

Laboratorium nr 5-6

Metody podziału sekretu

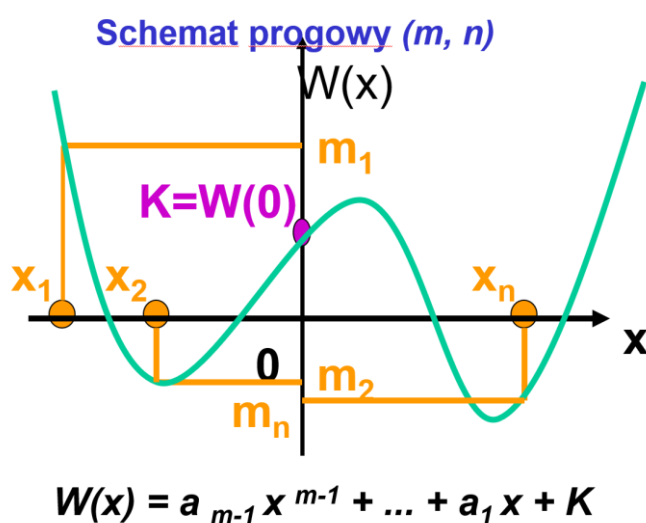
Termin wykonania: **do terminu laboratorium nr 7**

Liczba punktów: **6 + 4**

PRK: T-L-2

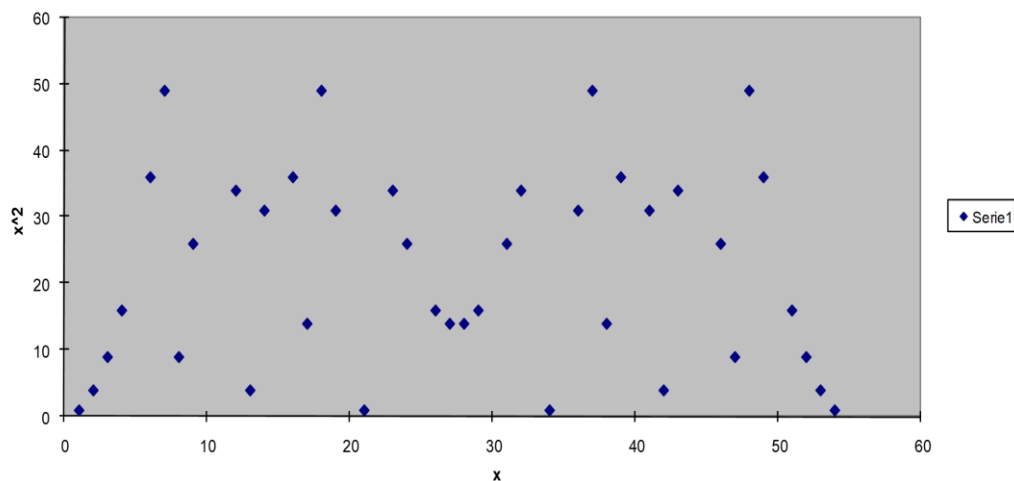
1. Opis laboratorium

Celem laboratorium jest implementacja i przebadanie metody podziału sekretu Shamir'a. Poniżej zamieszczono wizualizacje schematu progowego dla funkcji ciągłych oraz wizualizacje funkcji dyskretnych w ciałach skończonych (rysunki pochodzą z wykładu nr 3).



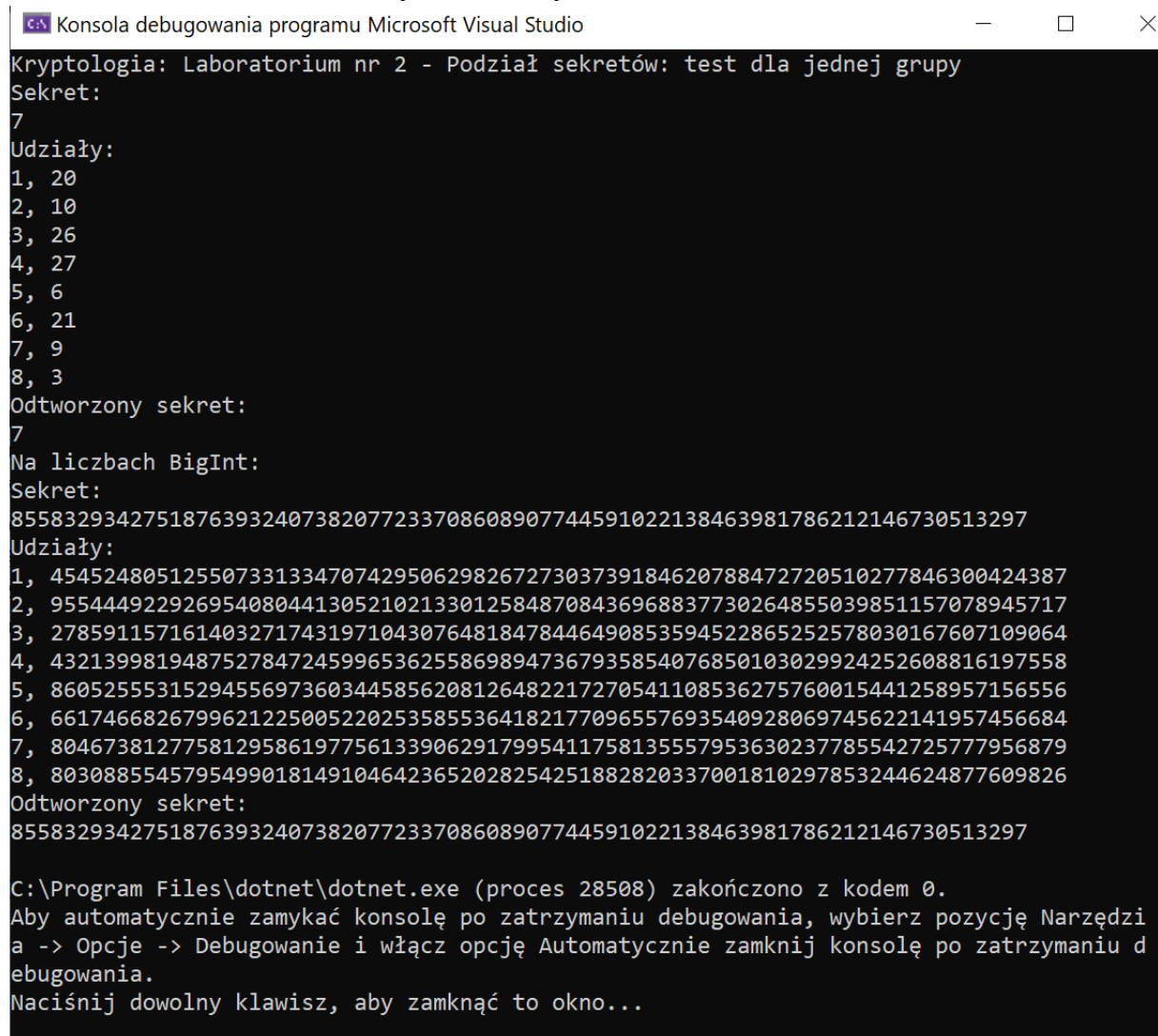
Praktyka – klasyczne komputery przetwarzają ciągi binarne, które można utożsamiać z liczbami całkowitymi

Wartości funkcji $f(x) = x^2$ w grupie multiplikatywnej Z_{55}^*



Wskazówki do wykonania zadania:

1. Na poniższym zrzucie ekranu pokazano częściowe rozwiązanie zadania, obliczanie cieni i odtwarzanie sekretu z użyciem metody A. Shamira:



```
Konsola debugowania programu Microsoft Visual Studio
Kryptologia: Laboratorium nr 2 - Podział sekretów: test dla jednej grupy
Sekret:
7
Udziały:
1, 20
2, 10
3, 26
4, 27
5, 6
6, 21
7, 9
8, 3
Odtworzony sekret:
7
Na liczbach BigInt:
Sekret:
85583293427518763932407382077233708608907744591022138463981786212146730513297
Udziały:
1, 45452480512550733133470742950629826727303739184620788472720510277846300424387
2, 95544492292695408044130521021330125848708436968837730264855039851157078945717
3, 27859115716140327174319710430764818478446490853594522865252578030167607109064
4, 43213998194875278472459965362558698947367935854076850103029924252608816197558
5, 86052555315294556973603445856208126482217270541108536275760015441258957156556
6, 66174668267996212250052202535855364182177096557693540928069745622141957456684
7, 80467381277581295861977561339062917995411758135557953630237785542725777956879
8, 80308855457954990181491046423652028254251882820337001810297853244624877609826
Odtworzony sekret:
85583293427518763932407382077233708608907744591022138463981786212146730513297

C:\Program Files\dotnet\dotnet.exe (proces 28508) zakończono z kodem 0.
Aby automatycznie zamykać konsolę po zatrzymaniu debugowania, wybierz pozycję Narzędzi
a -> Opcje -> Debugowanie i włącz opcję Automatycznie zamknij konsolę po zatrzymaniu d
ebugowania.
Naciśnij dowolny klawisz, aby zamknąć to okno...
```

2. Aby odtworzyć sekret (miejsce przecięcia z osią Y) nie trzeba odtwarzać całej funkcji.
3. Potęgowanie dużych liczb w ciele skończonym wymaga algorytmu potęgowania modularnego (pow mod).
4. Dzielenie liczb w ciele skończonym to obliczanie ich odwrotności. Służy do tego algorytm mod inverse . Algorytm ten przyjmuje jako wejście liczbę dodatnią. W przypadku, gdy mamy liczbę ujemną należy dodać do niej moduł.
5. Moduł musi być liczbą pierwszą, a w praktyce może być liczbą pierwszą z dużym prawdopodobieństwem.

2. Materiały

- Wykład nr 3 – większość informacji potrzebnych do wykonania zadania znajduje się w tym wykładzie
- J. Katz, Y. Lindell, Introduction to Modern Cryptography, Second Edition, CRC Press 2015
- http://iml.univ-mrs.fr/~kohel/tch/MATH3024/Lectures/lectures_11.pdf

3. Zadania do wykonania

Należy wykonać następujące zadania:

- 1) **Zadanie 5.1** (2 pkt + 2 pkt do terminu lab 5) – zaimplementuj przykład umieszczony w wykładzie na slajdach numer 9 i 10.
- 2) **Zadanie 5.2** (1 pkt) – uogólni przykład z zadania 1 tak, aby można było wybrać liczbę cieni (2-20) oraz wartość progową z zakresu 2 – 20. Sekretem jest liczba typu **int**.
- 3) **Zadanie 6.1** (2 pkt + 2 pkt do terminu lab 6) – ulepsz program z zadania 2 tak, aby argumentem była liczba typu **BigInt**
 - a) w tym zadaniu należy użyć biblioteki zawierającej obsługę liczb typu **BigInt**, np. dla C# polecana jest biblioteka BouncyCastle;
 - b) można korzystać z gotowych funkcji do obliczeń matematycznych, tj. odwrotność modulo, mnożenie modulo (w przypadku pobrania ich ze strony www lub wykładu należy w linijce przed daną funkcją w komentarzu umieścić jej pochodzenie).
- 4) **Zadanie 6.2** (1 pkt) – przetestuj czas odtwarzania sekretu dla trzech różnych rozmiarów cieni (tj. liczby *BigInt*) oraz trzech wybranych wartości progowych. Wynik umieść w tabeli. Podaj parametry komputera, na którym przeprowadzono testy. Odpowiedz na poniższe pytania:
 - a) Od czego zależy bezpieczeństwo metody podziału sekretu Shamir'a?
 - b) Czy w przypadku wykorzystania liczb typu *int* zaproponowana metoda będzie bezpieczna? Odpowiedź uzasadnij.