# Cryptology: Basic Definitions and a Simple Example

Dr. Chuck Rocca

roccac@wcsu.edu

https://sites.wcsu.edu/cryptology/

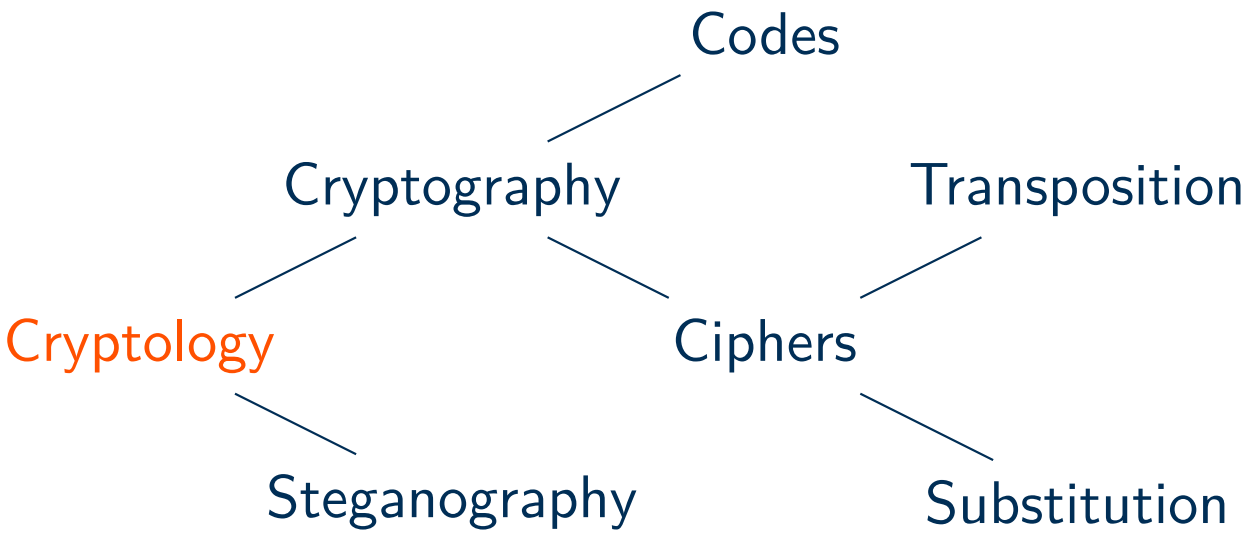

# Table of Contents



# Basic Definitions

**Definition (Cryptology)**

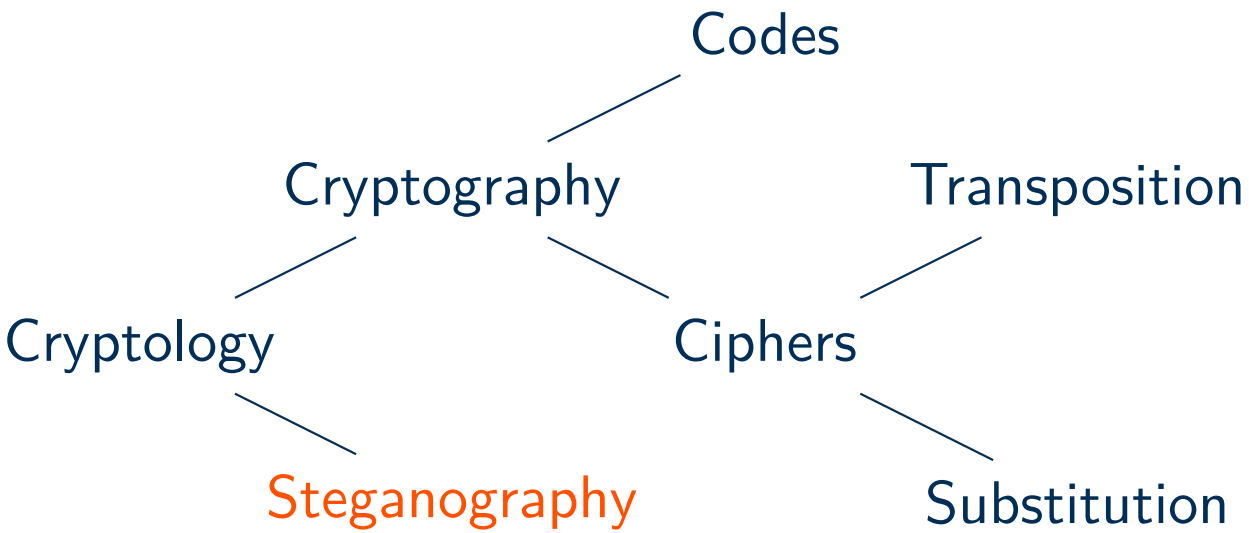
Cryptology is the science of keeping or discovering secrets.




# Basic Definitions

**Definition (Steganography)**

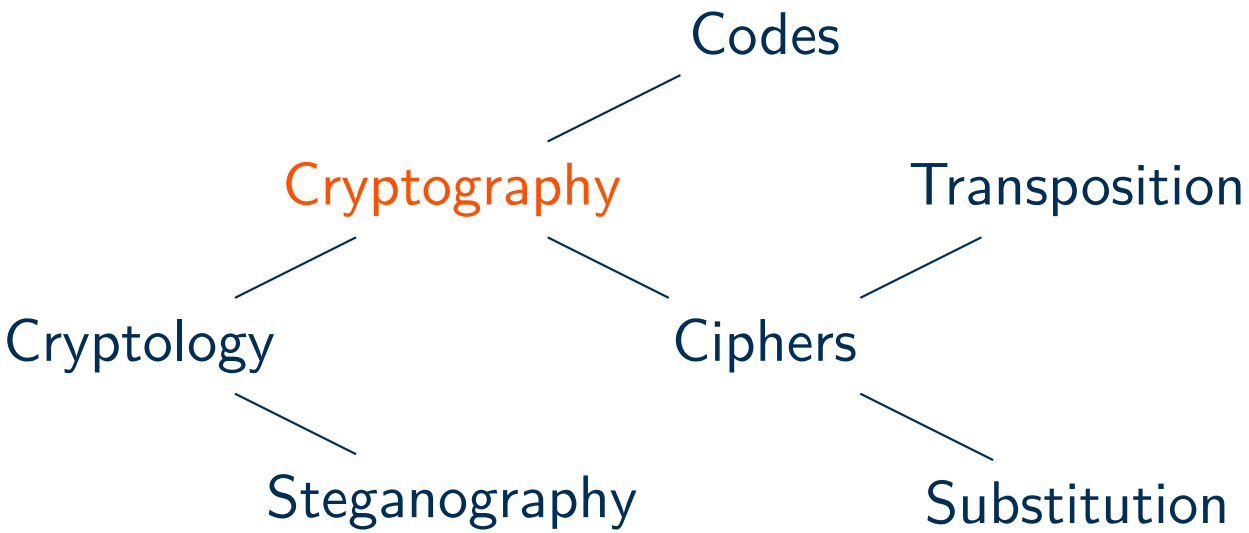
Steganography focuses on hiding the very existence of information.




# Basic Definitions

**Definition (Cryptography)**

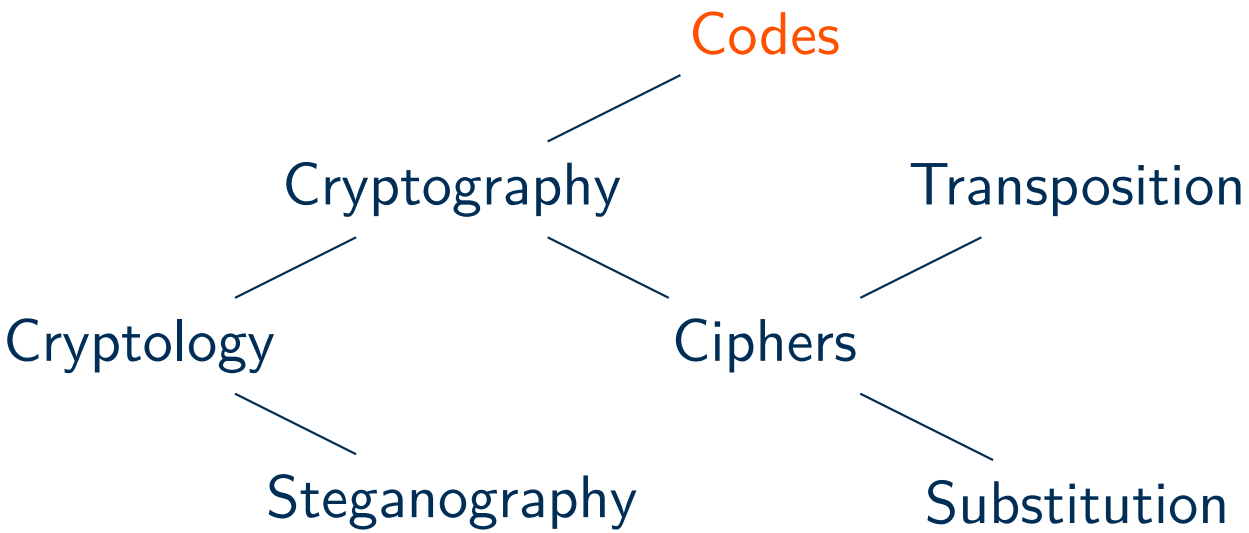
Cryptography focuses on hiding the meaning of information.




# Basic Definitions

**Definition (Codes)**

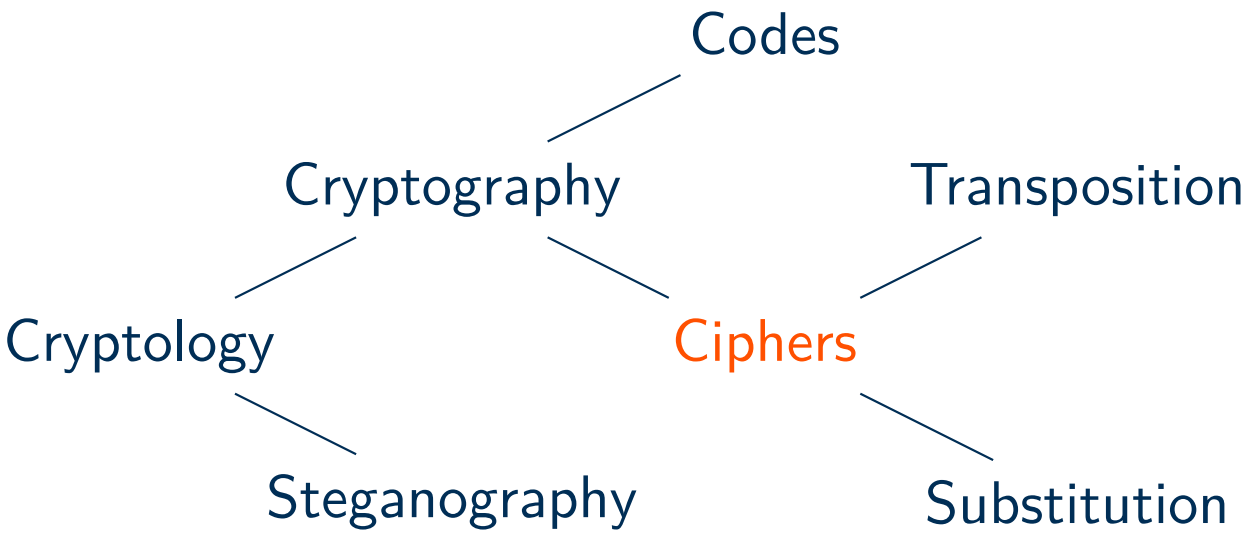
Codes change messages on the level of words or phrases.




# Basic Definitions

**Definition (Ciphers)**

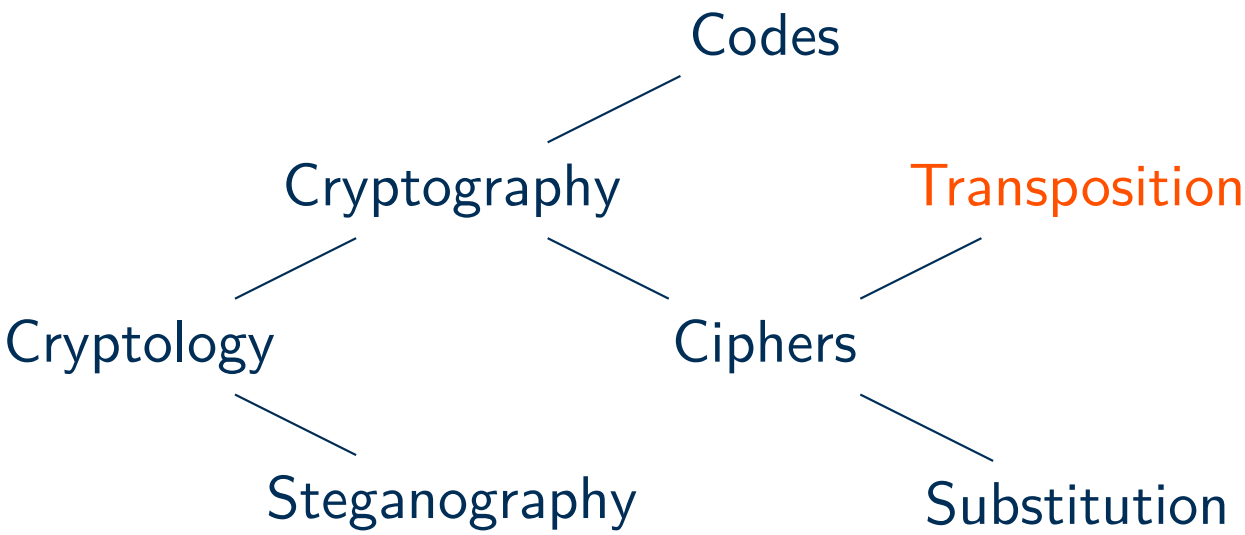
Ciphers change messages on the level of letters or blocks of letters.




# Basic Definitions

**Definition (Transposition Cipher)**

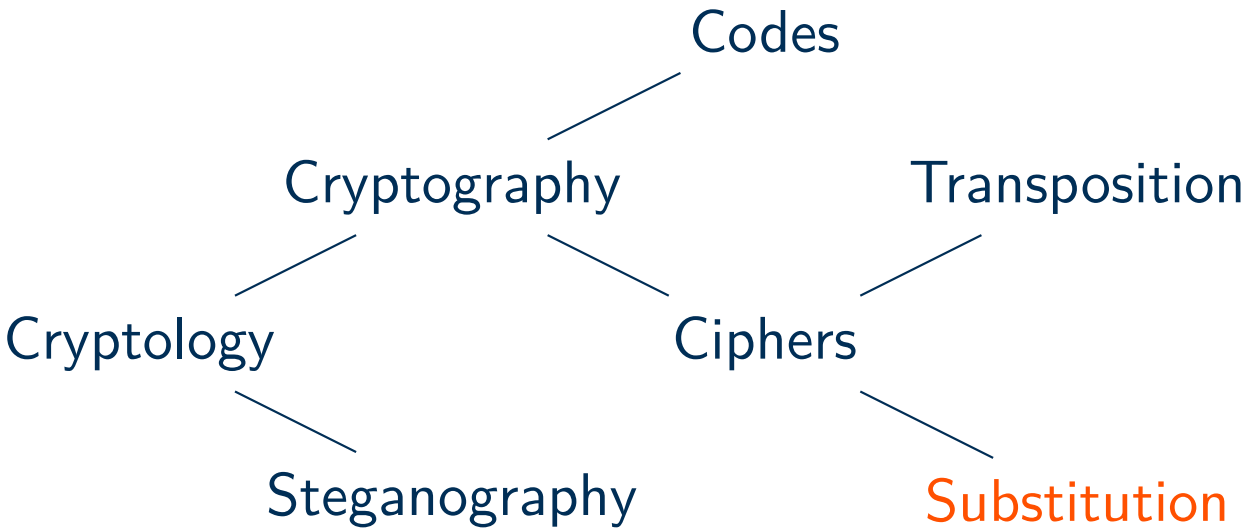
A Transposition Cipher changes a message by rearranging characters or blocks of characters (like an anagram).




# Basic Definitions

**Definition (Substitution Cipher)**

A Substitution Cipher changes a message by replacing characters or blocks of characters with other characters or blocks of characters.




# Table of Contents



# Atbash

## Atbash

In Jeremiah, the Bible references two places בבל (Babel) and ששך (Sheshach); these turn out to be the same place. The second name is an enciphered version of the first. This was done by lining up two copies of the alphabet with one of them in reverse order:

א ב ג ד ה ו ז ח ט י ך ל ם ן ס ע ף ץ ק ר ש ת
ת ש ר ק ץ ף ע ס ן ם ל ך י ט ח ז ו ה ד ג ב א

This means א (aleph) is paired with ת (taw), ב (beth) with ש (shin) and so on; hence it is given the name Atbash.

# Atbash

## Atbash - In English

In English the alphabets would line up to form this key:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

And we can encipher a message like the one below.

Plain Text:
the wizard quickly jinxed the gnomes before they vaporized.
Cipher Text:

# Atbash

## Atbash - In English

In English the alphabets would line up to form this key:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

And we can encipher a message like the one below.

Plain Text:

the wizard quickly jinxed the gnomes before they vaporized.

Cipher Text:

G

# Atbash

## Atbash - In English

In English the alphabets would line up to form this key:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

And we can encipher a message like the one below.

Plain Text:

the wizard quickly jinxed the gnomes before they vaporized.

Cipher Text:

GS

# Atbash

## Atbash - In English

In English the alphabets would line up to form this key:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

And we can encipher a message like the one below.

Plain Text:

the wizard quickly jinxed the gnomes before they vaporized.

Cipher Text:

GSV

# Atbash

## Atbash - In English

In English the alphabets would line up to form this key:

a b c d e f g h i j k l m n o p q r s t u v w x y z
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

And we can encipher a message like the one below.

Plain Text:
the wizard quickly jinxed the gnomes before they vaporized.
Cipher Text:
GSV DRAZIW JFRXPOB QRMCVW GSV TMLNVH YVULIV GSVB EZKLIRAVW.

# Atbash

## Atbash - In English

In English the alphabets would line up to form this key:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

Or, decipher one like this.

Cipher Text:

Z DRAZIW'H QLY RH GL EVC XSFNKH JFRXPOB RM ULT.

Plain Text:

# Atbash

## Atbash - In English

In English the alphabets would line up to form this key:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

Or, decipher one like this.

Cipher Text:

Z DRAZIW'H QLY RH GL EVC XSFNKH JFRXPOB RM ULT.

Plain Text:

a

# Atbash

## Atbash - In English

In English the alphabets would line up to form this key:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

Or, decipher one like this.

Cipher Text:

Z DRAZIW'H QLY RH GL EVC XSFNKH JFRXPOB RM ULT.

Plain Text:

a w

# Atbash

## Atbash - In English

In English the alphabets would line up to form this key:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

Or, decipher one like this.

Cipher Text:

Z DRAZIW'H QLY RH GL EVC XSFNKH JFRXPOB RM ULT.

Plain Text:

a wi

# Atbash

## Atbash - In English

In English the alphabets would line up to form this key:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

Or, decipher one like this.

Cipher Text:

Z DRAZIW'H QLY RH GL EVC XSFNKH JFRXPOB RM ULT.

Plain Text:

a wizard's job is to vex chumps quickly in fog.

# Table of Contents



# Monoalphabetic Substitution Cipher

**Definition (Monoalphabetic Substitution Cipher)**

A Monoalphabetic Substitution Cipher is a cipher in which we create a pairing between each letter of the alphabet and exactly one (mono) other letter or character. Atbash is an example of this.

# Plaintext - Ciphertext

**Definition (Plaintext)**

A plaintext message is the version of the message that we can read, i.e.:

a wizard's job is to vex chumps quickly in fog.

# Plaintext - Ciphertext

**Definition (Plaintext)**

A plaintext message is the version of the message that we can read, i.e.:

a wizard's job is to vex chumps quickly in fog.

**Definition (Ciphertext)**

A ciphertext message is the version of the message that we cannot read, i.e.:

Z DRAZIW'H QLY RH GL EVC XSFNKH JFRXPOB RM ULT.

# Encipher - Decipher

## Definition (Encipher)

We encipher a message when we change it from plaintext that we can read to ciphertext which we cannot. We will also sometimes use the term encrypt.

$$\text{plaintext} \longrightarrow \text{ciphertext}$$

# Encipher - Decipher

## Definition (Encipher)

We encipher a message when we change it from plaintext that we can read to ciphertext which we cannot. We will also sometimes use the term encrypt.

$$\text{plaintext} \longrightarrow \text{ciphertext}$$

## Definition (Decipher)

We decipher a message when we change it from ciphertext we cannot read to plaintext we can. We will also sometimes use the term decrypt. (Though that is technically wrong.)

$$\text{ciphertext} \longrightarrow \text{plaintext}$$

# Key-Algorithm

**Definition (Algorithm)**

In this context, an algorithm is the general process we follow to encipher or decipher a message such as replacing one letter with another.

# Key-Algorithm

**Definition (Algorithm)**

In this context, an algorithm is the general process we follow to encipher or decipher a message such as replacing one letter with another.

**Definition (Key)**

The key for a message is a generally secret piece of information that we combine with the algorithm and the plaintext or ciphertext when we encipher or decipher.

# Summary

- Atbash
- Cipher
- Cipher Algorithm
- Ciphertext
- Code
- Cryptography
- Cryptology
- Decipher ($\approx$ decrypt)
- Encipher (encrypt)
- Key
- Monoalphabetic Substitution Cipher
- Plaintext
- Steganography
- Substitution
- Transposition

See Also: `https://sites.wcsu.edu/cryptology/`

# Cryptology: Basic Definitions and a Simple Example

Dr. Chuck Rocca
roccac@wcsu.edu

https://sites.wcsu.edu/cryptology/