Nowoczesne Technologie WWW

semestr zimowy 2019/20

Lista nr 4

Termin realizacji:

całość: oddana na laboratorium przed upływem 19.12.2019

Zadania:

Zadanie 1. (30pkt łącznie) Wykorzystując poznane dotąd technologie stwórz stronę www - „Zakamarki kryptografii” prezentującą ładnie dwa poniższe zagadnienia kryptograficzne:

1. Algorytm szyfrowania probabilistycznego Goldwasser-Micali oraz niezbędne do zrozumienia go symbol Legendre'a oraz symbol Jacobiego, ich własności oraz algorytm ich wyliczania a także definicje reszty i niereszty kwadratowej modulo n.
2. Schemat progowy dzielenia sekretu Shamira ze wzorem na interpolację Lagrange'a i przykładem policzonym ręcznie dla niedużych liczb.

Wykorzystaj poniższe materiały (choć nie musisz się do nich ograniczać) i postaraj się odwzorować podobnie użyte konstrukcje.

Materiały do wykorzystania:

1. Schemat Goldwasser-Micali szyfrowania probabilistycznego

Algorytm generowania kluczy

(a) Wybierz losowo dwie duże liczby pierwsze p oraz q (podobnego rozmiaru),

(b) Policz $n = pq$,

(c) Wybierz $y \in \mathbb{Z}_n$, takie, że y jest nieresztą kwadratową modulo n i symbol Jacobiego $\left(\frac{y}{n}\right) = 1$ (czyli y jest pseudokwadratem modulo n),

(d) Klucz publiczny stanowi para (n, y), zaś odpowiadający mu klucz prywatny to para (p, q).

Algorytm szyfrowania

Chcąc zaszyfrować wiadomość m przy użyciu klucza publicznego (n, y) wykonaj kroki:

(a) Przedstaw m w postaci łańcucha binarnego $m = m_1 m_2 \ldots m_t$ długości t

(b) `For` i `from` 1 `to` t `do`
   `wybierz losowe` $x \in \mathbb{Z}_n^*$
   `If` $m_i = 1$ `then set` $c_i \leftarrow yx^2 \bmod n$
   `Otherwise set` $c_i \leftarrow x^2 \bmod n$

(c) Kryptogram wiadomości m stanowi $c = (c_1, c_2, \ldots, c_t)$

Algorytm deszyfrowania

Chcąc odzyskać wiadomość z kryptogramu c przy użyciu klucza prywatnego (p, q) wykonaj kroki:

(a) `For` i `from` 1 `to` t `do`
   `policz symbol Legendre'a` $e_i = \left(\frac{c_i}{p}\right)$ `(algorytm 3)`
   `If` $e_i = 1$ `then set` $m_i \leftarrow 0$
   `Otherwise set` $m_i \leftarrow 1$

(b) Zdeszyfrowana wiadomość to $m = m_1 m_2 \ldots m_t$

2. Reszta/niereszta kwadratowa

Definicja. Niech $a \in \mathbb{Z}_n$. Mówimy, że a jest *resztą kwadratową modulo* n (*kwadratem modulo* n), jeżeli istnieje $x \in \mathbb{Z}_n^*$ takie, że $x^2 \equiv a \pmod{p}$. Jeżeli takie x nie istnieje, to wówczas a nazywamy *nieresztą kwadratową modulo* n. Zbiór wszystkich reszt kwadratowych modulo n oznaczamy Q_n, zaś zbiór wszystkich nieresztkwadratowych modulo n oznaczamy $\overline{Q}_n$.

3. Symbol Legendre'a i Jacobiego

Definicja. Niech p będzie nieparzystą liczbą pierwszą a a liczbą całkowitą. *Symbol Legendre'a* $\left(\frac{a}{p}\right)$ jest zdefiniowany jako:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{jeżeli } p|a \\ 1 & \text{jeżeli } a \in Q_p \\ -1 & \text{jeżeli } a \in \overline{Q}_p \end{cases}$$

Własności symbolu Legendre'a. Niech $a, b \in \mathbb{Z}$, zaś p to nieparzysta liczba pierwsza. Wówczas:

- $\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}} \pmod{p}$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
- $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}$
- Jeżeli q jest nieparzystą liczbą pierwszą inną od p to:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$$

Definicja. Niech $n \geqslant 3$ będzie liczbą nieparzystą a jej rozkład na czynniki pierwsze to $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. *Symbol Jacobiego* $\left(\frac{a}{n}\right)$ jest zdefiniowany jako:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k}.$$

Jeżeli n jest liczbą pierwszą, to symbol Jacobieo jest symbolem Legendre'a.

Własności symbolu Jacobiego. Niech $a, b \in \mathbb{Z}$, zaś $m, n \geqslant 3$ to nieparzyste liczby całkowite. Wówczas:

- $\left(\frac{a}{n}\right) = 0, 1, \text{albo} - 1$. Ponadto $\left(\frac{a}{n}\right) = 0 \iff \gcd(a, n) \neq 1$
- $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
- $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
- $a \equiv b \pmod{n} \Longrightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
- $\left(\frac{1}{n}\right) = 1$
- $\left(\frac{-1}{n}\right) = (-1)^{\frac{(n-1)}{2}}$
- $\left(\frac{2}{n}\right) = (-1)^{\frac{(n^2-1)}{8}}$
- $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{(m-1)(n-1)}{4}}$

Z własności symbolu Jacobiego wynika, że jeżeli n nieparzyste oraz a nieparzyste i w postaci $a = 2^e a_1$, gdzie a_1 też nieparzyste to:

$$\left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right)\left(\frac{a_1}{n}\right) = \left(\frac{2}{n}\right)^e \left(\frac{n \bmod a_1}{a_1}\right)(-1)^{\frac{(a_1-1)(n-1)}{4}}$$

Algorytm obliczania symbolu Jacobiego $\left(\frac{a}{n}\right)$ (i Legendre'a) dla nieparzystej liczby całkowitej $n \geqslant 3$ oraz całkowitego $0 \leqslant a < n$

`JACOBI`(a, n)

(a) `If` $a = 0$ `then return 0`

(b) `If` $a = 1$ `then return 1`

(c) `Write` $a = 2^e a_1$, `gdzie` a_1 `nieparzyste`

(d) `If` e `parzyste set` $s \leftarrow 1$
`Otherwise set` $s \leftarrow 1$ `if` $n \equiv 1$ or $7 \pmod{8}$, `or set` $s \leftarrow -1$ `if` $n \equiv 3$ or $5 \pmod{8}$

(e) `If` $n \equiv 3 \pmod{4}$ `and` $a_1 \equiv 3 \pmod{4}$ `then set` $s \leftarrow -s$

(f) `Set` $n_1 \leftarrow n \bmod a_1$

(g) `If` $a_1 = 1$ `then return s`
`Otherwise return` $s \cdot$`JACOBI`(n_1, a_1)

Algorytm działa w czasie $\mathcal{O}\left((\lg n)^2\right)$ operacji bitowych.

4. Schemat progowy (t, n) dzielenia sekretu Shamira

Cel: Zaufana Trzecia Strona T ma sekret $S \geqslant 0$, który chce podzielić pomiędzy n uczestników tak, aby dowolnych t spośród nich mogło sekret odtworzyć.

Faza inicjalizacji:

- T wybiera liczbę pierwszą $p > \max(S, n)$ i definiuje $a_0 = S$,
- T wybiera losowo i niezależnie $t-1$ współczynników $a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$,
- T definiuje wielomian nad $\mathbb{Z}_p$:

$$f(x) = a_0 + \sum_{j=1}^{t-1} a_j x^j,$$

- Dla $1 \leqslant i \leqslant n$ Zaufana Trzecia Strona T wybiera losowo $x_i \in \mathbb{Z}_p$, oblicza: $S_i = f(x_i) \mod p$ i bezpiecznie przekazuje parę (x_i, S_i) użytkownikowi P_i.

Faza łączenia udziałów w sekret: Dowolna grupa t lub więcej użytkowników łączy swoje udziały - t różnych punktów (x_i, S_i) wielomianu f i dzięki interpolacji Lagrange'a odzyskuje sekret $S = a_0 = f(0)$.

5. Interpolacja Lagrange'a

Mając dane t różnych punktów (x_i, y_i) nieznanego wielomianu f stopnia mniejszego od t możemy policzyć jego współczynniki korzystając ze wzoru:

$$f(x) = \sum_{i=1}^{t} \left(y_i \prod_{1 \leqslant j \leqslant t,\, j \neq i} \frac{x - x_j}{x_i - x_j} \right) \mod p$$

Wskazówka: w schemacie Shamira, aby odzyskać sekret S, użytkownicy nie muszą znać całego wielomianu f. Wstawiając do wzoru na interpolację Lagrange'a $x = 0$, dostajemy wersję uproszczoną, ale wystarczającą aby policzyć sekret $S = f(0)$:

$$f(x) = \sum_{i=1}^{t} \left(y_i \prod_{1 \leqslant j \leqslant t,\, j \neq i} \frac{x_j}{x_j - x_i} \right) \mod p$$