# Zadanie laboratoryjne nr 2

- Celem zadania jest wyznaczenie szybkości działania zaimplementowanej funkcji skrótu i sprawdzenie jej pseudolosowości.
- Wyznaczyć czasy obliczania funkcji skrótu dla wiadomości o następujących długościach:
  1. 0 bajtów;
  2. ok. 100 bajtów;
  3. ok. 1 kB;
  4. ok. 1 MB.
- Na podstawie uzyskanych wyników obliczyć przepustowość skracania (liczbę bajtów skracanych przez program w jednostce czasu) osobno dla każdego z podpunktów 2., 3., 4.

# Zadanie laboratoryjne nr 2

- Przeprowadzić sprawdzenie zachodzenia efektu lawinowości dla funkcji skrótu w następujący sposób:
  - ustalić pozycję testowanego bitu $k$ - wybrać numer bitu, który będzie negowany, pozycja może dowolna od 1 do długości skrótu $n$;
  - ustalić liczbę iteracji $r$ przy generowaniu pliku do testu losowości - plik do testu musi mieć co najmniej 1 GiB, tzn., że dla skrótu o długości $n$ bitów $r \geq 2^{30} * 8/n$;
  - ustalić wiadomość startową $m$ - może to być dowolny $n$-bitowy ciąg losowy, np. skrót pustej wiadomości;
  - powtórzyć $r$ razy:
    - obliczyć skrót $H(m)$;
    - obliczyć skrót wiadomości $H(m')$ otrzymanej przez zanegowanie w wiadomości $m$ bitu na ustalonej pozycji $k$;
    - obliczyć różnicę skrótów $H(m) \oplus H(m')$ i dołączyć ją do pliku do testu losowości;
    - za kolejną wiadomość przyjąć skrót poprzedniej;

# Zadanie laboratoryjne nr 2

- Otrzymany 1 GiB plik poddać testowi losowości pakietem dieharder, w tym celu:
  - na systemie operacyjnym Linux zainstalować pakiet dieharder;
  - przy jego pomocy przetestować losowość wygenerowanego pliku;
  - sprawdzić i omówić otrzymane wyniki - czy pojawiły się testy z wynikiem Fail, ile było testów z wynikiem Weak. Na tej podstawie stwierdzić, czy wygenerowany plik można uznać za ciąg losowy.
- Na podstawie przeprowadzonego testu losowości ocenić, czy zaimplementowana funkcja skrótu wykazuje efekt lawinowości dla wybranego bitu wejściowego.

# Zadanie laboratoryjne nr 2

- Sporządzić sprawozdanie zawierające:
  - tabelkę z czasami obliczania skrótów oraz przepustowościami dla wiadomości o różnych długościach;
  - ustalone parametry testowania pseudolosowości - pozycja bitu $k$ oraz liczba iteracji $r$;
  - wynik testu (rezultat działania pakietu dieharder dla wygenerowanego pliku) - w postaci zrzutów ekranu;
  - końcową ocenę zachodzenia efektu lawinowości.
- Sprawozdanie w formacie PDF (wraz z dodatkowymi programami, skryptami utworzonymi w ramach realizacji zadania) należy skompresować do jednego pliku ZIP. Plik ten przesyła się poprzez moduł Zadania MS Teams.