Document of evolution of cryptology in different eras:

- Ancient era:
  - Scytale:
    It was used by the spartans for military communications . The scytale is a cylindrical tool(rod) made of wood or metal. The sender writes the original message on a strip of parchment which is wrapped around the rod. A parchment is a strip of animal skin. The parchment is wrapped around rod and then the message is written . When the parchment is removed it becomes a set of random letters. The receiver must have the cylindrical rod of the same diameter to decode the message.

image of scytale

- Electromechanical era:
  - Enigma machine (cryptography):
    When key is pressed, the electrical current flows through the rotors. When the rotor spins the light lights for the word typed with the new word.
    The signal reaches the reflectors and is bounced back through the rotors in the opposite direction.

Enigma machine

- Bombe(cryptanalysis):
  It was designed by Alan Turing to crack decode the Enigma machine. It was created in 1920.
  By using the known pieces of plaintext and ciphertext it could use different rotor setting and configuration to decode the messages created using the Enigma machine.

Image of Bombe

- Modern era:
  - Blockchain and Cryptocurrencies:
    1. Bitcoin:
       Bitcoin was created by Satoshi Nakamoto in 2009. Bitcoin is the first decentralised cryptocurrencies that relies on cryptographic techniques and blockchain technology for secure and transparent transactions without any interfierence.
    2. Smart contracts:
       Smart contacts are self executing contracts with the terms directly written into the code, ensuring secure transaction without any interfierance.

  - Computational Power:
    (a) Brute-Force Attacks:
    Increased computational power has made brut-force
    Attacks more feasible.
    (b) Side channel attacks:
    Attacker exploit physical implementation of cryptographic systems, such as power consumption or electromagnetic emission, to gain information about cryptographic keys.