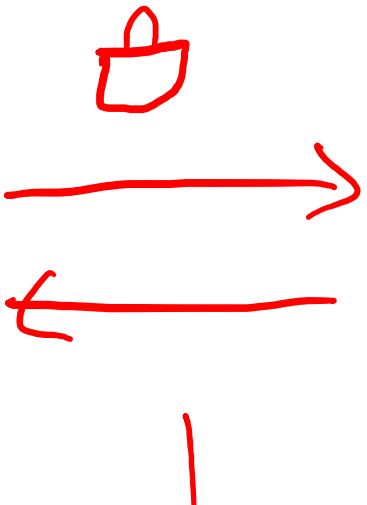
Hybrid crypto interactive Lecture 12b: 2022-04-06

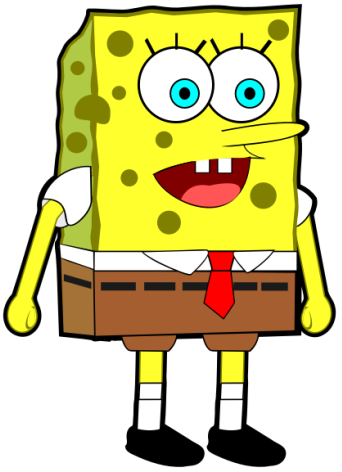
MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

A Communications Story

(A)lice from Alice's Adventures in Wonderland
Illustration by Arthur Rackham, 1907





Sponge(B)ob Squarepants
https://freesvg.org/sponge-bob-squarepant

(E)ve by Lucas Cranach the Elder (1528)

Eavesdropper

Symmetric vs asymmetric crypto

Symmetric encryption

- Uses same key for encryption and decryption.
- Fast, but doesn't work if Eve is able to intercept the key.
- Examples: Caesar cipher, Vigenère cipher, AES/Rijndael (2001)

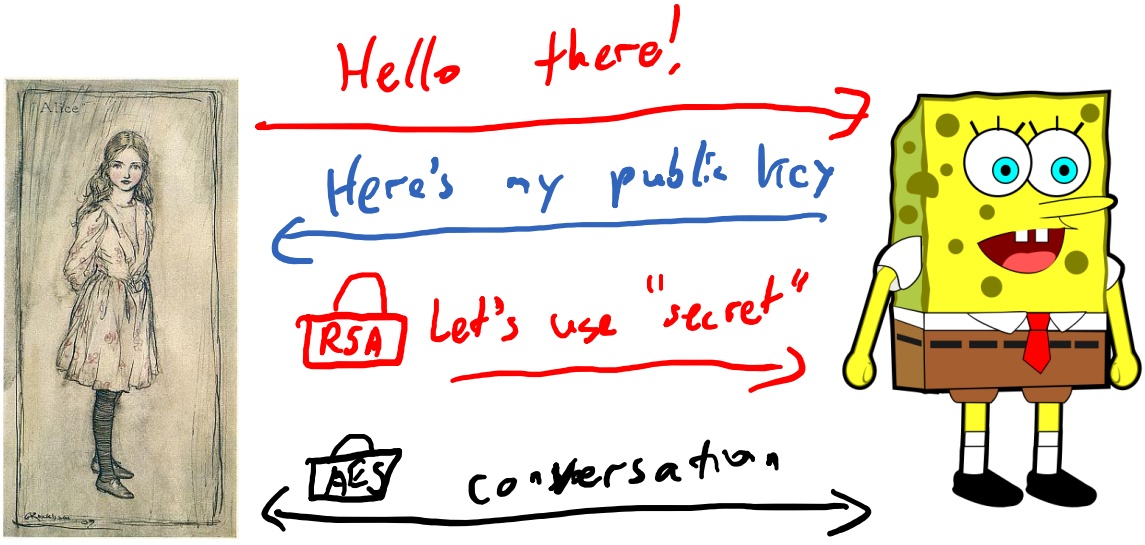
Asymmetric encryption

- A.k.a. public-key crypto
- Knowing how to encrypt doesn't tell you how to decrypt.
- Slow, because lots of math, but able to secure communications even if Eve hears everything.
- Examples: RSA, ElGamal

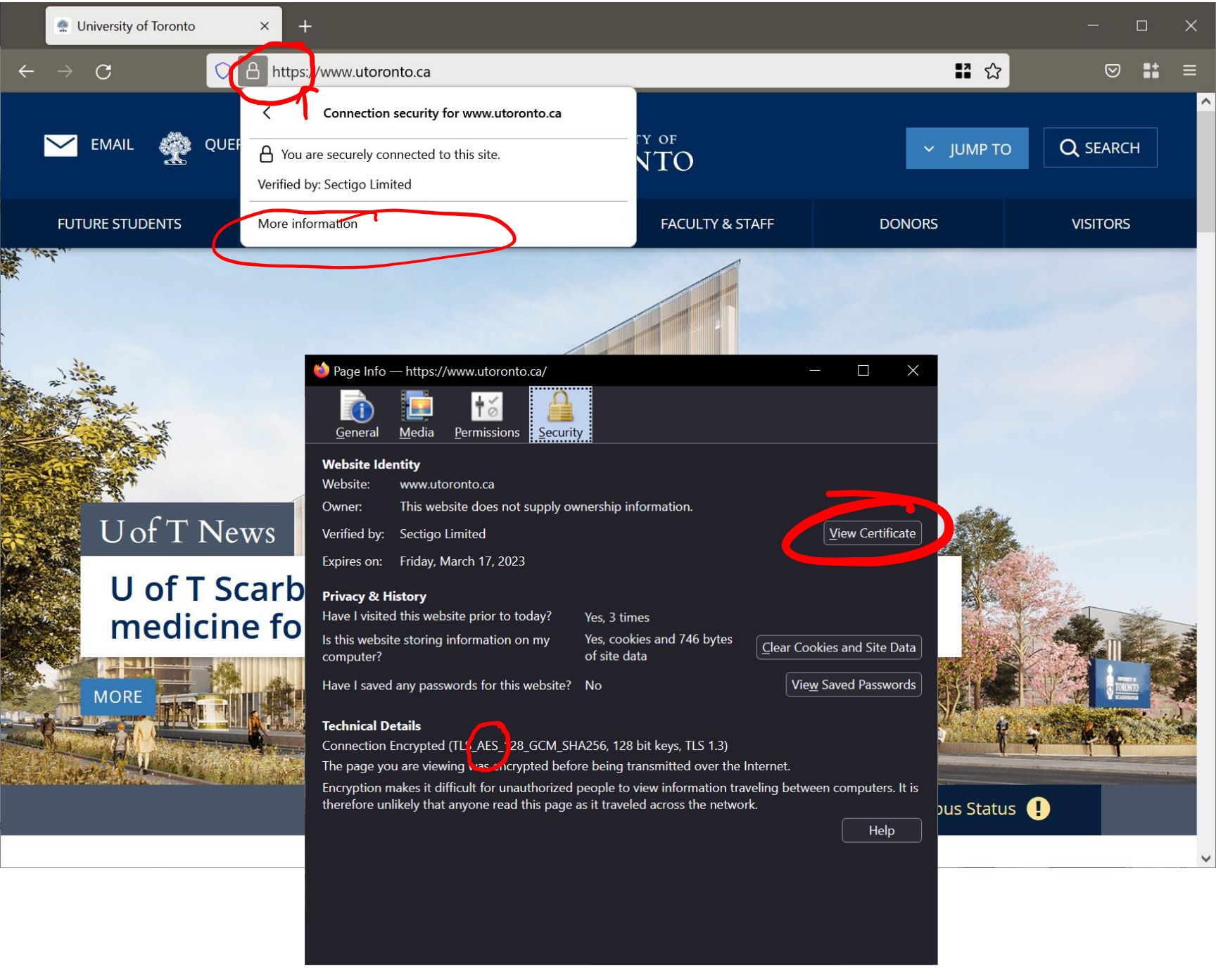
Hybrid cryptosystems

- We can get the best of both worlds by combining the two.
- Use the slow public-key cryptography (e.g. RSA) to exchange a small message containing a key for the symmetric method.
- Then use the fast symmetric encryption method (e.g. AES) for everything else.

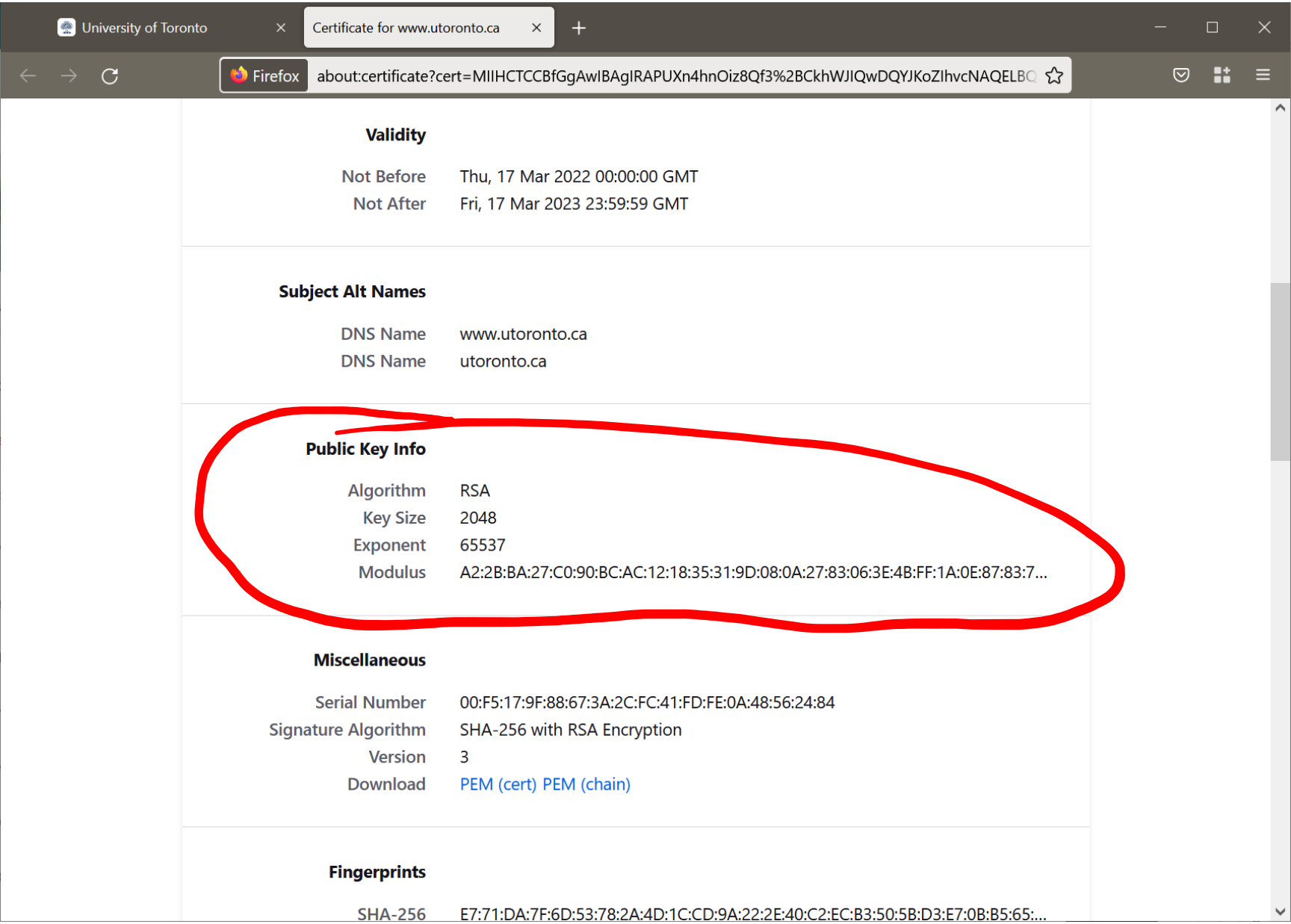
Old El Paso advertisement; Mia Agraviador pictured



Real-life example

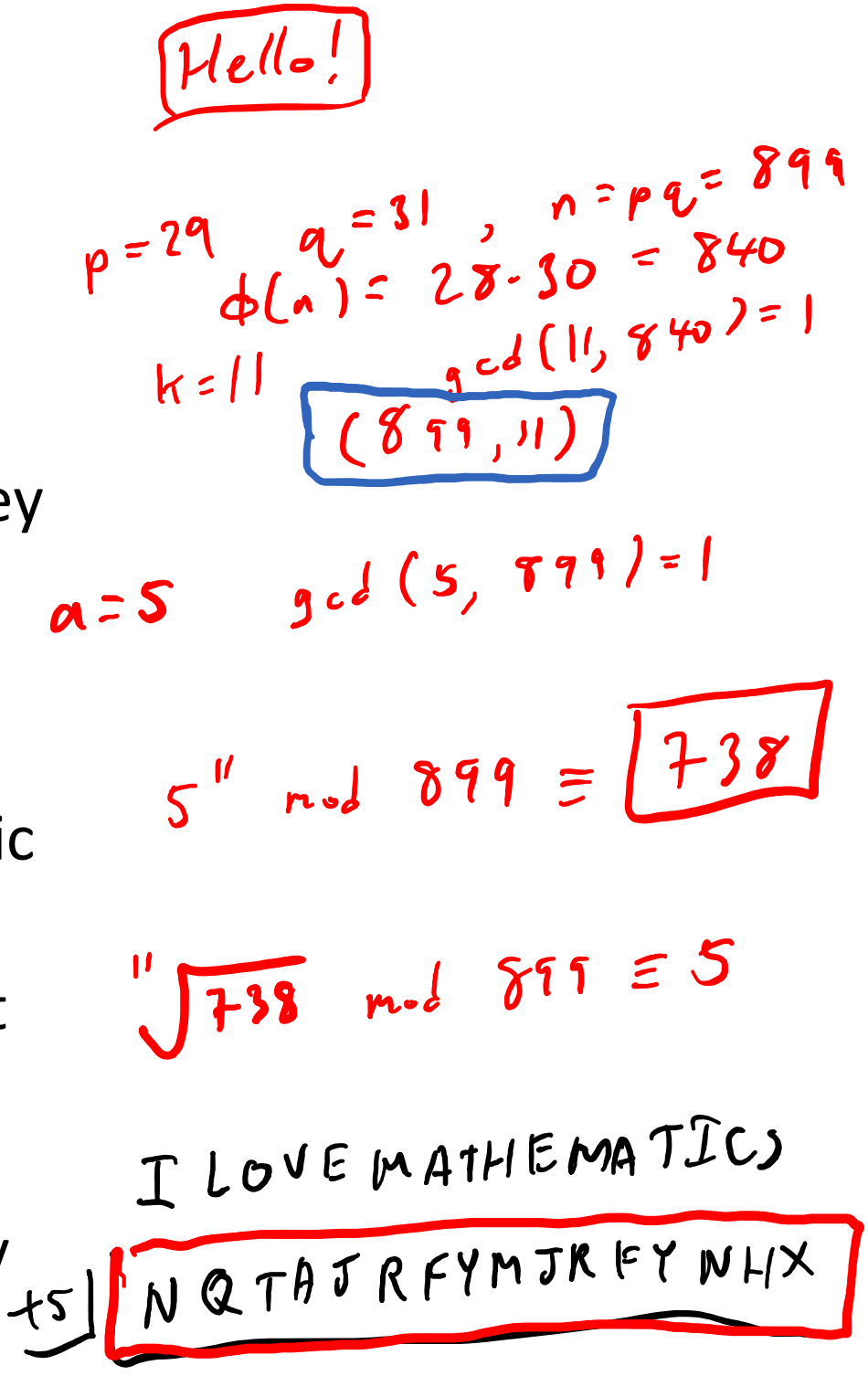


Real-life example



Toy example

- Alice: Hello there!
- Bob: generate RSA modulus/exponent
- Bob: sends public key
- Alice: choose symmetric key
- Alice: send RSA-encrypted symmetric key to Bob
- Bob: decrypts to get symmetric key
- Both: communicate using symmetric key and cipher.



Interactive exercise (groups of 3-5)

Part 1:

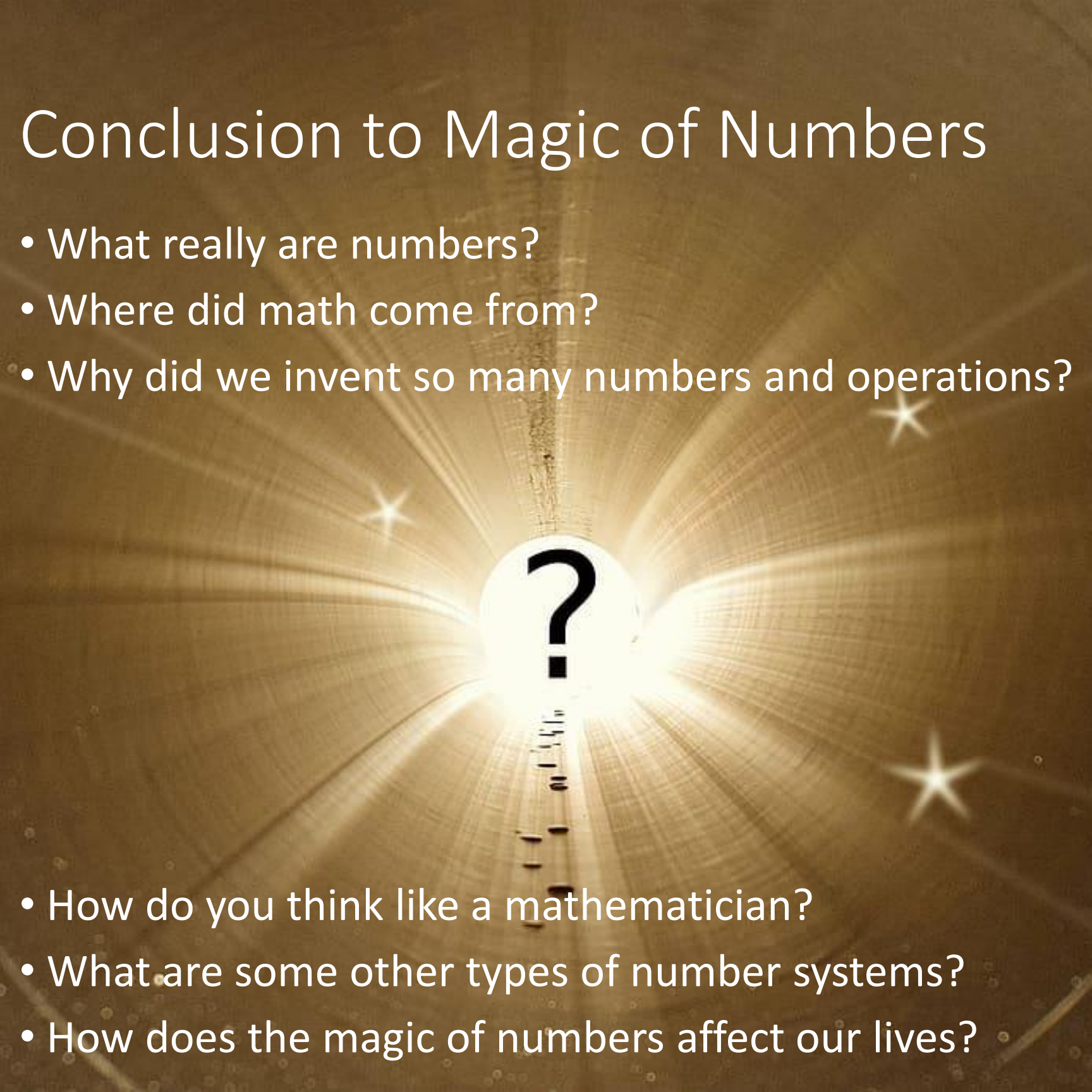
- Generate an RSA modulus n using 2-digit primes.
- Choose an exponent k such that $\gcd\big(k, \phi(n)\big) = 1$
- Choose a Caesar cipher key $a > 1$ with $\gcd(a, n) = 1$
- Encrypt the Caesar cipher key by $b \equiv a^k \pmod{n}$
- Write a short message of 15-30 characters.
- Encrypt the message using the Caesar cipher key a.
- Publish the message (n, k, b) and encrypted msg!

Part 2:

- Decrypt other groups messages.
- First compute $a \equiv \sqrt[k]{b} \pmod{n}$
- Then use Caesar cipher key to decrypt the message.

Conclusion to Magic of Numbers

- What really are numbers?
- Where did math come from?
- Why did we invent so many numbers and operations?



- How do you think like a mathematician?
- What are some other types of number systems?
- How does the magic of numbers affect our lives?