**CYBER SECURITY 20CS54I**

**SUBMITTED BY SAI GIRISH.V**

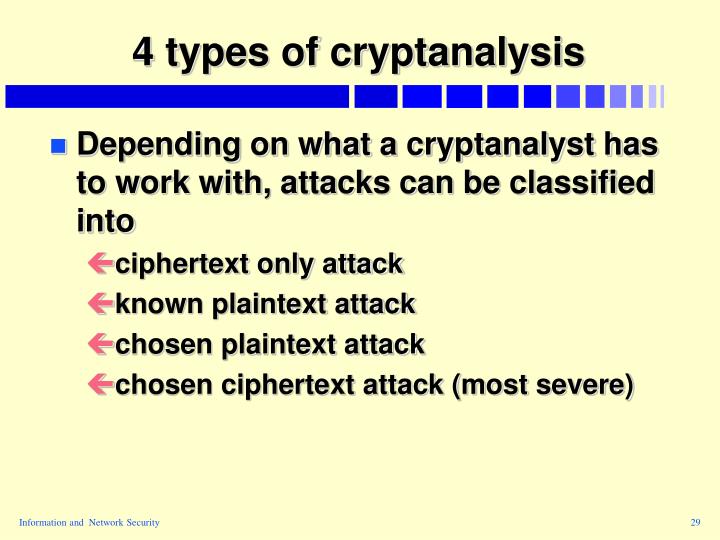
**CASE STUDY CRYPTANALYSIS**

**Information**

### What is cryptanalysis?

Cryptanalysis is the study of [ciphertext](https://www.techtarget.com/whatis/definition/ciphertext), ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them. For example, cryptanalysts seek to decrypt ciphertexts without knowledge of the [plaintext](https://www.techtarget.com/searchsecurity/definition/plaintext) source, encryption key or the algorithm used to encrypt it; cryptanalysts also target secure [hashing](https://searchsqlserver.techtarget.com/definition/hashing), digital signatures and other cryptographic algorithms.

**Types of cryptanalysis**



**How does** **cryptanalysis work**

Cryptanalysis is the art of**deciphering coded messages without being told the key**. To do this, hackers must break into cryptographic security systems to gain access to encrypted messages. Typically, cryptanalysis is only useful for hackers to obtain information illicitly.

**A hacks in cryptanalysis**

Brute force attack;The following is a list of the commonly used Cryptanalysis attacks;**Brute force attack** – this type of attack uses algorithms that try to guess all the possible logical combinations of the plaintext which are then ciphered and compared against the original cipher. This attacks are called**Cryptanalytic attacks**. The attacks rely on nature of the algorithm and also knowledge of the general characteristics of the plaintext, i.e., plaintext can be a regular document written in English or it can be a code written in Java. Therefore, nature of the plaintext should be known before trying to use the attacks.