|  |  |  |  |
| --- | --- | --- | --- |
| 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:  KRYPTOGRAFIA SYMETRYCZNA, TRYBY PRACY ALGORYTMÓW KRYPTOGRAFICZNYCH | | Data oddania sprawozdania: | OCENA: |

1. **Generowanie haseł.**



Obraz zawierający Czcionka, Grafika, logo, typografia

Opis wygenerowany automatycznieObraz zawierający Czcionka, Grafika, typografia, logo

Opis wygenerowany automatycznieObraz zawierający Czcionka, Grafika, logo, symbol

Opis wygenerowany automatycznie****************Obraz zawierający tekst, zrzut ekranu, numer, linia

Opis wygenerowany automatycznie

1. **Generowanie haseł (PESELI).**

**Obraz zawierający tekst, zrzut ekranu, wyświetlacz

Opis wygenerowany automatycznie**

1. **Generator (nie?) losowy.**

Funkcja rand() w języku C++ generuje pseudolosowe liczby zmiennoprzecinkowe w zakresie od 0 do RAND\_MAX. Jednakże, sama w sobie nie jest odpowiednia do generowania kryptograficznie silnych kluczy, ponieważ jest to funkcja deterministyczna, która może generować te same sekwencje liczb, jeśli zostanie użyta z takim samym ziarnem. Z tego powodu nie jest zalecana do generowania kluczy kryptograficznych.

Generowanie pojedynczych bajtów klucza przy użyciu rand()%256 oznacza, że każdy bajt klucza będzie miał wartość od 0 do 255. Ogólnie rzecz biorąc, każdy bajt klucza jest generowany niezależnie od pozostałych**.**

Jeśli znane są tylko dwa pierwsze bajty klucza (0x51 i 0x9A), to nie można jednoznacznie określić reszty klucza. Skoro każdy bajt klucza jest niezależnie generowany, to istnieje 256 możliwych wartości dla każdego bajtu, co daje 256^6 możliwych kombinacji całego klucza z dwoma podanymi pierwszymi bajtami klucza.

Przechwycenie trzeciego bajta klucza (0xBD) również nie jest pomocne w znalezieniu całego klucza, ponieważ nieznacznie zmniejsza to pulę dostępnych możliwości.

1. **Zadanie 4.3. Powstawanie błędów w szyfrogramie.**