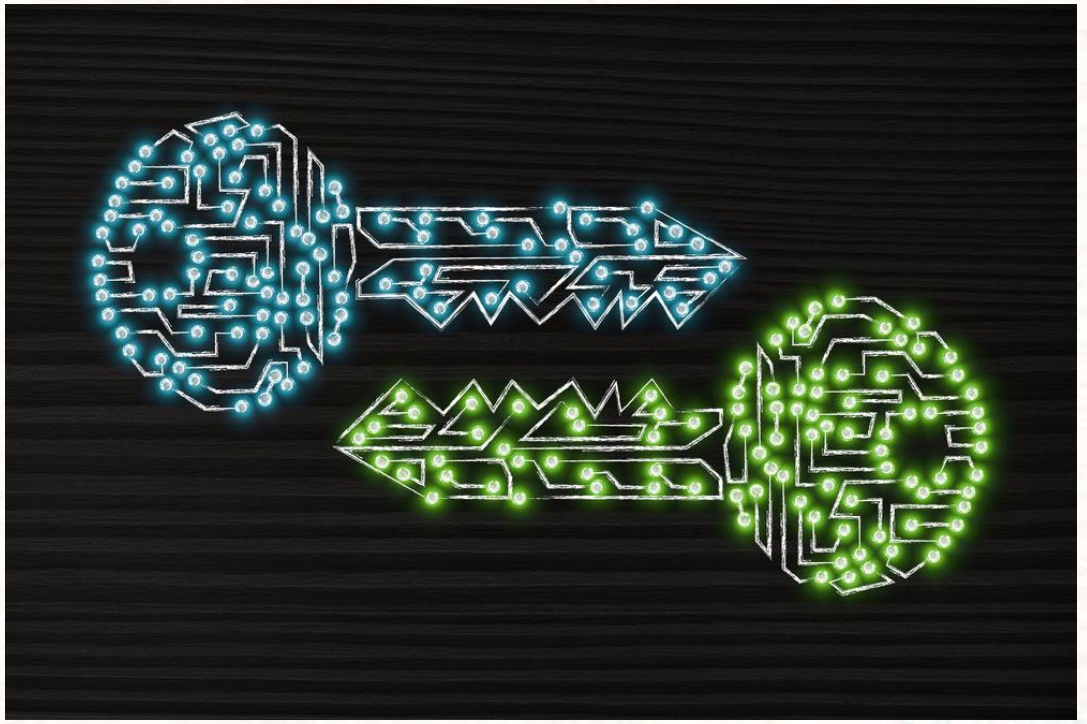
Cryptography

Teagan Stephenson

What is Cryptography?

- Kyrptos: hidden
- The study of cryptosystems
- Cryptosystem: a formalized cipher



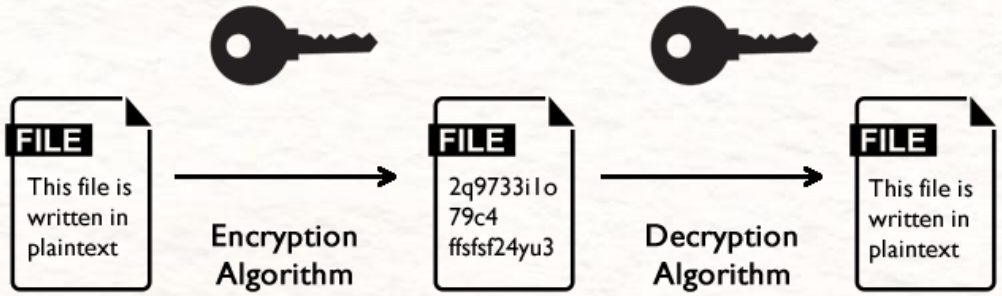
https://themerkle.com/ai-and-quantum-computing-pose-no-threat-to-cryptography-experts-say/

Why is it important?

- Security and privacy!
- Keep important data away from those who shouldn't have it
- Do you want someone to see your account password?

Cryptosystem:

- The tuple (P, C, K, E, D)
- P is the finite set of plaintexts
- C is the finite set of ciphertexts
- K is the keyspace
- E is the encryption rule
- D is the decryption rule

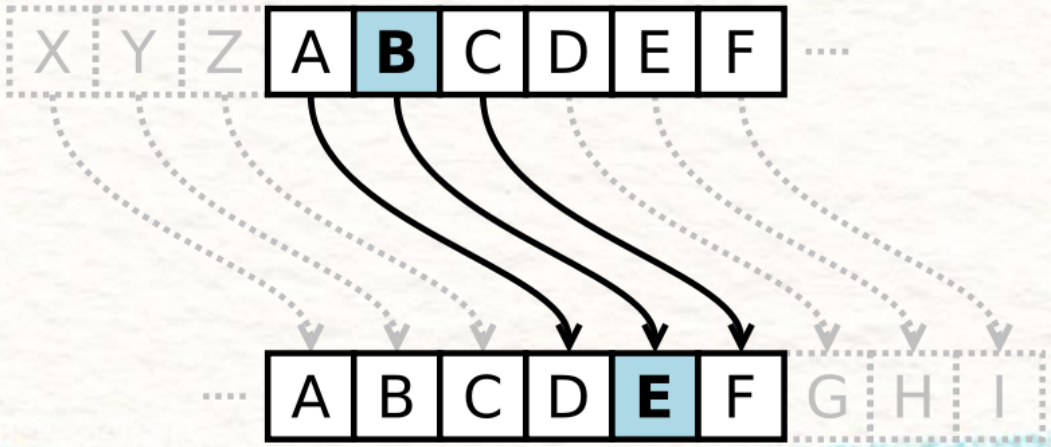


Basic types of ciphers

- Monoalphabetic
  - Substitution
  - Ceasar/shift
- Polyalphabetic
  - Vigenere
  - Playfair
- Transposition
  - Columnar
- Bit-level
  - One-time pad
  - AES
  - DES

Shift cipher

- $P = Z_{26}$
- $C = Z_{26}$
- $K = Z_{26}$
- $E = x + K \pmod{26}$
- $D = y - K \pmod{26}$



Example:

Encrypt "fun" with K = 10

'f' = 5 'u' = 20 'n' = 13

5 + 10 = 15 = 'p'
20 + 10 = 30 (mod 26) = 4 = 'e'
13 + 10 = 23 = 'x'

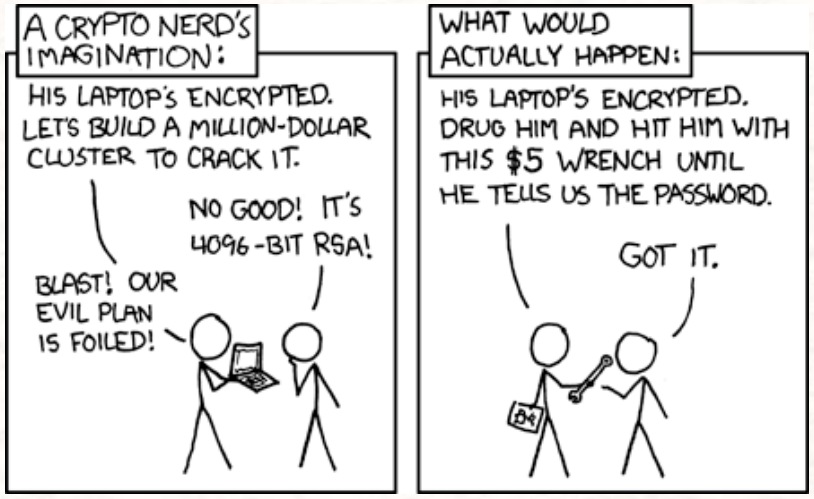
"pex"

Cryptanalysis:

- Crack the cipher!
- Even if only the ciphertext is known, may be able to use clues

Basic techniques:

- Brute force!
- Frequency analysis (monoalphabetic)



https://xkcd.com/538/

Perfect Secrecy

- Goal is to obtain perfect secrecy
- The ciphertext gives away no clues about the plaintext
- Cannot be decrypted without the key
- One-time pad

https://warriorgirl3.wordpress.com/2014/04/15/americas-secret-atomic-city/

One-time pad

- Perfect secrecy IF each bit of key is chosen at random AND the key is only used once
- $P = C = K = Z_2$
- K must be as long as the message
- Xor the message with K
- Impossible to crack, even with unlimited computing power
- Inconvenient to get key to both people

Public key encryption

- Assymetric key encryption
- Uses two different keys: public key and private key
- Private key only known by one computer
- Public key given to anyone
- Can only decrypt the encrypted message with the private key
- Allows for secure communication across the web
- Authenticating the public key can be an issue

https://www.publicdomainpictures.net/en/view-image.php?image=41544&picture=keys

DES and AES

Data Standard Encryption

- Adopted in 1977
- Symmetric key block cipher
- Uses 64-bit plaintext and 56-bit key
- key is too small for modern computers

Advanced Standard Encryption

- Adopted in 2001
- Symmetric key block cipher
- 128-bit plaintext
- 128, 192, or 256-bit key
- Replaced DES
- More secure than DES, and also more efficient

Sources:

- https://techdifferences.com/difference-between-des-and-aes.html
- https://computer.howstuffworks.com/encryption3.htm
- https://www.tutorialspoint.com/cryptography/traditional_ciphers.htm
- Dr. Marmorstein