



Encrypting/ Decrypting

Programming Club Group #4

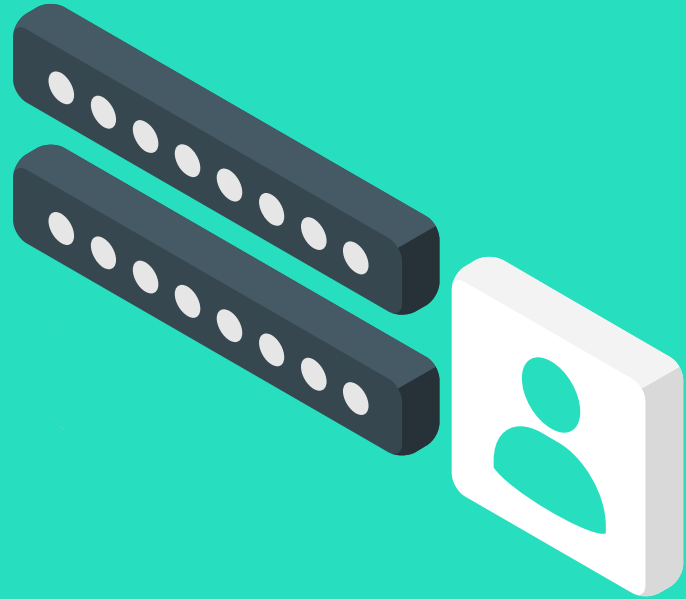
01 What is Cryptography?

Cryptography is a field where data is protected so that only intended recipients can understand what the data means. Encryption is a part of cryptography where letters are swapped based on some rule to hide the real meaning.



Caesar's Cipher

Caesar's Cipher is one of the oldest methods of encryption, where letters are shifted down the alphabet by some constant.



Caesar's cipher is very easy to decrypt through brute force; cycling through the possible amount the encrypted message was shifted by can even be done by hand. The few combinations is what makes it so vulnerable.

Attacking Caesar's Cipher



Substitution Cipher



A substitution cipher is where letters of the alphabet are replaced by another letter according to a fixed key. For example, in one key a could always be replaced by r.

Frequency Analysis



- **Cracking the substitution cipher**

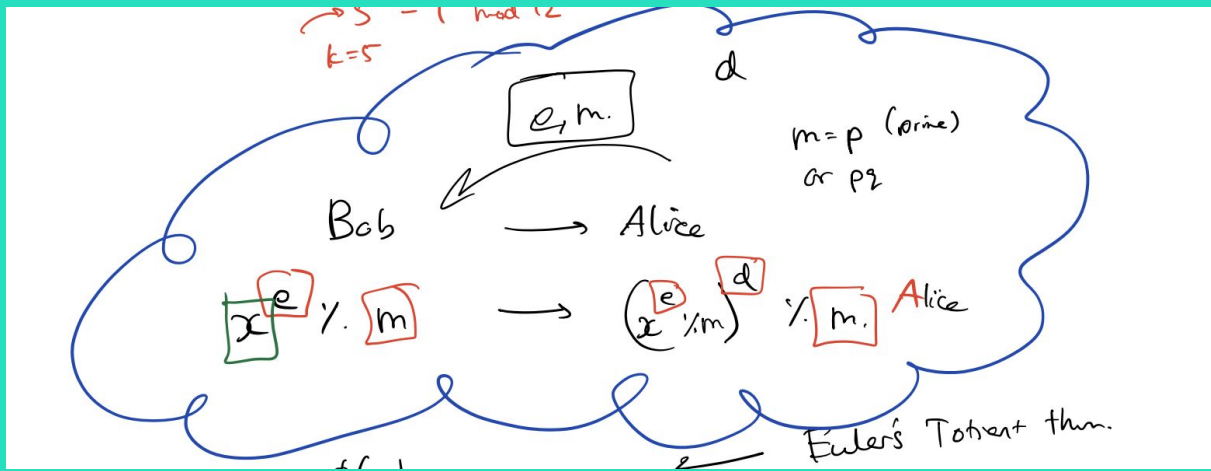
A frequency analysis can be run to try and crack the substitution cipher. In a nutshell, it compares the frequency of letters used in the English language to the encrypted message. Then it will try to match each letter to its counterpart, verifying if the resulting message is coherent.

Demonstration

We will now present to you a
live demonstration of a
frequency analysis done on a
substitution cipher scheme
that was implemented by our
group!



RSA Encryption/Decryption



We will do a quick overview of how RSA, a more complicated example of cryptography, works.

Thanks!



CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.

Please keep this slide for attribution.