Protokoły kryptograficzne
Podpisy niezaprzeczalne
Zadanie laboratoryjne 4.

5 maja 2021

1 Zadania

Zadania:

1. Zaimplementować w środowisku *sagemath* schemat podpisu niezaprzeczalnego (schemat przedstawiony w rozdziale 2.).

2 Opis schematu podpisu niezaprzeczalnego

Założenia:

- Znana jest publicznie liczba pierwsza p (charakterystyka ciała $\mathbb{F}_p$) oraz element pierwotny g ciała $\mathbb{F}_p$.
- Podpisujący posiada parę kluczy: prywatny x, gdzie $x \in < 1, \ldots, p-1 >$ spełnia $NWD(x, p-1) = 1$; publiczny $X = g^x \pmod p$.
- Wiadomość m reprezentowana jest jako liczna całkowita.

Opis algorytmu generacji podpisu:

1. Podpisujący **A** wyznacza podpis z pod wiadomością m obliczając

$$z = m^x \ (mod\ p).$$

Opis protokołu weryfikacji podpisu:

1. użytkownik **B** wybiera dwie liczby losowe a i b, obie mniejsze niż p i przesyła do użytkownika **A** wynik obliczeń:

$$c = m^a g^b \ (mod\ p),$$

2. użytkownik **A** wybiera liczbę losową q mniejszą od p, oblicza i przesyła do użytkownika **B** wyniki działań:

$$s_1 = c\ g^q \ (mod\ p), \quad s_2 = (c\ g^q)^x \ (mod\ p);$$

3. użytkownik **B** przesyła do **A** wartości a i b, tak więc użytkownik **A** może potwierdzić, że użytkownik **B** nie oszukiwał w kroku (1).

4. użytkownik **A** przesyła do **B** wartość q, więc użytkownik **B** może użyć z ($z = m^x \ (mod\ p)$) i obliczyć $\hat{s}_1$ i $\hat{s}_2$:

$$\hat{s}_1 = c\ g^q \ (mod\ p), \quad \hat{s}_2 = (X)^{b+q} z^a \ (mod\ p)$$

Jeżeli $\hat{s}_1 == s_1$ i $\hat{s}_2 == s_2$, to podpis jest poprawny. W przeciwnym przypadku podpis nie jest poprawny.

3 Wytyczne

W ramach zadania należy zaimplementować procedury realizujące następujące elementy:

1. procedurę generacji pary kluczy prywatny/publiczny zgodnie z założeniami z rozdziału 2.,
2. procedurę generacji podpisu,
3. protokół weryfikacji podpisu.

Parametrami wejściowymi są: wiadomość do podpisu m, liczność ciała w bitach b.

3.1 Polecenia środowiska *sagemath*

Biblioteki i polecenia środowiska *sagemath*, które można wykorzystać przy realizacji zadania:

- deklaracja ciała prostego: `F=GF(p)`
- generacja losowego elementy z ciała: `a=F.random_element()`
- wyznaczenie elementu pierwotnego ciała $\mathbb{F}_p$: `b=F.primitive_element()`

4 Rozliczenie zadań

W celu rozliczenia zadania należy przesłać w ramach narzędzia $MicrosoftTeams$ jeden plik tekstowy (koniecznie format txt) zawierający:

- kody zaimplementowanych funkcji;
- sekwencję wywołań funkcji realizujących kroki protokołu:
  - numer kroku z informacją, która strona go realizuje,
  - jakie wartości zostały w danym kroku wyznaczone (z wypisaniem tych wartości),
  - co jest wysyłane do innych uczestników protokołu (również z wypisaniem wartości).

Na początku pliku w komentarzu proszę umieścić własne dane (imię, nazwisko, grupa szkoleniowa). Zaimplementowane procedury jak i wykonywane kroki muszą byś opatrzone komentarzami (w kodzie źródłowym).