Zadanie laboratoryjne nr 3

- Celem zadania jest przeprowadzenie ataku znajdującego pierwszy przeciwobraz funkcji skrótu oraz ustalenie dla jakiej długości skrótu znalezienie pierwszego przeciwobrazu jest wykonalne dla konkretnej funkcji skrótu.
- Na podstawie wyznaczonych wcześniej przepustowości ustalić, ile wiadomości można skrócić w akceptowalnym czasie, np. 3 godzin.
- Na tej podstawie wyznaczyć długość skrótu w bajtach, dla której atak na pierwszy przeciwobraz będzie możliwy do przeprowadzenia w tym akceptowalnym czasie.

Zadanie laboratoryjne nr 3

- Dla tak ustalonej długości skrótu przeprowadzić atak na pierwszy przeciwobraz:
  1. wygenerować losowy skrót h o ustalonej długości;
  2. dla dowolnych (losowych) wiadomości m (o długości np. 100B) wyznaczać skróty $H(m)$, aż do otrzymania skrótu $H(m) = h$;
  3. jeżeli w założonym czasie nie uda się znaleźć takiej wiadomości, to zmniejszyć długość skrótu o 1 bajt i powtórzyć atak (dla tego samego h);
  4. jeżeli wiadomość o zadanym skrócie uda się znaleźć, to ustalić ile wiadomości trzeba było skrócić do momentu znalezienia szukanego pierwszego przeciwobrazu, a atak powtórzyć dla skrótu wydłużonego o 1 bajt, jeżeli taka długość nie była jeszcze atakowana.

Zadanie laboratoryjne nr 3

- Sporządzić sprawozdanie z wykonanego zadania, w którym znajdzie się:
  - oszacowana liczba skrótów, które można wyznaczyć w akceptowalnym czasie;
  - wyznaczona długość skrótu, dla której przeprowadzenie ataku na pierwszy przeciwobraz wydaje się wykonalne;
  - zadany losowy skrót h;
  - wszystkie znalezione przeciwobrazy (wiadomości), które dały zadany skrót - zrzuty ekranu, na których widać wiadomość i jej skrót - oraz liczbę skrótów wyznaczonych do znalezienia każdego z tych przeciwobrazów;
  - długosc skrótu, dla której atak na pierwszy przeciwobraz się nie powiódł - przekroczył akceptowalny czas wraz z liczbą skrótów, które wyznaczono do momentu przerwania.

Zadanie laboratoryjne nr 3

- 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.