|  |  |  |  |
| --- | --- | --- | --- |
| POLITECHNIKA LUBELSKA  Wydział Elektrotechniki i Informatyki  Informatyka | **Bezpieczeństwo Informacji**  **Prowadzący: dr Waldemar Suszyński** | | |
| Nazwisko i Imię | Semestr  IV | Rok akademicki  2023/2024 | Grupa:  IIST 4.5 |
| 1. |
| Data wykonania ćwiczenia: | GL 9 |
| Temat ćwiczenia:  SKRÓTY KRYPTOGRAFICZNE | | Data oddania sprawozdania: | OCENA: |

1. **Wykorzystanie algorytmów nieodwracalnej funkcji skrótu go generowania skrótu wiadomości.**



**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie**

Obraz zawierający tekst, zrzut ekranu, Czcionka, design

Opis wygenerowany automatycznie

Po wykonaniu poleceń zmienił się hash hasła dla użytkownika kubuntu. Przy zalogowaniu użyto hasła kubuntu. Taka metoda nie jest biezpieczna.

1. **Funkcje skrótu a bezpieczeństwo przechowywanych haseł.**

****

1. **Keyed Hash oraz HMAC**

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Nie, nie jest. Jednak przyjęło się by korzystać z konkretnych długości kluczy przy konkretnych funkcjach.

1. **Losowość nieodwracalnej funkcji skrótu.**

**Obraz zawierający tekst, Czcionka, oprogramowanie, Strona internetowa

Opis wygenerowany automatycznie**

1. **Bezpieczeństwo funkcji skrótu.**

Skróty różnią się w przypadku SHA256. W przypadku MD5 skróty są te same. Oznacza to że nie są bezpieczne. Nie użyłbym md5 do podpisu bo zbyt łatwo go podrobić.

1. **Nieodwracalność kontra odporność na kolizje (bonus)**

**-**