Introduction to Cryptography

Daniel Mancia

University of Texas at Austin

September 27, 2019

Table of Contents

Table of Contents

What is Cryptography?

What is Cryptography?

Figure 1: "Crypto"

What is Cryptography?

- The practice and study of techniques for secure communication in the presence of third parties called adversaries.

What is Cryptography?

- The practice and study of techniques for secure communication in the presence of third parties called adversaries.
- Why do we need cryptography?

Vocabulary

- **Plaintext:** Text that is plain.
- **Encryption:** Process of encoding plaintext data such that only the intended recipient can read it.
- **Ciphertext:** The result of encryption. Unreadable garbage.
- **Decryption:** The inverse of encryption. Given a ciphertext we decode it to get back the plaintext.
- **Key:** Secret piece of information that customizes the encryption.

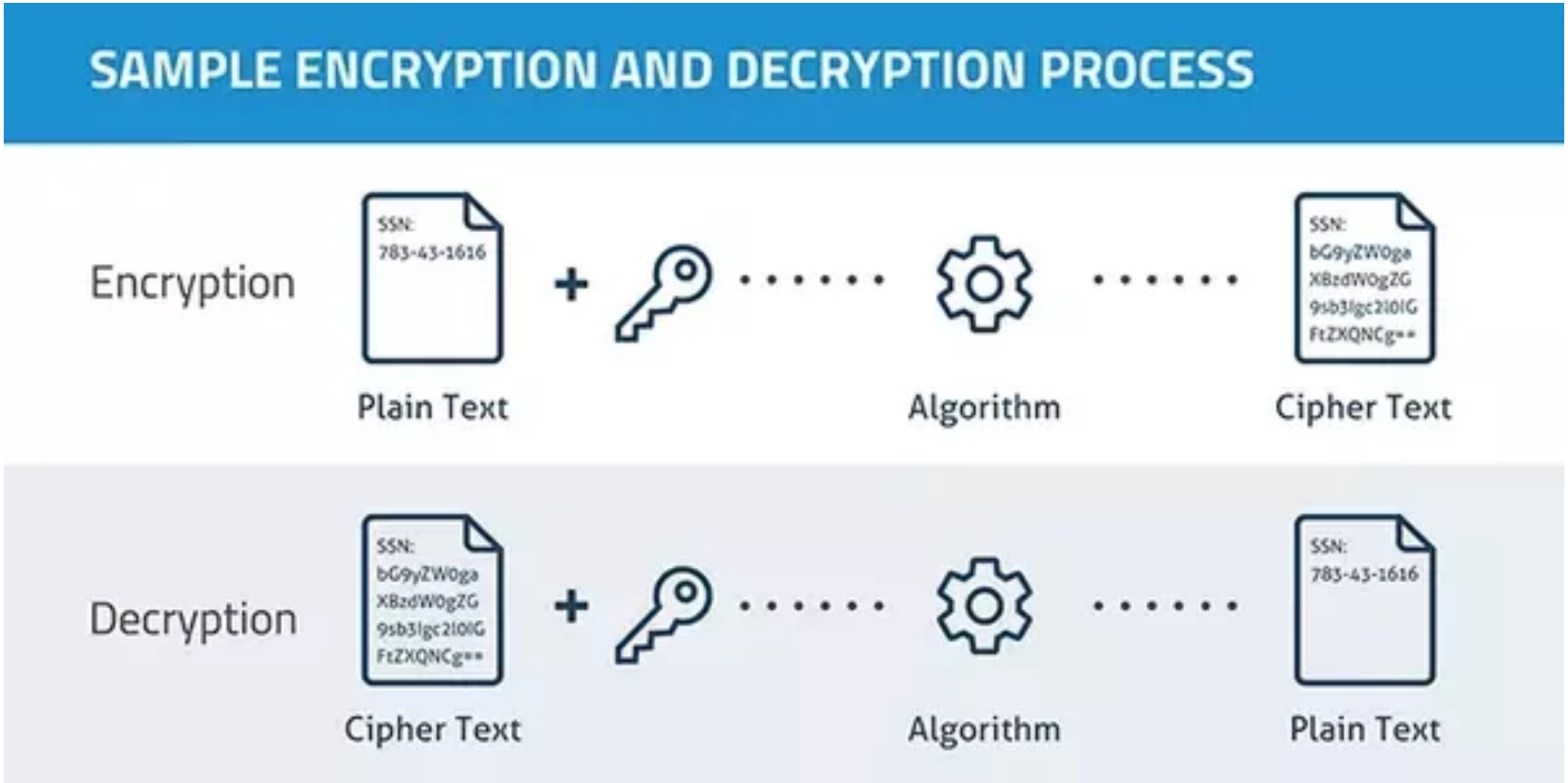

Figure 1: Crypto.

Table of Contents

Classical Cryptography

- Classical cryptography consists of encryption methods (ciphers) that don't require a machine or computer.

Classical Cryptography

- Classical cryptography consists of encryption methods (ciphers) that don't require a machine or computer.
- Two types of ciphers were common: transposition and substitution.

Transposition cipher

- A transposition cipher is a method of encryption that permutes or reorders the letters of the plaintext message.
- Encryption: Reorder the letters of the message
- Decryption: Do the reordering backwards.

Transposition cipher

- A transposition cipher is a method of encryption that permutes or reorders the letters of the plaintext message.
- Encryption: Reorder the letters of the message
- Decryption: Do the reordering backwards.

```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

Figure 2: Rail Fence cipher

Example of a transposition cipher

Fig. 3 Scytale Tool

Figure 3: Scytale Tool used by the Ancient Greeks

Substitution Cipher

- A substitution cipher differs from a transposition cipher where the letters of the plaintext remain in the same position but each letter or group of letters is altered in some way.

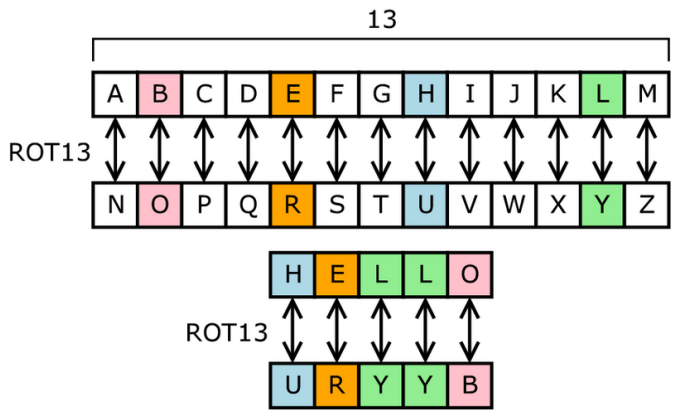

Figure 4: ROT13

Types of substitution ciphers

- **Simple substitution:** Plaintext letters are substituted individually.
- **Polygraphic substitution:** Plaintext letters are substituted in groups.
- **Monoalphabetic cipher:** Fixed substitution alphabet is used throughout the entire message.
- **Polyalphabetic cipher:** Used different substitution alphabets on different parts of the message.

Substitution Ciphers in History

- **Atbash cipher:** Used to encrypt the Hebrew alphabet.
- **Mlecchita vikalpa:** "the art of understanding writing in cypher, and the writing of words in a peculiar way
- **Polybius Square:** 5x5 Grid
- **Ceasar Cipher:** Simple substitution cipher used by Julius Ceasar. Each letter shifted ro the right by 3.
- **Hill Cipher:** Invented by Lester S. Hill. First cipher that was practical to operate on more than three symbols at once.

One Time Pad

- The most secure encryption technique that cannot be cracked.
- PLAINTEXT $\oplus$ KEY $=$ CIPHERTEXT

One Time Pad

- The most secure encryption technique that cannot be cracked.
- PLAINTEXT $\oplus$ KEY $=$ CIPHERTEXT
- Uncrackable if the following conditions are ALL met:
  - Truly random
  - At least as long as the plaintext
  - Never reused
  - Kept in complete secret.

Crib Dragging

- If the key is resused then for plaintext p_1, p_2 we have two ciphertext c_1, c_2.
- Notice that $c_1 \oplus c_2 = (p_1 \oplus k) \oplus (p_2 \oplus k) = p_1 \oplus p_2$.
- We can guess words and xor it with this result and if the output isn't garbage then that words is probably in the plaintext.

Frequency Analysis

- **Frequency Analysis:** We can use statistics to crack ciphers.
- Count letters and determine their frequencies.

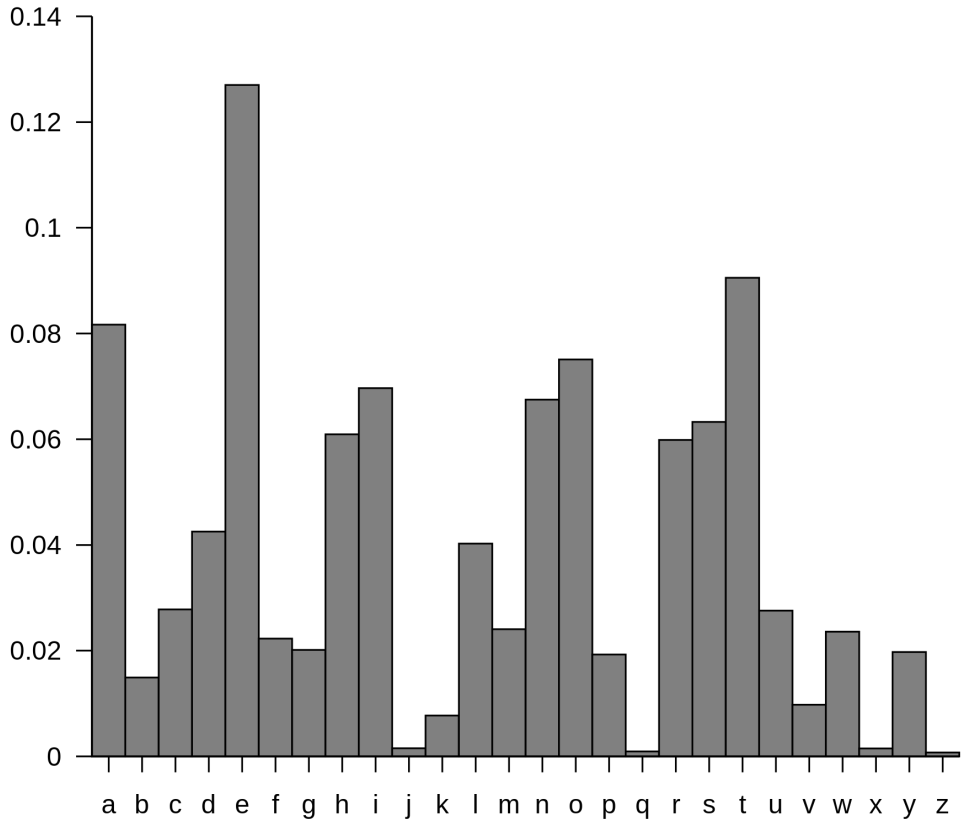

Figure 5: Etaoin shrdlu

Table of Contents

Math

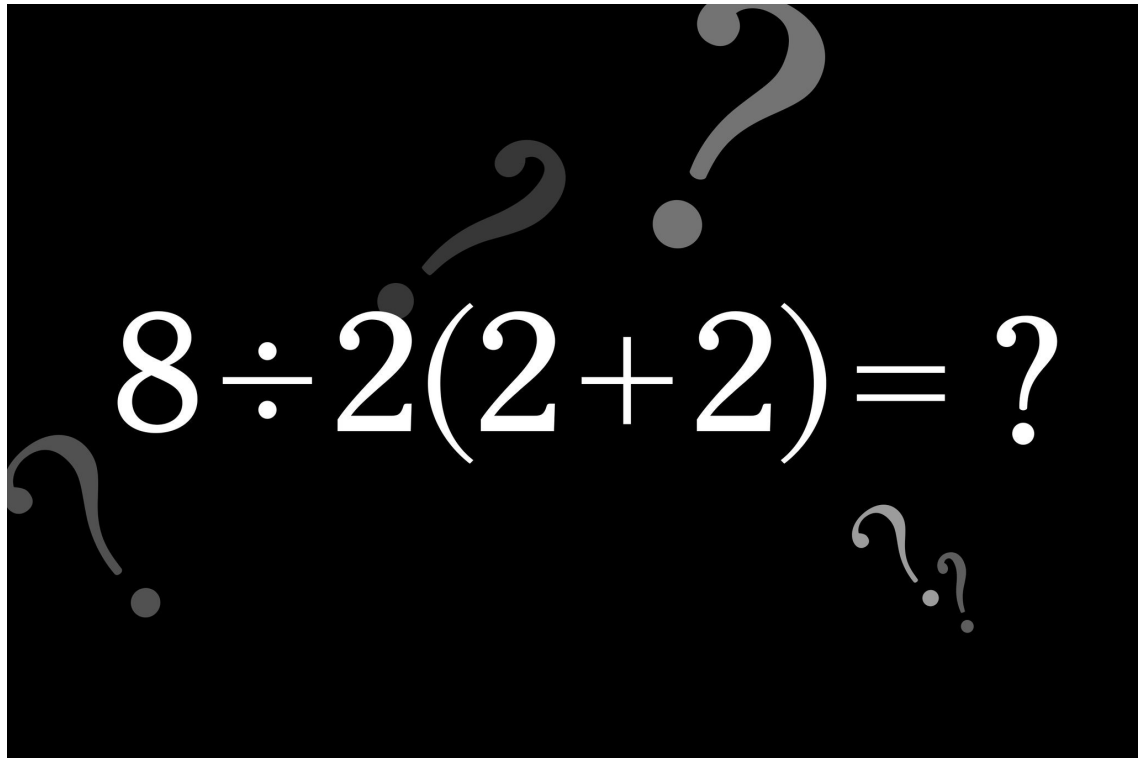

Figure 6: Math

Modern Cryptography

- Most modern cryptography algorithms are very secure.
- All ciphers before the 1970s were **symmetric key algorithms**.
- This means that the private key must be shared through a secure channel.

Modern Cryptography

- Most modern cryptography algorithms are very secure.
- All ciphers before the 1970s were **symmetric key algorithms**.
- This means that the private key must be shared through a secure channel.
- What if we shared a key with the world and allow anyone to send us messages that can only be decrypted by our private key?

Modern Cryptography

- Most modern cryptography algorithms are very secure.
- All ciphers before the 1970s were **symmetric key algorithms**.
- This means that the private key must be shared through a secure channel.
- What if we shared a key with the world and allow anyone to send us messages that can only be decrypted by our private key? hahaha jkjk...

Modern Cryptography

- Most modern cryptography algorithms are very secure.
- All ciphers before the 1970s were **symmetric key algorithms**.
- This means that the private key must be shared through a secure channel.
- What if we shared a key with the world and allow anyone to send us messages that can only be decrypted by our private key? hahaha jkjk... Unless?

Public Key vs Private Key

Public Key vs Private Key		
	Public Key	**Private Key**
Definition	A published key that can be used to send a secure message to a receiver.	A secret key that can be used to decrypt messages encrypted with the corresponding public or private key.
Applies to	Asymmetric Encryption	Asymmetric Encryption Symmetric Encryption

Figure 7: Keys

Public Key Encryption

- Also known as Asymmetric Encryption.
- These algorithms are under the assumption that some problem is very hard to solve.
- As long as the private key is computationally "hard" to compute, we are safe.

RSA

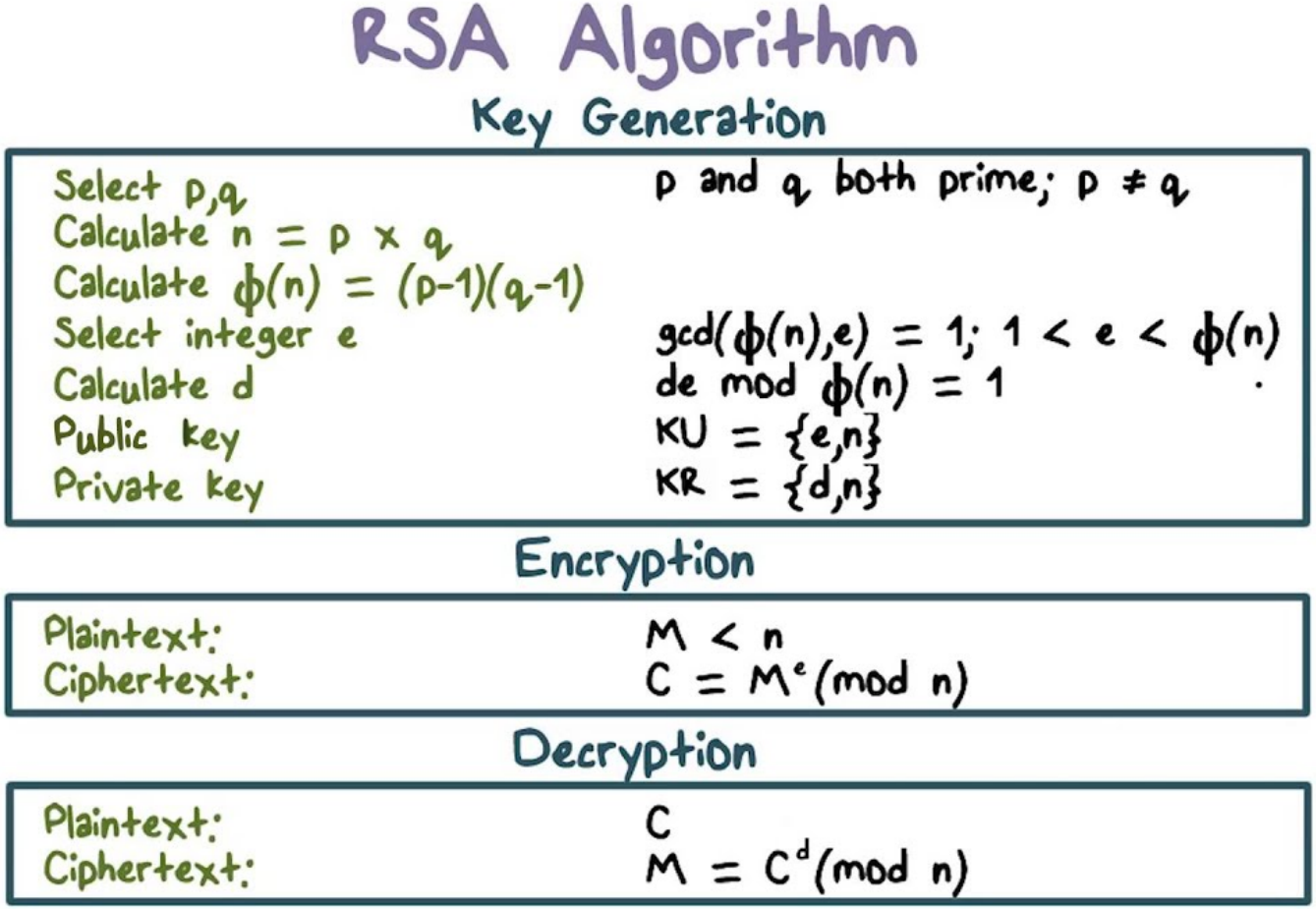

Figure 8: Cartoon rsa

Diffie-Hellman

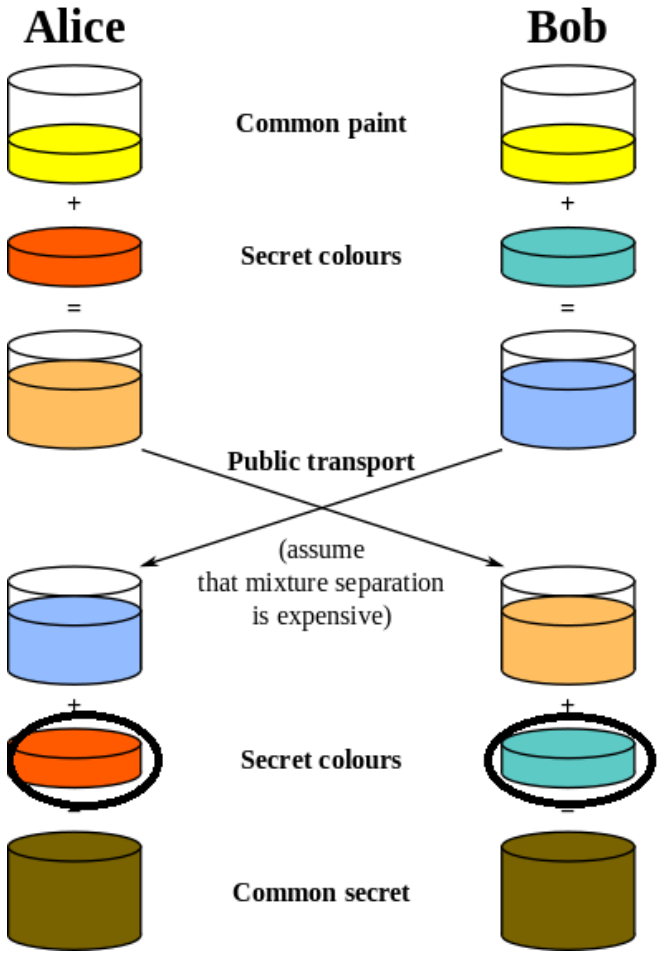

Figure 9: Diffie-Hellman with Paint

Digital Signatures

- Alice first signs her message with her private key and sends the message to Bob.
- Bob can then verify that Alice send the message by using her private key.

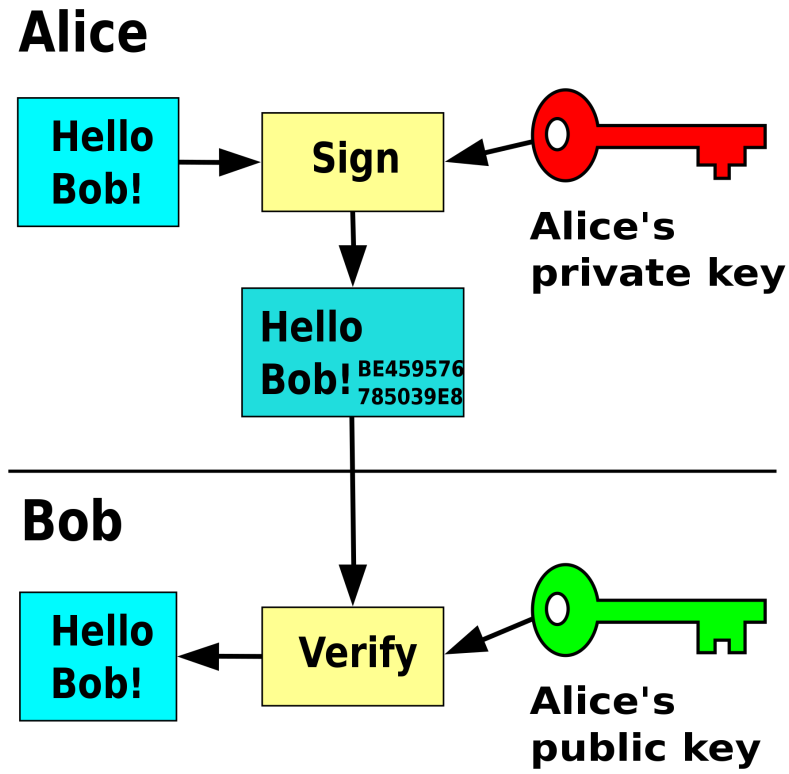

Figure 10: Digital Signatures

Postmodern Cryptography

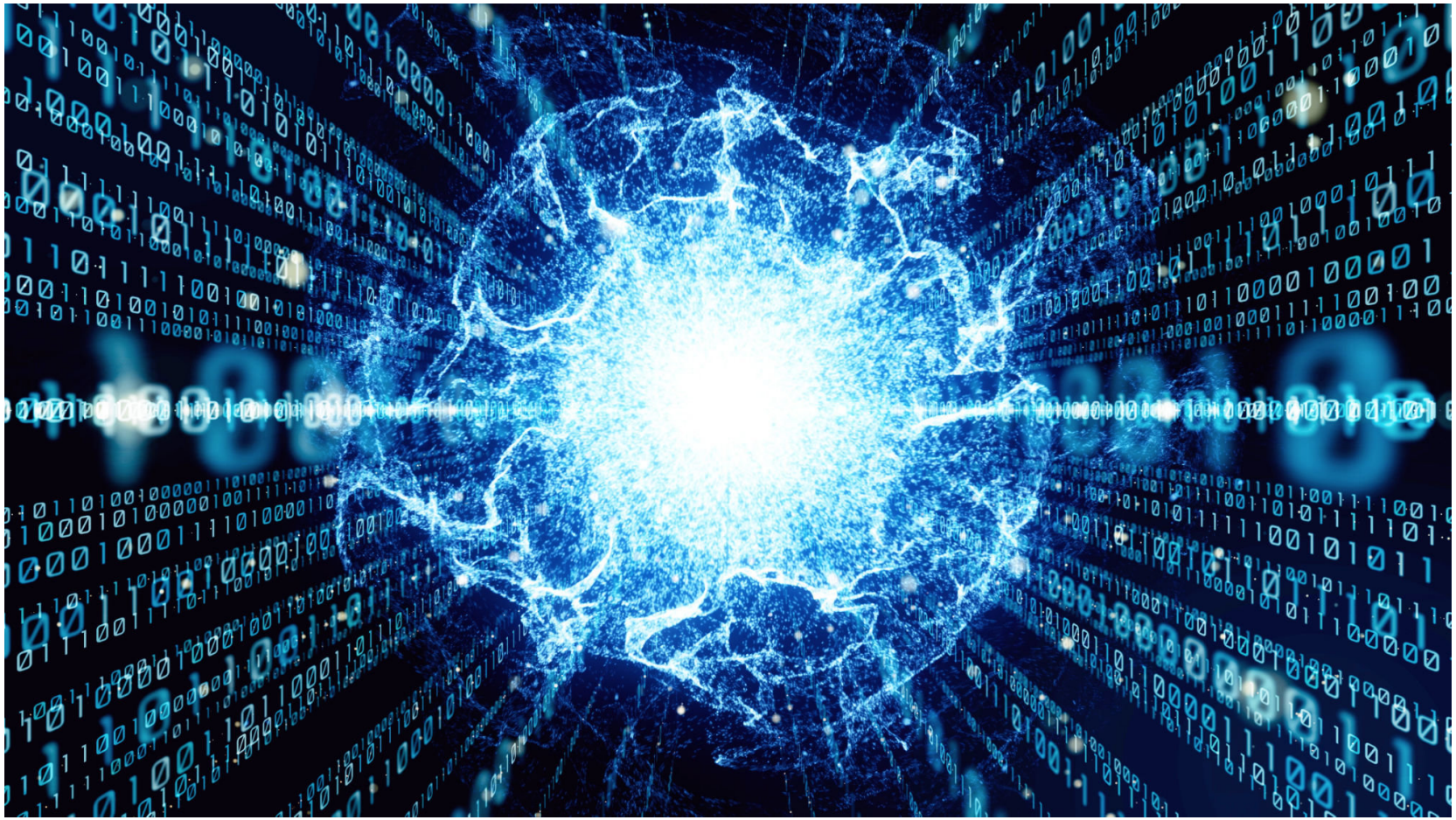

Figure 11: First google image result when searching "Quantum Computing"

Future Topics

- Quantum Cryptography
- Math
- Stream/Block ciphers
- Hashing
- Advanced attacks