Bez nazwy

Deadline: 11 Grudnia (Wstępny zarys)

Mateusz Szelecki:

- **Kontekst:** Historia konkursu NIST i dlaczego wybrano Keccak.
- **Architektura:** Opis stanu jako macierzy $5 \times 5 \times w$ (Keccak-f[1600]).
- **Rundy:** Wyjaśnienie liczby rund ($n_r = 24$).
- **Operacje Liniowe:** Opis matematyczny i cel operacji **Theta (θ)** (mieszanie kolumn) oraz **Rho (ρ) / Pi (π)** (permutacje).

Kacper Rothkegel:

- **Operacje Nieliniowe:** Opis kluczowej operacji **Chi (χ)** (nieliniowość) oraz stałej **Iota (ι)**.
- **Bezpieczeństwo:** Analiza odporności na ataki różnicowe, liniowe i algebraiczne.
- **Właściwości:** Opis znaczenia nieliniowości w ochronie przed atakami.

Deadline: 31 Grudnia (Implementacja w Python)

Mateusz Szelecki:

- Stworzenie szkieletu klasy Keccak i głównej pętli permutacji.
- Implementacja kodu funkcji liniowych: θ, ρ, π.

Kacper Rothkegel:

- Implementacja kodu funkcji nieliniowych i stałych: χ, ι.
- Weryfikacja poprawności implementacji przy użyciu oficjalnych wektorów testowych (Known Answer Tests).

Deadline: 15 Stycznia (Oddanie projektu)

Mateusz Szelecki:

- **Analiza parametrów:** Wnioski na temat wpływu zmniejszenia stanu (np. Keccak-f[800]) na bezpieczeństwo/wydajność.
- **Teoria dyfuzji:** Opis/wizualizacja teoretyczna rozprzestrzeniania się zmian w bitach (po 1, 2, 4 rundach).
- Złożenie całej dokumentacji teoretycznej i technicznej.

Kacper Rothkegel:

- **Eksperyment Lawinowy:** Skrypt zmieniający 1 bit stanu wejściowego i mierzący różnice w wyjściu.
- **Wizualizacja:** Wygenerowanie wykresu rosnącego: liczba rund vs odległość Hamminga.

Radosław Chruściński:

- Krótka charakterystyka pozostałych finalistów konkursu SHA-3
- Konstrukcja Sponge Function, faza absorbing i squeezing, diagram blokowy
- Znane słabości poprzednika (SHA-2), zestawienie SHA-3 vs SHA-2
- Implementacja kodu ataku kolizji na funkcję SHA-3 ze zredukowaną ilością rund