Requirement analysis

-first version-

**Project Overview:**

The project aims to develop a post-quantum cryptanalysis tool based on Stern's algorithm, with a focus on efficiently decoding linear codes. This tool will be designed to address cryptographic systems based on coding theory. It is expected to provide a minimal codeword as an output.

**Project Components:**

1. Selection of Cryptanalyst - Stern:
   * The project involves choosing Jacques Stern, a prominent cryptographer, to provide expertise and lead the development.
2. Post-Quantum Cryptosystem Attack:
   * The primary objective is to create an attack tool that can be applied to post-quantum cryptosystems.
   * The attack will be based on Stern's algorithm and will focus on decoding linear codes used in cryptographic systems.
3. Implementation on Large Matrices:
   * The project requires efficient implementation to handle large matrices commonly found in post-quantum cryptographic systems.
4. Preprocessing:
   * Preprocessing steps will be integrated into the tool to enhance the efficiency and effectiveness of the cryptanalysis process.
5. Completion of Cryptanalysis Tool:
   * The project will encompass the development of additional features and functionalities necessary for successful cryptanalysis.

**Technical Details:**

1. Cryptanalysis Approach:
   * Stern's algorithm will serve as the core technique for error correction and decoding of linear codes.
2. Use Case - Information Set Decoding:
   * The cryptanalysis tool will primarily target linear code decryption and will be applicable in cryptography systems based on coding theory.
3. Linear Equation Ax=s:
   * The tool will focus on solving linear equations of the form Ax=s, where A represents the parity-check matrix and s is the syndrome.
   * The solution must have specific weight constraints, either exactly matching a weight or falling below a certain weight limit.
4. Specific Parameter 't':
   * In the context of coding theory and cryptography, the project will address the problem of finding solutions to Ax=s such that the weight of the solution is exactly 't' or at most 't'.
5. Concrete Cryptanalysis:
   * The tool may include concrete attacks, exploiting specific vulnerabilities in cryptographic systems.

**Additional Project Aspects:**

* **Diagrams:**
  + Visual representations or diagrams will be created to illustrate the functioning and processes of the cryptanalysis tool.

**Project Scope and Goals:**

The project aims to develop a robust post-quantum cryptanalysis tool based on Stern's algorithm, catering to the decoding of linear codes in cryptographic systems. It will handle large matrices efficiently and provide solutions to linear equations with specific weight constraints. The tool may also include concrete attacks to enhance its effectiveness.

**Project Team:**

* BARBIR D. IUSTIN-ŞTEFĂNEL ([iustin\_barbir@yahoo.ro](mailto:iustin_barbir@yahoo.ro))
* NĂPÎRLICĂ V. MARIAN-DANIEL ([marian\_daniel\_14@yahoo.com](mailto:marian_daniel_14@yahoo.com))
* PRICOPI M.C. EDUARD-ANTONIO ([eduard.antonio2001@yahoo.com](mailto:eduard.antonio2001@yahoo.com))

This requirement analysis outlines the key components, technical aspects, and objectives of the project, ensuring a clear understanding of its scope and goals.