ELEC 572 Project – SHA-3 Cryptanalysis

The project goal is analyzing SHA-3 to:

- Generating a pre-image of an output truncated to 80 bits
- Generating a collision of an output truncated to 160 bits.

For:

KECCAK[c=160, r=b-c] with b = 200:

- The capacity is fixed to 160 bits: this implies a security level of 2^{80} against generic collision search.
- The width b of KECCAK-f[b] is 200: the width values that support the chosen capacity.
- The number of rounds n_r = 2.

The project is divided into SIX parts:

Part I: Theta Mapping Function (5 Marks)

- Generating a pre-image/collision of an output state array.

Part II: Rho Mapping Function (5 Marks)

- Generating a pre-image/collision of an output state array.

Part III: Pi Mapping Function (5 Marks)

- Generating a pre-image/collision of an output state array.

Part IV: Chi Mapping Function (5 Marks)

- Generating a pre-image/collision of an output state array.

Part V: Iota Mapping Function (10 Marks)

- Generating a pre-image/collision of an output state array for each round.

Part VI: Generating a pre-image/collision of an output truncated to 80/160 bits (30 Marks)

Note:

- Datasets will be provided for each part.
- Each group is free to choose pre-image or collision hash attack.
- Each group is free to use any Cryptographic (Analytic, Statistical, or any other) attack technique.
- Progress checkpoint (June 15).

Project Paths