



**TECHNO
INTERNATIONAL
BATANAGAR**



Topic Name: Difference Between Linear & Differential Cryptanalysis

SUBMITTED BY : KARTIK PAUL

ROLL NO. : 33200121007

YEAR : 4th YEAR (2021-2025)

BRANCH : CSE

SUBJECT : Cryptography & Network Security(PEC-CS801)

Introduction

Linear and Differential Cryptanalysis are two of the most powerful cryptanalysis techniques used to analyze symmetric-key ciphers, particularly block ciphers. Finds high-probability linear expressions that relate input and output bits. Finds high-probability differential characteristics to track propagation of differences.



Difference Between Linear & Differential Cryptanalysis

Cryptanalysis is the study of breaking cryptographic algorithms to analyze their security. Two widely known techniques are **Linear Cryptanalysis** and **Differential Cryptanalysis**, used primarily against block ciphers.

- ◆ **Linear Cryptanalysis** relies on statistical approximations and requires **known plaintexts**.
- ◆ **Differential Cryptanalysis** exploits input-output differences and requires **chosen plaintexts**.
- ◆ **Modern cryptographic algorithms** are designed to resist both by increasing **non-linearity, diffusion, and avalanche effects**.

Linear Cryptanalysis

- 1.** A **known-plaintext attack** that finds linear relationships between plaintext, ciphertext, and key bits.
- 2.** Uses **linear approximations** to predict encryption behavior.
- 3.** Requires a large number of **known plaintext-ciphertext pairs**
- 4.** First used effectively against **DES by Matsui in 1993**.

Example : If a cipher operation can be approximated as a linear equation, attackers can estimate key bits based on statistical analysis.

Differential Cryptanalysis

1. A **chosen-plaintext attack** that analyzes how input differences affect output differences.
2. Uses **probability distributions** of input-output differences to predict behavior.
3. Requires a large number of **chosen plaintext pairs** with specific differences.
4. First used against **DES & FEAL** by **Biham & Shamir** in **1990**.

Example : If changing one bit in the plaintext leads to a predictable change in ciphertext, attackers can exploit this to recover the key.



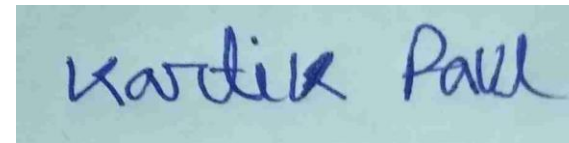
Conclusion

In conclusion, management studies play a vital role in the corporate scenario, offering numerous benefits to individuals, organizations, and the economy as a whole. By applying management studies principles, corporations can enhance competitiveness, improve customer satisfaction, increase employee engagement, drive innovation, and achieve sustainable growth.

DECLARATION

I hereby declare that this ppt is made by me only and not downloaded or copied from any other sources.

Date: 20.02.2025



Signature

Name : Kartik Paul

Roll NO : 33200121007