Protokoły kryptograficzne
Podział Wiadomości Poufnych
Zadanie laboratoryjne 3a.
Zadanie laboratoryjne 3b.

22 kwietnia 2021

1 Zadania

Zadania:

1. Zaimplementować w środowisku *sagemath* schemat z wielomianem interpolacyjnym Lagrange'a (zadanie 3a.).
2. Zaimplementować w środowisku *sagemath* schemat Karnina-Greene'a-Hellmana (zadanie 3b.).

2 Opis protokołów

2.1 Schemat z wielomianem interpolacyjnym Lagrange'a

Kroki protokołu: Mamy wiadomość M, którą chcemy podzielić, w tym celu wykonujemy czynności:

1. Wybieramy liczbę pierwszą p, która jest większa niż liczba możliwych cieni i większa niż wartość tajemnicy, która ma być współdzielona.
2. Generowany jest dowolny wielomian stopnia $k-1$ (dla k z n osób uprawnionych do odtworzenia wiadomości) postaci:

   $$f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1 x + M \ (mod\ p)$$

   gdzie współczynniki $a_{k-1}, a_{k-2}, \ldots, a_1 \in \mathbb{Z}_p$ są wybrane losowo i utrzymane w tajemnicy. Są zapominane po wydaniu cieni osobom upoważnionym, natomiast p jest ujawniane.
3. Wyznaczamy cienie poprzez wyznaczenie wartości wielomianu w n różnych punktach $x_i \in \mathbb{Z}$, $x_i > 0$:

   $$l_i = f(x_i)$$

4. Wysyłamy to poszczególnych użytkowników systemu x_i, odpowiadającą jej wartość l_i oraz liczbę pierwszą p.

5. Do wyznaczenia M musi się zebrać dowolny podzbiór k osób posiadających cienie. Mogą one wtedy wyznaczyć $a_{k-1}, a_{k-2}, \ldots, a_1$ oraz M poprzez odtworzenie postaci wielomianu $f(x)$ (rozwiązanie układu k kongruencji z k niewiadomymi $a_{k-1}, a_{k-2}, \ldots, a_1$ i M).

2.2 Schemat Karnina-Greene'a-Hellmana

Założenia:

- Działania wykonujemy w ciele $\mathbb{F}_{q^m}$.
- Wybieramy element pierwotny α ciała $\mathbb{F}_{q^m}$.
- Przez α_i oznaczamy α^i (α_i^j oznacza $(\alpha^i)^j$).
- Ciało $\mathbb{F}_{q^m}$ oraz element α znane są wszystkim uczestnikom protokołu.
- Przez M oznaczać będziemy tajemnicę reprezentowaną jako element ciała $\mathbb{F}_{q^m}$.

Opis protokołu (Generacja cieni):

1. Zaufana strona wybiera losowo elementy $a_1, a_2, \ldots, a_{k-1} \in \mathbb{F}_{q^m}$.
2. Zaufana strona wyznacza n cieni s_i $(i = 1, \ldots, n)$ w następujący sposób

$$\begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_{n-1} \\ s_n \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{k-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_{n-1} & \alpha_{n-1} & \ldots & \alpha_{n-1}^{k-1} \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} \begin{pmatrix} M \\ a_1 \\ a_2 \\ \vdots \\ a_{k-1} \end{pmatrix}$$

3. Zaufana strona przesyła cienie (i, s_i) w sposób poufny uczestnikom systemu.

Opis protokołu (Odtwarzanie tajemnicy):

1. Uczestnicy $i_1, i_2, \ldots, i_k$ wyznaczają macierz

$$D = \begin{pmatrix} 1 & \alpha_{i_1} & \alpha_{i_1}^2 & \ldots & \alpha_{i_1}^{k-1} \\ 1 & \alpha_{i_2} & \alpha_{i_2}^2 & \ldots & \alpha_{i_2}^{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_{i_k} & \alpha_{i_k} & \ldots & \alpha_{i_k}^{k-1} \end{pmatrix}, \quad i_j \neq n$$

albo

$$D = \begin{pmatrix} 1 & \alpha_{i_1} & \alpha_{i_1}^2 & \ldots & \alpha_{i_1}^{k-1} \\ 1 & \alpha_{i_2} & \alpha_{i_2}^2 & \ldots & \alpha_{i_2}^{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_{i_{k-1}} & \alpha_{i_{k-1}} & \ldots & \alpha_{i_{k-1}}^{k-1} \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}, \quad i_k = n$$

2. Następnie na podstawie k cieni $s_{i_1}, s_{i_2}, \ldots, s_{i_k}$wyznaczają tajemnicę

$$\begin{pmatrix} M \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix} = D^{-1} \begin{pmatrix} s_{i_1} \\ s_{i_2} \\ \vdots \\ s_k \end{pmatrix}$$

3 Wytyczne

3.1 Schemat z wielomianem interpolacyjnym Lagrange'a

W ramach zadania należy zaimplementować procedury realizujące następujące elementy:

1. procedurę generację cieni.
2. protokół odtwarzania tajemnicy.

Parametrami wejściowymi są: tajemnica do podziału M, parametry schematu k i n.

3.2 Schemat Karnina-Greene'a-Hellmana

W ramach zadania należy zaimplementować procedury realizujące następujące elementy:

1. procedurę generację cieni.
2. protokół odtwarzania tajemnicy.

Parametrami wejściowymi są: tajemnica do podziału M, ciało $\mathbb{F}_{q^m}$ oraz element α, parametry schematu k i n.

3.3 Polecenia środowiska *sagemath*

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

- deklaracja ciała prostego: `F=GF(p)`
- generacja lodowego elementy z ciała: `a=F.random_element()`
- deklaracja pierścienia wielomianów nad ciałem: `P=PolynomialRing(F,'x')` lub `P.<x>=F[]`
- deklaracja wielomianu z pierścienia P: `f=x**3+5*x**2+7`
- wyznaczenie wartości wielomianu f dla $x = 2$: `y=f(2)`
- deklaracja ciała $\mathbb{F}_{q^m}$: `G.<a>=GF(q**m)`
- wyznaczenie elementu pierwotnego ciała $\mathbb{F}_{q^m}$: `b=G.primitive_element()`
- deklaracja macierzy zerowej o wymiarach m na n nad ciałem F: `A=zero_matrix(F,m,n)`
- wyznaczenie macierzy odwrotnej do macierzy kwadratowej: `Ainv=A.inverse()`
- deklaracja zerowego wektora o długości n nad ciałem F: `B=zero_vector(F,n)`
- deklaracja wektora nad ciałem F: `B=vector(F,[1,2,3])`
- wykonanie mnożenia macierzy A i wektora B ($A \cdot B$): `X=A*B` lub `A.solve_right(B)`

4 Rozliczenie zadań

W celu rozliczenia zadań należy przesłać w ramach narzędzia $MicrosoftTeams$ dla każdego z zaimplementowanych protokołów 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 każdego z plików w komentarzu proszę umieścić własne dane (imię, nazwisko, grupa szkoleniowa). Zaimplementowane procedury jak i wykonywane kroki muszą byś opatrzone komentarzami (w kodzie źródłowym).

Wymagania dotyczące przesyłania rozwiązań

- Realizacja schematu z wielomianem interpolacyjnym Lagrange'a jest w ramach „Zadania 3a".
- Realizacja schematu Karnina-Greene'a-Hellmana rozliczana jest w ramach „Zadania bb".