History of Cryptography and Cryptanalysis

Kurt Pan

March 21, 2025

Table of Contents

1. The birth of cryptography

2. The Evolution of Secret Writing
   - Steganography
   - Codes
   - Ciphers
   - Passwords

3. History of Cryptanaysis

4. Modern Cryptography

It must be that as soon as a culture has reached a certain level, probably measured largely by its **literacy**, **cryptography** *appears spontaneously - as its parents,* **language** *and* **writing**, *probably also did.*

The multiple human needs and desires that demand **privacy** *among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write.*

Cultural diffusion seems a less likely explanation for its occurrence in so many areas, many of them distant and isolated.

(Kahn 1967, p. 84).

Table of Contents

1. The birth of cryptography

2. The Evolution of Secret Writing
    - Steganography
    - Codes
    - Ciphers
    - Passwords

3. History of Cryptanaysis

4. Modern Cryptography

Steganography

Steganography

Secret communication achieved by hiding the *existence* of a message.

- (Greek) Scraping the wax off a pair of wooden folding tablets, writing on the wood underneath and then covering the message over with wax again.
- (Chinese) Wrote messages on fine silk, which was scrunched into a tiny ball and covered in wax.
- Writing in invisible ink.

`https://emoji.paulbutler.org/?mode=decode`
(Can you find the invisible msg in the 3rd bullet point?)
Interception of the message immediately compromises all security.

Codes

Code

A code always takes the form of a book where a numerical or alphabetic codeword is substituted for a complete word or phrase from the plaintext.

e.g Morse code, Commercial code, Base58

- The best way to break a code is to

  ~~steal the codebook~~!

Crypto

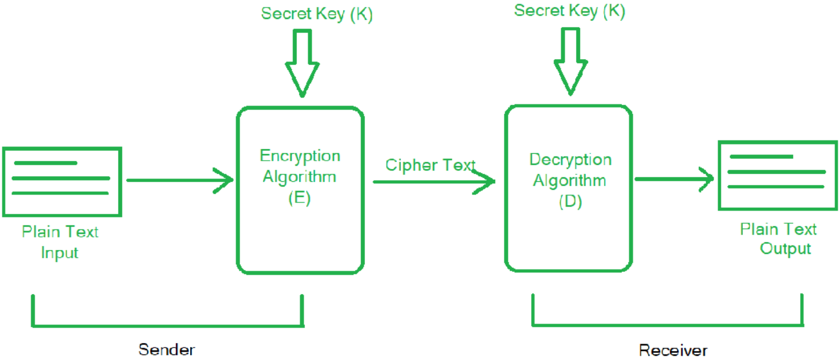
> *In contemporary public discourse, it is quite common to refer to* **crypto** *as* **encryption***,but encryption is just one term in the broader science of* **cryptology***, the science of making and breaking* **ciphers***.*

- cryptography: making ciphers , by cryptographers
- cryptanalysis: breaking ciphers, by cryptanalysts
- cipher: a mathematical function that allows its user to transform a plaintext message into a ciphertext message (Encryption/Decryption)
- cryptographer : to design ciphers strong enough so unauthorized persons cannot figure out how to transform ciphertexts back into plaintext and read the messages without permission.
- cryptanalyst : to figure out how the cipher is designed so they can transform ciphertexts back into plaintext and read the messages without permission, usually without the sender even knowing

Cipher

The aim of cryptography is not to hide the *existence* of a message, but rather to hide its *meaning*, a process known as **encryption**.

Without knowing the scrambling protocol, the enemy should find it difficult, if not impossible, to re-create the original message from the encrypted text.



Transposition

The letters of the message are simply *rearranged*, effectively generating an anagram.

Rail Fence Transposition

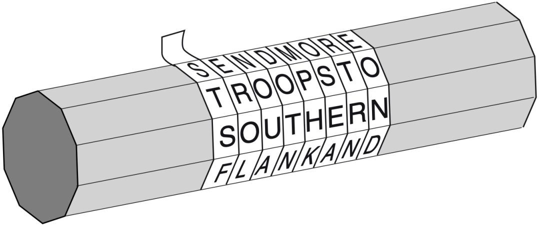
THY SECRET IS THY PRISONER; IF THOU LET IT GO, THOU ART A PRISONER TO IT

↓

T Y E R T S H P I O E I T O L T T O H U R A R S N R O T
H S C E I T Y R S N R F H U E I G T O A T P I O E T I

↓

TYERTSHPIOEITOLTTOHURARSNROTHSCEITYRSNRFHUEIGTOATPIOETI



The Spartan scytale

Substitution Cipher

To pair letters of the alphabet at *random*.

A	**D**	**H**	**I**	**K**	**M**	**O**	**R**	**S**	**U**	**W**	**Y**	**Z**
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
V	**X**	**B**	**G**	**J**	**C**	**Q**	**L**	**N**	**E**	**F**	**P**	**T**

- In transposition each letter retains its *identity* but changes its *position*,
- In substitution each letter changes its *identity* but retains its *position*.

e.g. Caesar , Vigenere, OTP

Cipher

Cipher is the name given to any form of *cryptographic substitution* in which *each letter* is replaced by another letter or symbol.

Passwords

Password Authentication

A method of *proving identity* rather than encrypting messages.

- Unlike codes and ciphers, passwords are used for **authentication**
- Key differences:
  - Codes: Replace words/phrases with other symbols
  - Ciphers: Transform message content
  - Passwords: Verify user identity
- Historical examples:
  - Military watchwords (”Who goes there?”)
  - Secret societies’ passphrases
  - Ancient guard posts’ challenge-response systems

Modern Password Systems

Key Concepts

Modern passwords are stored as *cryptographic hashes*, not plaintext.

- Security features:
  - One-way hash functions
  - Salt values
  - Key stretching
- Common vulnerabilities:
  - Dictionary attacks
  - Rainbow tables
  - Social engineering

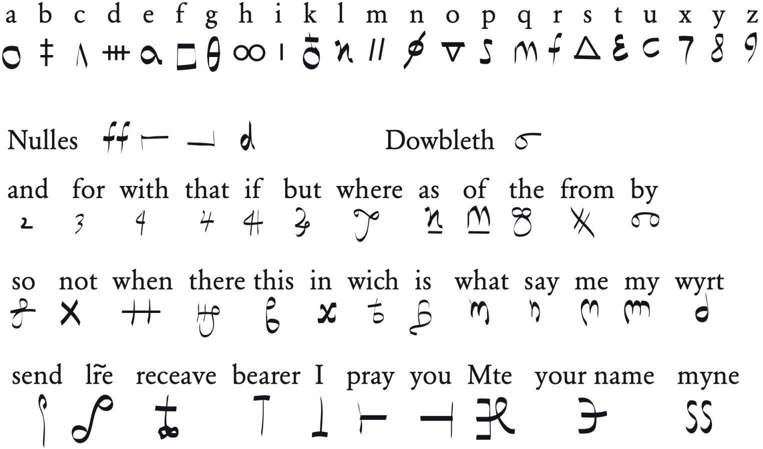
Table of Contents

1. The birth of cryptography
2. The Evolution of Secret Writing
   - Steganography
   - Codes
   - Ciphers
   - Passwords
3. History of Cryptanaysis
4. Modern Cryptography

The Cipher of Mary Queen of Scots

The birth of cryptography, the substitution cipher and the invention of codebreaking by frequency analysis.

> *(October 15, 1586) , Mary Queen of Scots was on trial for treason. She had been accused of plotting to assassinate Queen Elizabeth in order to take the English crown for herself.*
>
> *Elizabeth would sanction Mary's execution only if Walsingham could prove beyond any hint of doubt that she had been part of the assassination plot. ...The challenge for Walsingham was to demonstrate a clear link between Mary and the plotters.*
>
> *(Mary) had been careful to ensure that all her correspondence with the conspirators had been written in cipher. ... Mary believed that even if Walsingham had captured the letters, he could have no idea of the meaning of the words within them.*
>
> *Not for the first time,* **a life hung on the strength of a cipher***.*
>
> *(Singh 2002, p. 6-8).*



a b c d e f g h i k l m n o p q r s t u x y z

Nulles

Dowbleth

and for with that if but where as of the from by

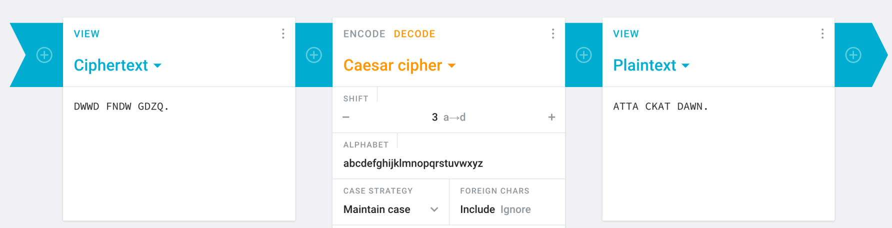
so not when there this in wich is what say me my wyrt

send lr̃e receave bearer I pray you Mte your name myne

Figure 9 The execution of Mary Queen of Scots.

Breaking the Caeser Cipher

brute force attack !



DWWD FNDW GDZQ.

SHIFT
3 a→d

ALPHABET
abcdefghijklmnopqrstuvwxyz

CASE STRATEGY
Maintain case

FOREIGN CHARS
Include Ignore

ATTA CKAT DAWN.

Breaking Substitution Cipher

random permutation

Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Key	Q	E	P	R	W	O	X	B	K	J	N	Y	A
Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Key	V	H	G	L	C	F	D	I	T	S	U	Z	M

127 billion years for brute force attack.

- letter frequency attack
- known-plaintext attack

Breaking the Vigenre Cipher

The ”Unbreakable” Cipher

The Vigenre cipher remained unbroken for 300 years and was known as ”le chiffre indchiffrable”

Keyword	W	H	I	T	E	W	H	I	T	E	W	H	I	T	E	W	H	I	T	E	W	H	I
Plaintext	d	i	v	e	r	t	t	r	o	o	p	s	t	o	e	a	s	t	r	i	d	g	e
Ciphertext	Z	P	D	X	V	P	A	Z	H	S	L	Z	B	H	I	W	Z	B	K	M	Z	N	M

- Broken by Charles Babbage (1850s):
  - Discovered repeating patterns in ciphertext
  - Determined key length using these patterns
  - Applied frequency analysis to each shift
- Friedrich Kasiski (1863):
  - Published first public method
  - Known as the Kasiski examination

Enigma and Midway

[VIDEO]

Mathematical Cryptanalysis

19th Century Methods

- Index of coincidence
- Probability theory
- Pattern recognition

Key Contributions

- William F. Friedman
- Claude Shannon
- Alan Turing

Impact

These mathematical foundations transformed cryptanalysis from an art into a science

Kerckhoffs' Principle

Kerckhoffs' Principle

The security of a cryptosystem **must not** depend on keeping secret the crypto-algorithm. The security depends only on keeping secret the **key**. [a]

[a] A Brief Biography of Auguste Kerckhoffs by Peng SUN

Table of Contents

Modern Era (19th-20th Century)

- Telegraph and radio communication drove cipher development
- World War I: ADFGVX cipher
- World War II:
    - German Enigma machine
    - Allied cryptanalysis at Bletchley Park
    - American SIGABA machine

The Birth of Modern Cryptography

Shannon's Information Theory (1940s)

Claude Shannon established the theoretical foundation of modern cryptography:

- Information entropy
- Perfect secrecy
- Confusion and diffusion principles

Key Developments

- Transition from mechanical to electronic systems
- Development of computer-based encryption
- Birth of public-key cryptography

Symmetric vs Asymmetric Cryptography

Symmetric

- Same key for encryption and decryption
- DES (1977)
- AES (2001)
- Faster computation

Asymmetric

- Public/private key pairs
- RSA (1978)
- ECC (1985)
- Key distribution advantage

Public Key Infrastructure (PKI)

Components

- Digital certificates
- Certificate authorities (CAs)
- Public key directories
- Certificate revocation lists

Applications

- HTTPS/TLS
- Digital signatures
- Secure email (S/MIME)
- Code signing

Modern Security Goals

Core Security Properties

- **Confidentiality**: Preventing unauthorized access
- **Integrity**: Ensuring data hasn't been modified
- **Authenticity**: Verifying the origin of data
- **Non-repudiation**: Cannot deny sending/receiving

Security Models

- IND-CPA (Chosen Plaintext Attack)
- IND-CCA (Chosen Ciphertext Attack)
- Forward Secrecy
- Romdom Oracle Model

Emerging Technologies

Post-Quantum Cryptography

- Lattice-based cryptography
- Hash-based signatures
- Multivariate cryptography
- NIST standardization process

New Paradigms

- Homomorphic encryption
- Secure multi-party computation
- Blockchain technology
- Quantum key distribution

Future Challenges

Emerging Threats

- Quantum computing threats
- Post-quantum cryptography
- AI-based attacks
- Zero-day vulnerabilities

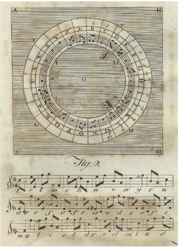
Research Directions

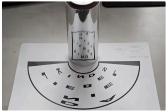
- Quantum-resistant algorithms
- Homomorphic encryption
- Lightweight cryptography
- Privacy-preserving computation

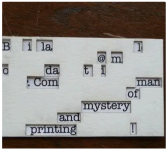
Crypto *is both a mathematical* **science** *and an* **artistic** *practice that enables particular kinds of human relationships.*

Crypto is unlike other sciences because cryptography is about intelligent **adversaries** *who are actively fighting over whether secrets will be revealed.*

From this perspective,crypto can be considered an art, specifically an **art of communication**.







Thanks!