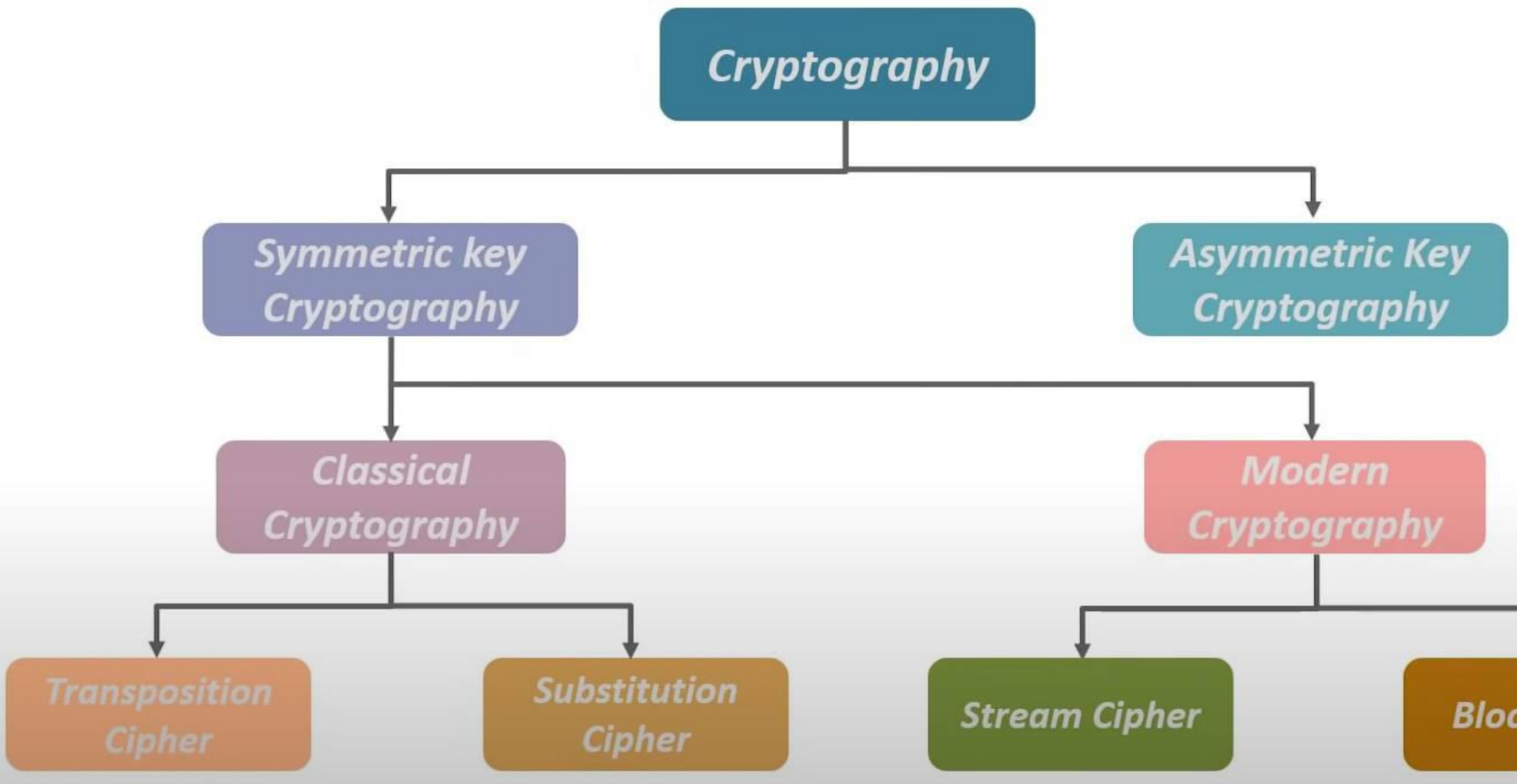
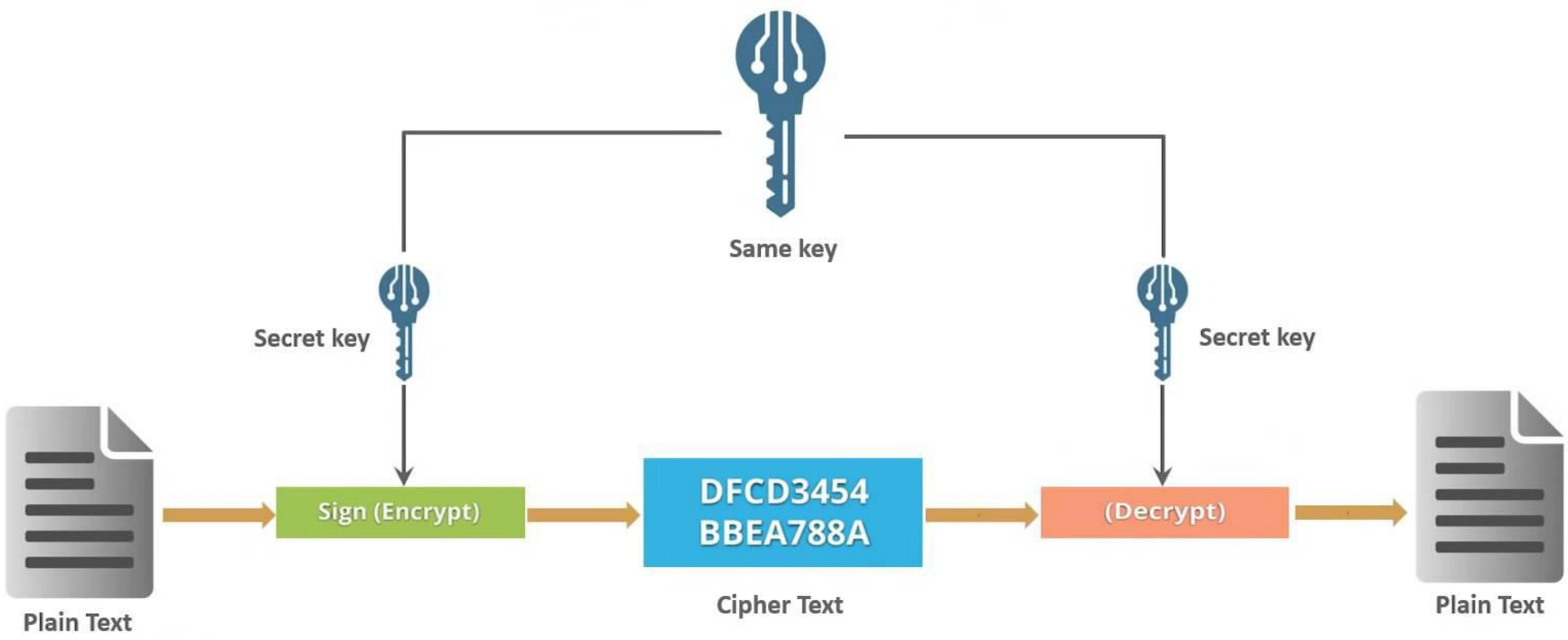
What is Cryptography? | Introduction to Cryptography | Cryptography for Beginners | Edureka

Classification of Cryptography



Symmetric Key Cryptography

*An **encryption** system in which the sender and receiver of a message share a single, common **key** that is used to encrypt and decrypt the message. ... The most popular **symmetric-key** system is the Data **Encryption** Standard (DES)*



Transposition Cipher

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext

1	2	3	4	5	6
M	E	E	T	M	E
A	F	T	E	R	P
A	R	T	Y		

4	2	1	6	3	5
T	E	M	E	E	M
E	F	A	P	T	R
Y	R	A		T	

Plain Text: MEET ME AFTER PARTY

Key Used: 421635

Cipher Text: TEMEEMEFAPTRYRAT

Substitution Cipher

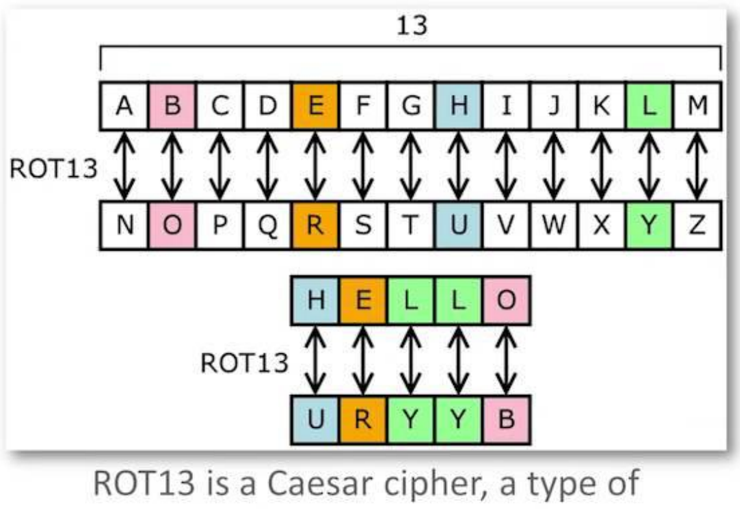
Method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth

Plaintext Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Keyword: Zebras

Ciphertext Alphabet: ZEBRASCDFGHIJKLMNOPQTUVWXY

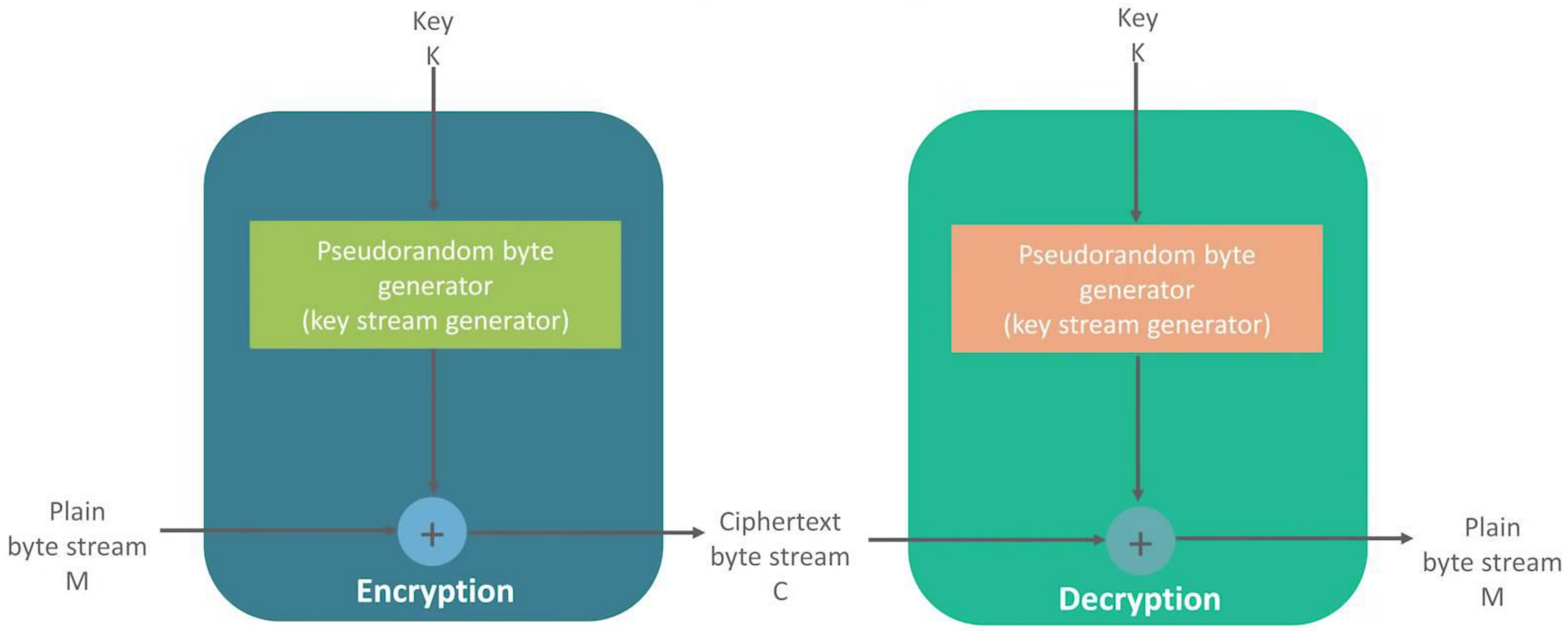
A message of: flee at once. We are discovered!
enciphers to: SIAA ZQ LKBA. VA ZOA RFPBLUAOAR!
SIAAZ QLKBA VAZOA RFPBL UAOAR



ROT13 is a Caesar cipher, a type of substitution cipher. In ROT13 alphabet is rotated 13 steps

Stream Cipher

A symmetric or secret-key encryption algorithm that encrypts a single bit at a time. With a Stream Cipher, the same plaintext bit or byte will encrypt to a different bit or byte every time it is encrypted



Block Cipher

An encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers