Podstawy Ochrony Danych – laboratorium AGC
Funkcje skrótu

Cel ćwiczenia laboratoryjnego: zapoznanie się działaniem i własnościami jakie powinna posiadać dobra funkcja skrótu.

Materiały do laboratorium: materiały z wykładu

Przykład działania funkcji skrótu dla danego wejścia, dla pojedynczej zmiany 1 bitu na wejściu, na wyjściu zmieni się każdy bit z prawdopodobieństwem 0,5.

1. Fraza wejściowa: Kot (1001011 1101111 1110100)
   - MD5: c0d03d2d3e717da54ffdfc8a76c0f089
   - SHA-1: a0e5cd812455e04d6e33646cd8dc17e05b674231
   - SHA-2 (256): aedaac3e798149ebaec99435ea67f2ff1fc8b5cd2f3b039b885bdf8c04678c03

2. Fraza wejściowa: Kou (1001011 1101111 1110101)
   - MD5: 5aca6ec2885546912b2ea534d5225e60
   - SHA-1: f2c526b471623ac117ed27682b293f397c75ea4e
   - SHA-2 (256): f20417e10d864ea23cc002ced9e9aec51babf1aa8660054c36b870fa4a834784

Zadania:

1. Przygotuj aplikację, która pozwoli na wygenerowanie wartości skrótu zapisanego szesnastkowo na podstawie tekstowego wejścia, zadanego przez użytkownika. Skorzystaj z bibliotek natywnie dostępnych w wybranym środowisku programistycznym. Uwzględnij funkcje skrótu MD5, SHA-1, wszystkie warianty SHA-2 oraz SHA-3.
2. Porównaj szybkość działania poszczególnych funkcji oraz długość ciągów wyjściowych. Użyj zbioru danych wejściowych o zróżnicowanej długości.
3. Wygeneruj skrót dla słowa wejściowego, nie dłuższego niż 4 znaki. Skopiuj wartość uzyskaną dla funkcji MD5 i sprawdź, czy wartość wejściowa jest powszechnie znana. Co można powiedzieć o bezpieczeństwie skrótów z krótkich haseł składowanych w bazach danych?
4. Na podstawie powszechnie dostępnych źródeł odpowiedz na pytanie – czy funkcję MD5 można uznać za bezpieczną? Czy dotychczas zostały znalezione dla niej jakiekolwiek kolizje?
5. Dla wybranej przez siebie funkcji skrótu, zbadaj kolizje na pierwszych 12 bitach skrótu.
6. Losowość wyjścia funkcji skrótu (kryterium SAC – Strict Avalanche Criteria) – przy zmianie pojedynczego bitu na wejściu, wszystkie bity wyjściowe powinny zmienić się z prawdopodobieństwem 0,5 każdy. Dla wybranej funkcji skrótu zbadaj tę własność.

Sprawozdanie:
Sporządź sprawozdanie z zajęć. Powinno ono obejmować:

1. Screenshot z aplikacji.
2. Omówienie sposobu implementacji.
3. Określenie roli soli w tworzeniu skrótów.
4. Odpowiedź oraz jej uzasadnienie na pytanie postawione w pkt. 4.
5. Zestawienie uzyskanych wyników wraz ze stosownymi wnioskami.