Classical Cryptography

Confusion vs Diffusion

Confusion = Substitute

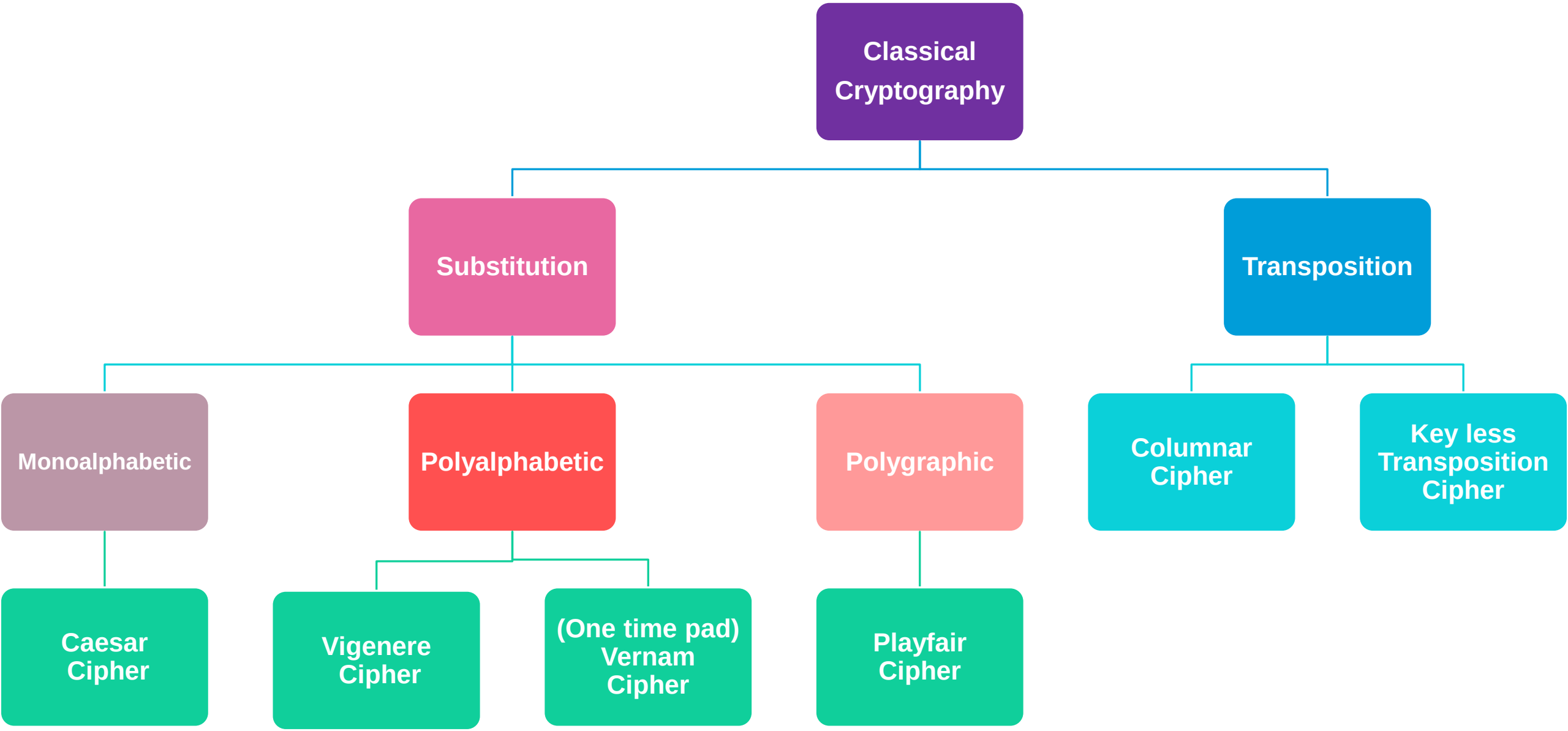
moon → prrq

Diffusion = Premutation or Transposition

moon → nomo

- **Confusion** is the relationship between the plaintext and ciphertext. it should be as random (confusing) as possible.
- **Substitution** replaces one character for another, this provides diffusion.
- **Diffusion** is how the order of the plaintext should be "diffused" (dispersed) in the ciphertext.
- **Permutation** or **transposition** provides confusion by rearranging the characters of the plaintext.

Classical Cryptography



Thank you