Podstawy kryptografii

Zastosowanie kryptografii asymetrycznej - protokół Diffiego-Hellmana

Adam Olech

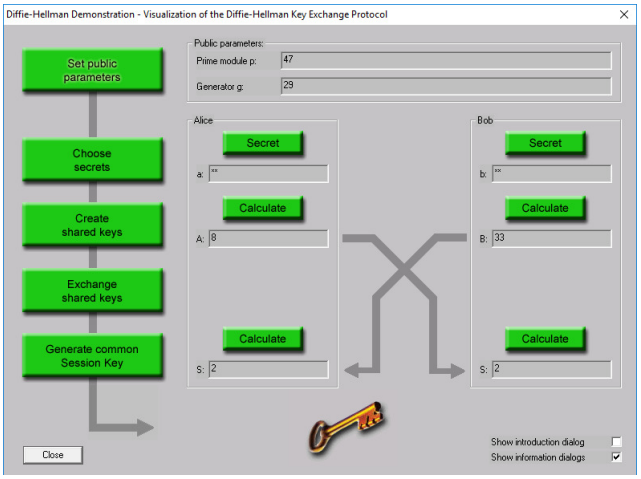
5 grudnia 2021

Spis treści

1 Wyniki eksperymentu z Cryptoolem

1.1 Moduł liczby pierwszej 47

W tym przegiegu użyto małej liczby pierwszej 47 oraz liczby generatora 29.



Alice wybrała swoją utajnioną liczbę a o wartości 16. Bob natomiast ustalił analogicznie liczbę b o wartości 31.
Na podstawie uprzednio wybranych liczb, Alice i Bob obliczają wartości, które wymienią miedzy sobą.
Za pomocą wymienionych miedzy sobą liczb, Alice i Bob w niezależny sposób są w stanie wyliczyć klucz sesyjny (obojgu powinien wyjść ten sam).

1.1.1 Weryfikacja obliczeniowa

$$p = 47, q = 29, a = 16, b = 31 \tag{1}$$

$$A = g^a \pmod p = 29^{16} \pmod{47} = 8 \tag{2}$$

$$B = g^b \pmod p = 29^{31} \pmod{47} = 33 \tag{3}$$

$$s_A = B^a \pmod p = 33^{16} \pmod{47} = 2 \tag{4}$$

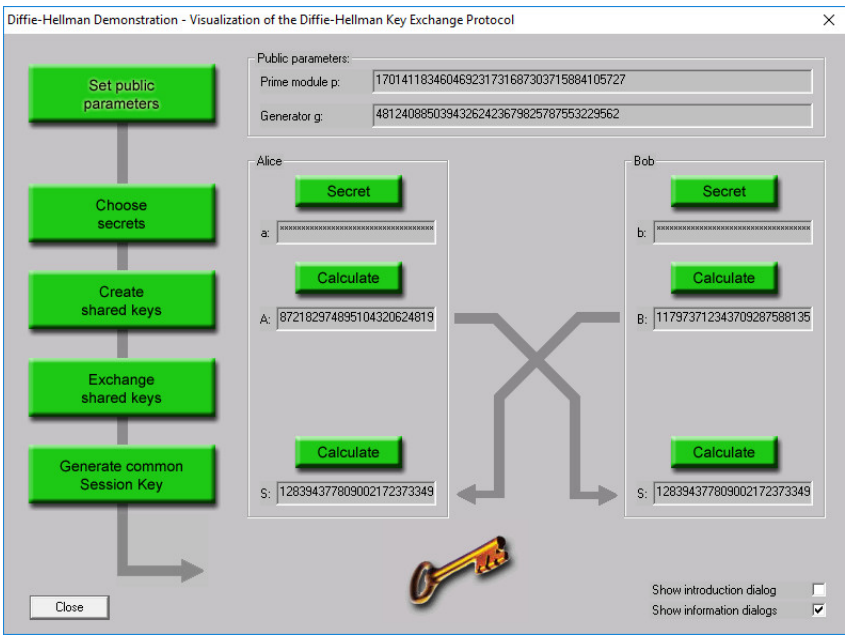
$$s_B = A^b \pmod p = 8^{31} \pmod{47} = 2 \tag{5}$$

1.2 Moduł dużej liczby pierwszej

W kolejnym przebiegu jako moduł p użyto następującej dużej liczby pierwszej odkrytej przez Édouarda Lucasa w 1876 roku:

$$170141183460469231731687303715884105727 \tag{6}$$

Liczba ta ma 39 cyfr.



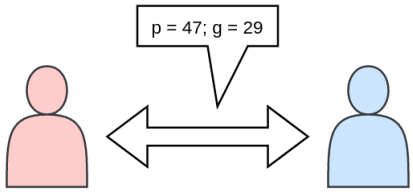
W wyniku działania programu uzyskano następujące wartości:

- **g**: 48124088503943262423679825787553229562
- **a**: 659633877059227199290710358487299325O2
- **b**: 830980141637211539966223306338057831 68
- **A**: 87218297489510432062481913308967573137
- **B**: 11797371234370928758813585338285474435 1
- **SA**: 12839437780900217237334993885632944480 3
- **SB**: 12839437780900217237334993885632944480 3

Obie wartości końcowe są takie same.

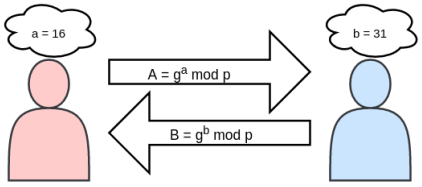
2 Opis protokołu Diffiego-Hellmana

Na początku komunikacji Alice i Bob wspólnie i jawnie uzgadniają, że będą używać danej liczby p oraz g (warto tutaj wspomnieć, że w przypadku biblioteki *OpenSSL* ten parametr domyślnie przyjmuje wartość 2). Ważne jest, by przy każdej kolejnej sesji używali innego zestawu liczb.



Rysunek 1: Uzgodnienie początkowych parametrów

Następnie, każde z nich z osobna wybiera tajną liczbę i przesyła do siebie nawzajem resztę z dzielnia liczby g podniesionej do potęgi tajnej liczby przez liczbę p.



Rysunek 2: Wysłanie liczb A i B

Na sam koniec, Alice i Bob oddzielnie wyliczają resztę z dzielnie otrzymanej liczby podniesionej do potęgi swojej tajnej liczby przez liczbę p. Wbrew naiwnej intuicji, pomimo różnych parametrów, oboje uzyskują tę samą liczbę.

Rysunek 3: Wysłanie liczb A i B

3 Wnioski

Protokół Diffiego-Hellmana rozwiązuje problem wymiany kluczy używanych w algorytmach kryptografii symetrycznej. Wygenerowany u obu stron ten sam sekret można użyć do zabezpieczenia dalszej komunikacji. Wcześniej takiej wymiany dokonywano fizycznie, w zaufany sposób, na przykład przy pomocy kuriera, co do którego należało być pewnym, że nie ma złych intencji.
Zastosowane są tutaj operacje arytmetyki modularnej, których odwrócenie jest kosztowne obliczeniowo.
Obie strony wysyłają do siebie informacje niezabezpieczonym kanałem, które dla postronnego obserwatora, z wyżej wymienionego powodu, są bezużyteczne.