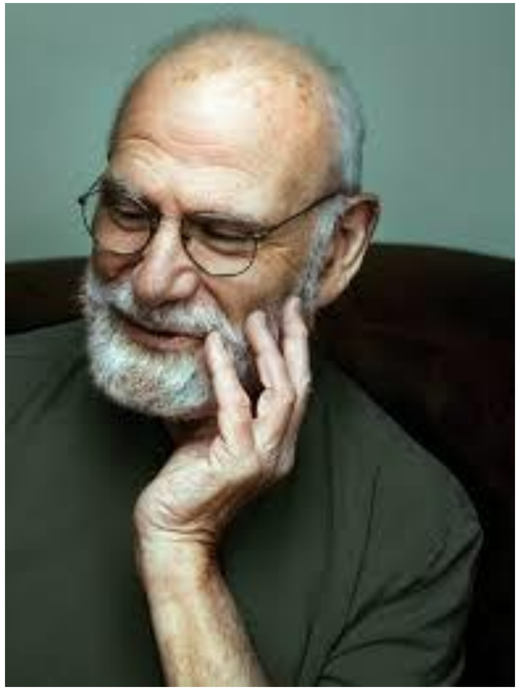
Nature

A cicada that emerges every 12 years will synchronize with all predators having a life cycle of 2, 3, 4, 6 or 12 years, whereas emerging every 13 years reduces that chance.

Math Brains?

“authors described the performance of Michael, a young man with ASD, who could factorize prime numbers greater than 10,000 with a 70% accuracy (compared to a mathematically trained control subject who scored only 40% accuracy and slower response times)”

- *https://biologydirect.biomedcentral.com/articles/10.1186/s13062-022-00326-w*
- *The Man Who Mistook His Wife for a Hat*
    - *Oliver Sacks*



Magic Squares

The smallest magic square composed of consecutive odd primes *including the number 1* is of order 12

1	823	821	809	811	797	19	29	313	31	23	37
89	83	211	79	641	631	619	709	617	53	43	739
97	227	103	107	193	557	719	727	607	139	757	281
223	653	499	197	109	113	563	479	173	761	587	157
367	379	521	383	241	467	257	263	269	167	601	599
349	359	353	647	389	331	317	311	409	307	293	449
503	523	233	337	547	397	421	17	401	271	431	433
229	491	373	487	461	251	443	463	137	439	457	283
509	199	73	541	347	191	181	569	577	571	163	593
661	101	643	239	691	701	127	131	179	613	277	151
659	673	677	683	71	67	61	47	59	743	733	41
827	3	7	5	13	11	787	769	773	419	149	751

Fractals

- https://www.youtube.com/watch?v=VZSjRgQhvSM