Laboratorium

Wybrane zagadnienia kryptograficzne

2020/2021

Anna Grocholewska-Czuryło
Politechnika Poznańska

Informacje ogólne

mail: anna.grocholewska-czurylo@put.poznan.pl

pok. 733
konsultacje: wtorek 14-15,
albo uzgodnione wcześniej mailowo on-line

Laboratorium: 15h
Wykład: 15h

Kolokwium zaliczeniowe z wykładów.
Laboratorium: ocena wykonanych ćwiczeń laboratoryjnych.

Tematyka wykładów

- Szyfrowanie symetryczne
  - Szyfry blokowe - komponenty szyfrów blokowych,
  - tryby pracy szyfrów ECB, CBC, OFB, CTR,
  - Szyfry strumieniowe,
  - Kryptoanaliza szyfrów blokowych
- Szyfrowanie asymetryczne
  - RSA,
  - RSAES-OAEP - optimal asymmetric encryption padding,
  - Ataki na RSA,
  - Podpis cyfrowy DSS, Ataki na podpis,
  - D-H,
  - Krzywe eliptyczne
- Integralność
  - Funkcje skrótu, MDC, MAC, Rodzaje funkcji skrótu, Ataki na funkcje skrótu, CMAC, GCM, CCM
- Certyfikaty i PKI
  - Ogólny problem klucza publicznego, Modele zaufania, X.509, Odwołanie certyfikatu,
  - Jak zabezpieczyć algorytm D-H, Ataki na certyfikaty 2008
- Uwierzytelnianie
  - Metody i protokoły uwierzytelniania, Metody uzgadniania klucza sesyjnego, Ataki na protokoły uzgadniania klucza

Literatura

Ochrona danych i zabezpieczenia w systemach teleinformatycznych, prac. zbiorowa pod red. J. Stokłosy, WPP

Kryptografia i ochrona danych, Dorothy E. R. Denning, WNT

Kryptografia dla praktyków, Bruce Schneier

Teoria bezpieczeństwa systemów komputerowych, Pieprzyk J., Hardjono T., Seberry J.

Kryptografia stosowana, Menezes A. at all

Narzędzia

- Implementacje programów - można korzystać z dowolnego języka programowania
- Korzystanie z gotowych funkcji kryptograficznych dostępnych w danym języku - określa prowadzący, w zależności od konkretnego zadania do wykonania

Tematyka poszczególnych zajęć

1. Zajęcia organizacyjne - zadanie na rozgrzewkę: Podział sekretu
2. Szyfry blokowe - tryby pracy szyfrów blokowych
3. Generatory ciągów losowych - implementacja algorytmu BBS i testy losowości ciągów (NIST/FIPS)
4. Kryptografia asymetryczna - implementacja algorytmu RSAi algorytmu Diffiego-Helmana - wyznaczania wspólnego klucza

Tematy cd..

5. Badanie własności funkcji skrótu
6. Steganografia - algorytm najmniej znaczącego bitu
7. Kryptografia wizualna - graficzny podział sekretu
8. ....

Oceny

- oceniane będą zaimplementowane algorytmy/sprawozdania z tych implementacji (szczegółowe warunki będą podawane przy każdym zadaniu - różne stopnie trudności/dodatkowe funkcje dla chętnych)
- termin oddania
- ważnym elementem w sprawozdaniu są wnioski z ćwiczenia/implementacji
- prace/sprawozdania takie same lub podobne otrzymują ocenę 2.0

Nazewnictwo plików

- Wymagane jest następujące stosowanie nazewnictwa plików:
- Imie_Nazwisko_grupa_NrĆwiczenia.pdf
-

Reguły udziału w zajęciach laboratoryjnych

- włącz swoją kamerkę podczas zajęć laboratoryjnych
- używaj podniesionej ręki - żeby zgłosić chęć powiedzenia czegoś
- upewnij się, że masz wyłączony mikrofon, wtedy kiedy nie mówisz

Anna Grocholewska-Czuryło

Podział sekretu
Zadanie na rozgrzewkę

Sekret

Sekret

- hasło do ważnego zasobu np. systemu operacyjnego,
- symetryczny klucz służący do szyfrowania i deszyfrowania danych,
- asymetryczny klucz prywatny używany do cyfrowego podpisywania wiadomości.

Pierwsze protokoły opracowali: Adi Shamir i George Blackley w 1979

Podział sekretu

Podział sekretu - protokół kryptograficzny, złożony z pary algorytmów:

- rozdzielającego
- łączącego

Podział realizowany jest z zachowaniem następujących wymogów:

- wymóg poprawności - co najmniej t spośród n udziałów pozwala na odtworzenie sekretu s
- wymóg prywatności - znajomość mniejszej liczby niż t spośród n udziałów uniemożliwia wyznaczenie s

Jest to protokół (t,n) - progowy,
n - to udziały

Zastosowania

- Zarządzanie kluczami kryptograficznymi - do zabezpieczenia transakcji elektronicznych
- Uwierzytelnianie - autoryzowana grupa użytkowników potwierdza swoją tożsamość
- Np. do kontroli strategicznej broni nuklearnej - Federacja Rosyjska

Klasyfikacja metod

1. Trywialne (ang. *trivial secret sharing*)- metody należące do tej grupy umożliwiają podział sekretu w taki sposób, że wszystkie wygenerowane udziały są konieczne do jego odtworzenia $(t = n)$.

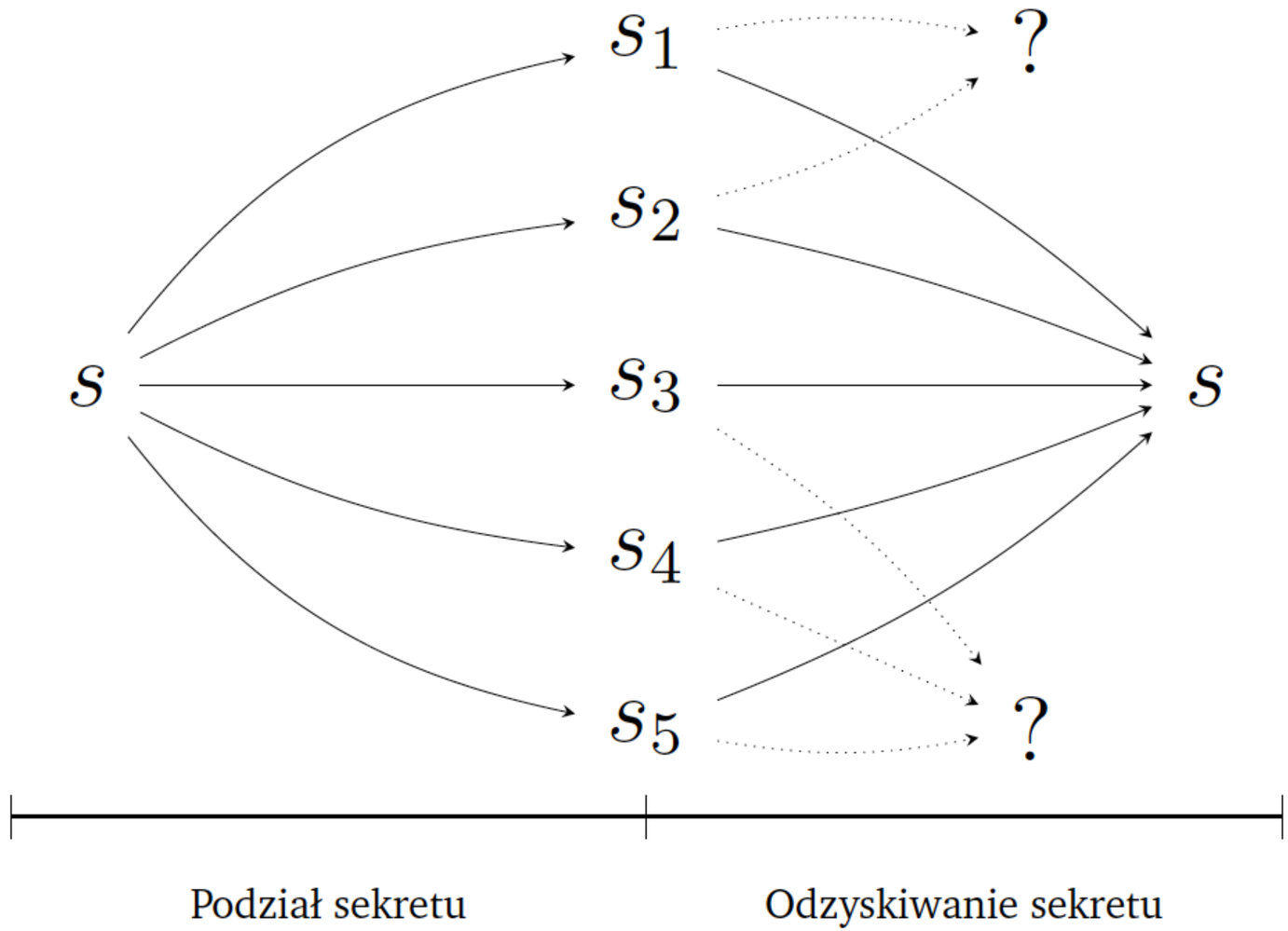
2. Efektywne (ang. *efficient secret sharing*) - korzystając z tego rodzaju metod można podzielić sekret w taki sposób, że nie wszystkie jego fragmenty będą potrzebne do jego rekonstrukcji $(t \leqslant n)$.

Klasyfikacja metod cd.

3. Weryfikowalne (ang. *verifiable secret sharing*) - mogą opierać się na metodach efektywnych jak np. opisany algorytm w [13] wykorzystujący schemat Shamira. Dodatkowo udostępniane są informacje pozwalające zweryfikować czy wygenerowane udziały są prawidłowe, jak również czy zebrane fragmenty podczas rekonstrukcji sekretu nie zostały sfałszowane.

4. Proaktywne (ang. *proactive secret sharing*) - metody, w których udziały są okresowo aktualizowane (obliczane od nowa). Dzięki temu osoba próbująca je przejąć ma utrudnione zadanie, ponieważ musi zgromadzić wszystkie fragmenty pochodzące z tego samego okresu czasowego.

Trywialna metoda dzielenia sekretu



Metoda trywialna

Sekret reprezentowany jest za pomocą liczby całkowitej s z zakresu 0 do $k-1$. Fragmenty s_1, s_2, ..., s_{n-1} są generowane losowo, każdy z nich jest równy liczbie mniejszej od k. Ostatni udział obliczany jest z wykorzystaniem wzoru

$$s_n = (s - s_1 - s_2 - \ldots - s_{n-1}) \bmod k$$

Mając do dyspozycji wszystkie elementy można odzyskać sekret korzystając ze wzoru

$$s = (s_1 + s_2 + \ldots + s_n) \bmod k$$

Przykład

Sekret jest liczbą z zakresu 0 do 999 ($k = 1000$) i jest równy 456 ($s = 456$),

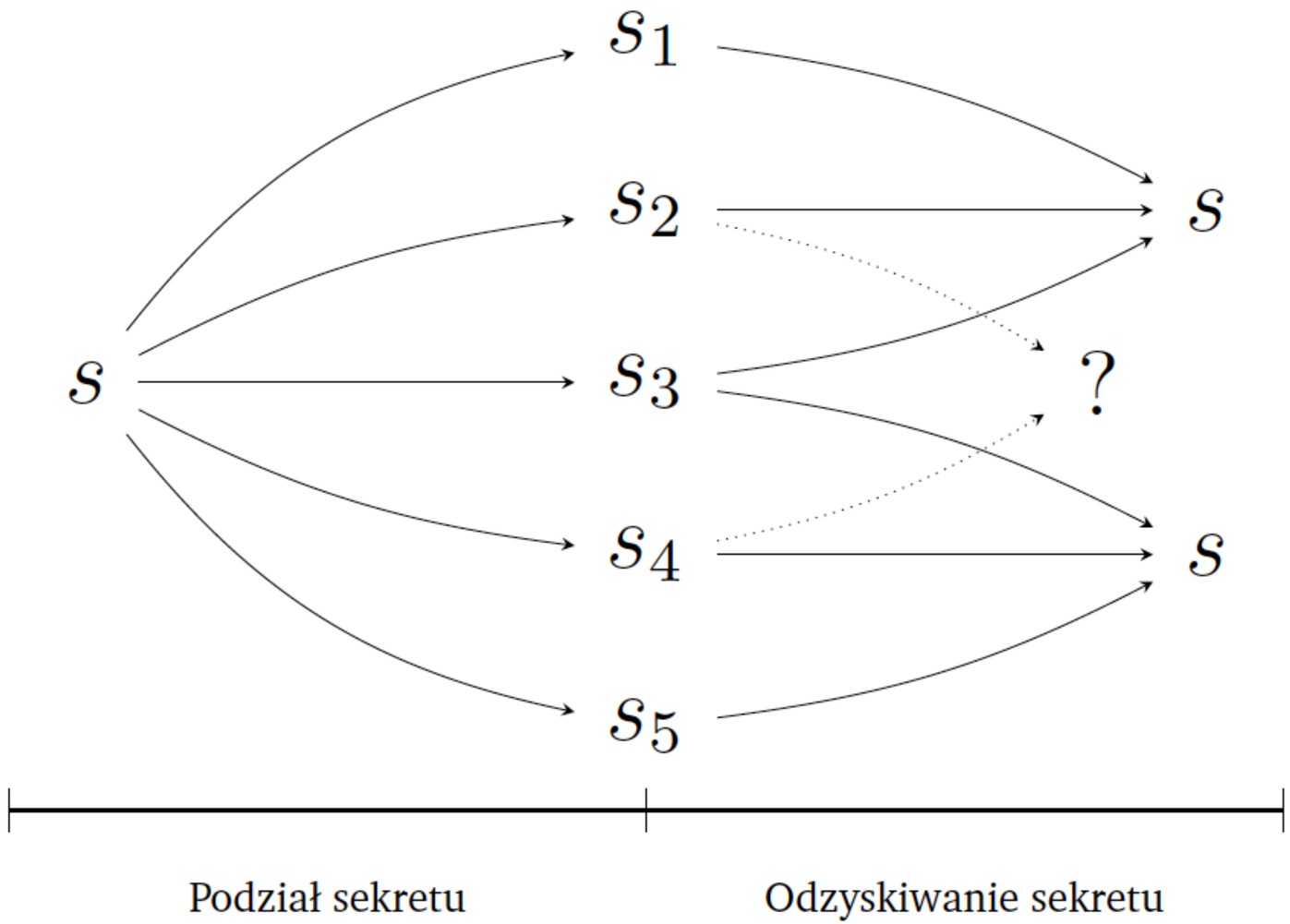
Ma być podzielony na 3 fragmenty ($n = 3$). Wygenerowano losowo udziały $s_1 = 856$ oraz $s_2 = 231$. Ostatni z nich, s_3 jest obliczany z wykorzystaniem wzoru:

$$s_3 = (s - s_1 - s_2) \bmod k = (456 - 856 - 231) \bmod 1000 = -631 \bmod 1000 = 369$$

W celu uzyskania treści sekretu należy skorzystać ze wzoru:

$$s = (s_1 + s_2 + s_3) \bmod k = (856+231+369) \bmod 1000 = 456$$

Schemat Shamira (t,n)



Schemat Shamira

Metoda została oparta na interpolacji wielomianowej Lagrange'a.

Wiadomo, że:

- dwa punkty jednoznacznie wyznaczają linię prostą,
- trzy są konieczne w celu odwzorowania paraboli w układzie współrzędnych,
- istnieje jeden i tylko jeden wielomian *f(x)* stopnia *t – 1* taki, że dla każdego *i* zachodzi równość $f(x_i) = y_i$.

Aby podzielić sekret *s* na *n* udziałów $s_1, s_2, \ldots, s_n$
należy wygenerować losowy wielomian stopnia *t – 1,* w którym sekret jest równy jego wyrazowi wolnemu ($a_0 = s$)

$$f(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1}$$

Algorytm rozdzielający

1. Wygeneruj losową, dużą liczbę p taką, że $p \in \mathbb{P} : p > s, p > n$.

2. Wybierz $t - 1$ losowych liczb $a_1, a_2, \ldots, a_{t-1}$.

3. Dla każdego $i = 1, 2, \ldots, n$ oblicz:

$$s_i = s + \sum_{j=1}^{t-1} a_j x^j \bmod p$$

4. Każdy z udziałów reprezentowany jest jako para współrzędnych:

$$(x, y) = (x, f(x)) = (i, s_i)$$

Algorytm łączący

Sekret można odtworzyć na dwa sposoby. Pierwszy z nich polega na rozwiązaniu układu t równań liniowych:

$$\begin{cases} s_1 = s + a_1 x_1 + a_2 x_1^2 + \ldots + a_{t-1} x_1^{t-1} \bmod p \\ s_2 = s + a_1 x_2 + a_2 x_2^2 + \ldots + a_{t-1} x_2^{t-1} \bmod p \\ \ldots \\ s_t = s + a_1 x_t + a_2 x_t^2 + \ldots + a_{t-1} x_t^{t-1} \bmod p \end{cases}$$

Drugą z możliwości jest wykorzystanie wielomianu interpolacyjnego Lagrange'a:

$$f(x) = \sum_{i=1}^{t} s_i \ell_i(x) \text{ gdzie } \ell_i(x) = \prod_{j=1, i \neq j}^{t} \frac{x - x_j}{x_i - x_j} \bmod p \tag{3.5}$$

Przykład

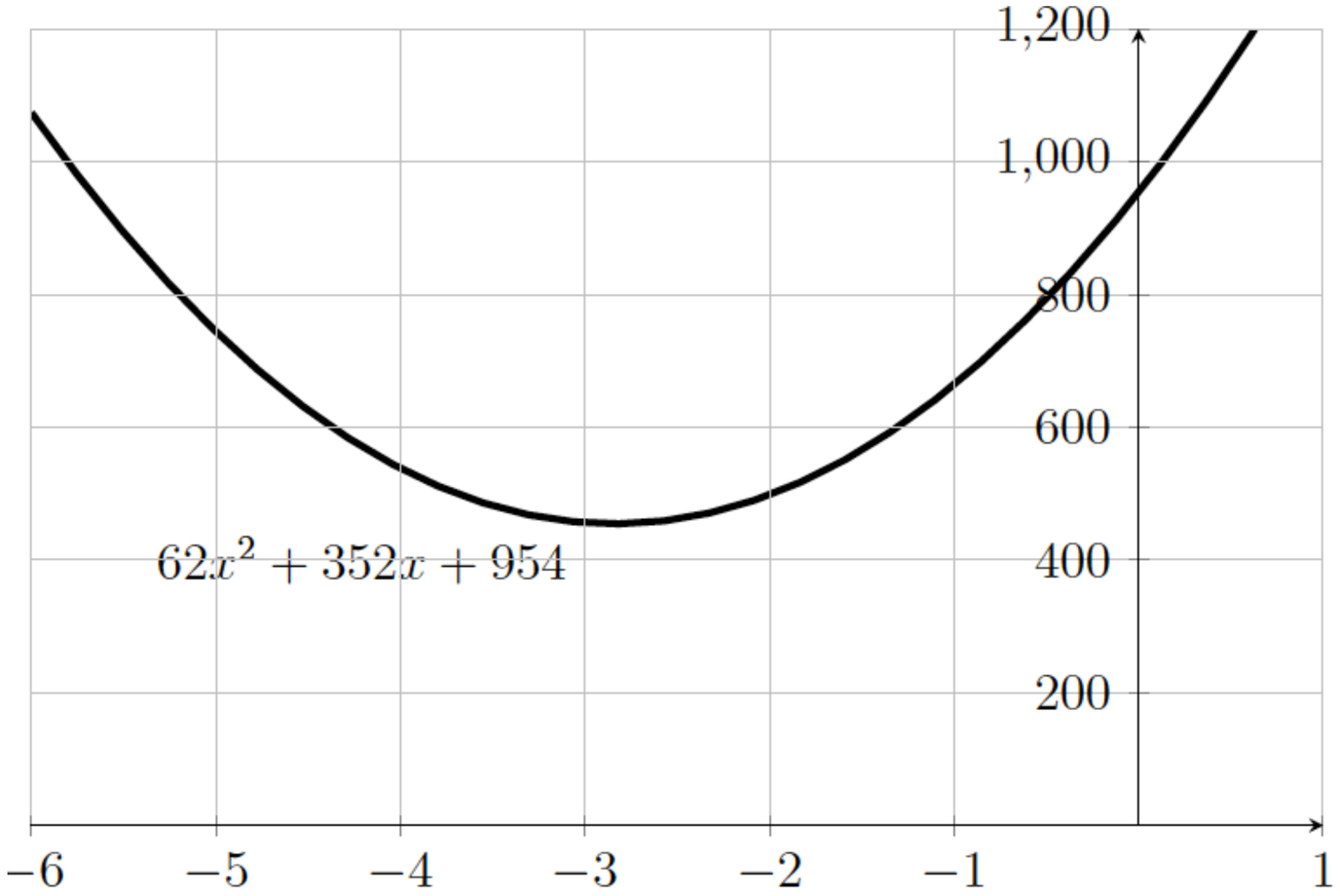
Sekret wynosi 954 ($s = 954$). Zostanie podzielony na 4 fragmenty ($n = 4$), z których 3 będą wymagane do jego odtworzenia ($t = 3$). Wygenerowano losowo wymagane stałe:

- $p = 1523$,
- $a_1 = 352$,
- $a_2 = 62$.

Otrzymamy wielomian drugiego stopnia (t-1):

$$f(x) = a_2x^2 + a_1x^1 + a_0 = 62x^2 + 352x + 954$$

Wykres wielomianu



Podział sekretu

$$s_1 = f(1) = 62x^2 + 352x + 954 \bmod 1523 = 1368$$

$$s_2 = f(2) = 62x^2 + 352x + 954 \bmod 1523 = 1906 \bmod 1523 = 383$$

$$s_3 = f(3) = 1045$$

$$s_4 = f(4) = 308$$

Łączenie sekretu

Do odtworzenia sekretu wykorzystano udziały s_1, s_3, s_4 rozwiązując układ równań:

$$\begin{cases} 1368 = a_0 + a_1 + a_2 \bmod 1523 \\ 1045 = a_0 + 3a_1 + 9a_2 \bmod 1523 \\ 308 = a_0 + 4a_1 + 16a_2 \bmod 1523 \end{cases}$$

Po dokonaniu obliczeń zostały wyznaczone wartości: $a_2 = 62$, $a_1 = 352$, $a_0 = s = 954$.

obliczenie sekretu z interpolacji wielomianowej

Do interpolacji wielomianowej wykorzystano następujące punkty w układzie współrzędnych: $(x_0, y_0) = (2, 383)$, $(x_1, y_1) = (3,1045)$, $(x_2, y_2) = (4, 308)$ i obliczono:

$$\ell_0(x) = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x - 3}{2 - 3} \cdot \frac{x - 4}{2 - 4} = \frac{x^2 - 7x + 12}{2} = \frac{1}{2}x^2 - \frac{7}{2}x + 6$$

$$\ell_1(x) = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x - 2}{3 - 2} \cdot \frac{x - 4}{3 - 4} = \frac{x^2 - 6x + 8}{-1} = -x^2 + 6x - 8$$

$$\ell_2(x) = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x - 2}{4 - 2} \cdot \frac{x - 3}{4 - 3} = \frac{x^2 - 5x + 6}{2} = \frac{1}{2}x^2 - \frac{5}{2}x + 3$$

cd..

Powstałe wielomiany $\ell_0(x)$, $\ell_1(x)$, $\ell_2(x)$ należy pomnożyć przez odpowiadające im współrzędne y_0, y_1, y_2:

$$y_0\ell_0(x) = 383 \cdot (\frac{1}{2}x^2 - \frac{7}{2}x + 6) \bmod 1523 = \frac{383}{2}x^2 - \frac{2681}{2}x + 775$$

$$y_1\ell_1(x) = 1045 \cdot (-x^2 + 6x + 8) \bmod 1523 = -1045x^2 + 178x - 745$$

$$y_2\ell_2(x) = 308 \cdot (\frac{1}{2}x^2 - \frac{5}{2}x + 3) \bmod 1523 = 154x^2 - 770x + 924$$

W ostatnim kroku dodano wyrazy wolne wielomianów $y_0\ell_0(x)$, $y_1\ell_1(x)$, $y_2\ell_2(x)$: $775 - 745 + 924 = 954 = s$. Wykonanie algorytmu łączącego udziały doprowadziło do uzyskania sekretu s.

Właściwości

1. Rozmiar każdego fragmentu s_i nie przekracza rozmiaru sekretu s.

2. Jeżeli t nie ulega zmianie, można dodawać nowe fragmenty poprzez obliczenie wartości wielomianu $f(x)$ w kolejnym, unikalnym punkcie.

3. Fragmenty s_i można zmodyfikować bez zmiany sekretu s. W tym celu należy wyznaczyć nowy wielomian $f(x)$ z takim samym jak poprzednio wyrazem wolnym a_0. Częsta zmiana tego typu pomaga zwiększyć bezpieczeństwo. Należy mieć jednak na uwadze, że udziały można połączyć tylko wtedy, gdy wszystkie pochodzą z tego samego wielomianu $f(x)$.

Zadania szczegółowe

1. Zaimplementuj aplikację, która pozwala na podział oraz odtworzenie sekretu przy użyciu metody trywialnej. Określ dla jakich wartości metoda ta nie jest bezpieczna. Wskaż podstawowe wady wynikające z użycia trywialnego podziału sekretu.
2. Opracuj program umożlwiający podział oraz odtworzenie sekretu zgodnie ze schematem Shamira. Narzędzie powinno wizualizować poszczególne etapy działania algorytmu oraz pozwalać na modyfikację parametrów takich jak:
    a. całkowita liczba udziałów,
    b. wymagana liczba udziałów,
    c. sekret,
    d. liczba pierwsza.

    Jaka jest minimalna, wymagana liczba udziałów, aby algorytm działał poprawnie?