

RAM Maths Circle

February 22, 2026

Nagpur

Introduction

A cipher is a set of well-defined rules or an algorithm used to perform encryption and decryption, transforming readable data (plaintext) into an unreadable, scrambled format (ciphertext) and vice-versa. It is a foundational tool in cryptography, used to protect the confidentiality and security of digital information.

We will use the same two plaintext sentences so we can compare how the ciphers behave: Math Is Fun

1 CAESAR CIPHER (shift 3)

The Caesar cipher is a foundational, simple substitution technique where each letter in plaintext is shifted a fixed number of positions down the alphabet. Named after Julius Caesar, who used it for secure communication, it uses a numerical "key" (e.g., shift of 3: A becomes D). While easy to implement, it is weak against modern brute-force attacks.

Encryption rule: Each letter moves 3 positions forward in the alphabet (A→D, B→E, ..., X→A, Y→B, Z→C). - MATH IS FUN → PDWK LV IXQ - WE CRACK CODES → ZH FUD FN FRGHV

Decryption (shift back 3 or forward 23):

PDWK LV IXQ → MATH IS FUN ZH FUD FN FRGHV → WE CRACK CODES

2 ATBASH CIPHER (reverse alphabet)

The Atbash cipher is an ancient, simple substitution cipher that encodes text by reversing the alphabet, mapping A to Z, B to Y, and so on. Originally used for Hebrew, it acts as a mirror code where the first letter is replaced by the last, and vice-versa. It is its own inverse, meaning the same process decrypts the message.

- Encryption rule:

AZ, BY, CX, ..., MN (simple mirror of the alphabet). - MATH IS FUN → NZGS RH UFM - WE CRACK CODES → DV XIZXP XLWVH

Decryption:

Apply Atbash again (it's its own inverse!) → back to original.

3 VIGENERE CIPHER (polyalphabetic — more advanced secure than the others)

The Vigenère cipher is a foundational, classical polyalphabetic substitution cipher developed in the 16th century (often attributed to Blaise de Vigenère, though first described by Giovan Battista Bellaso in 1553). It was nicknamed le chiffre indéchiffrable (the indecipherable cipher) because it resisted analysis for three centuries, marking a significant advancement over simpler Caesar ciphers.

- Keyword: KEY (repeated to match message length)

- Encryption rule:

For each letter, shift by the corresponding letter of the key (K=10, E=4, Y=24).

Example walkthrough for "MATH IS FUN" Plaintext: M A T H I S F U N Key (repeated): K E Y K E Y K E Y Shifts: +10 +4 +24 +10 +4 +24 +10 +4 +24 Ciphertext: W E X R M W P Y W

So: MATH IS FUN → WEXR MW PYW

WE CRACK CODES (with same key KEY repeated): Plaintext: W E C R A C K C O D E S Key: K E Y K E Y K E Y K E Y → I I B D F I S I X N I E

Decryption (subtract the key shifts instead of adding): back to original.