System ankietowania – Dokumentacja

Prowadzący:

Prof. dr hab. Mirosław Kutyłowski

Róża Kuźma,

Jan Tatarynowicz

Wersja 1.2

1. Wprowadzenie

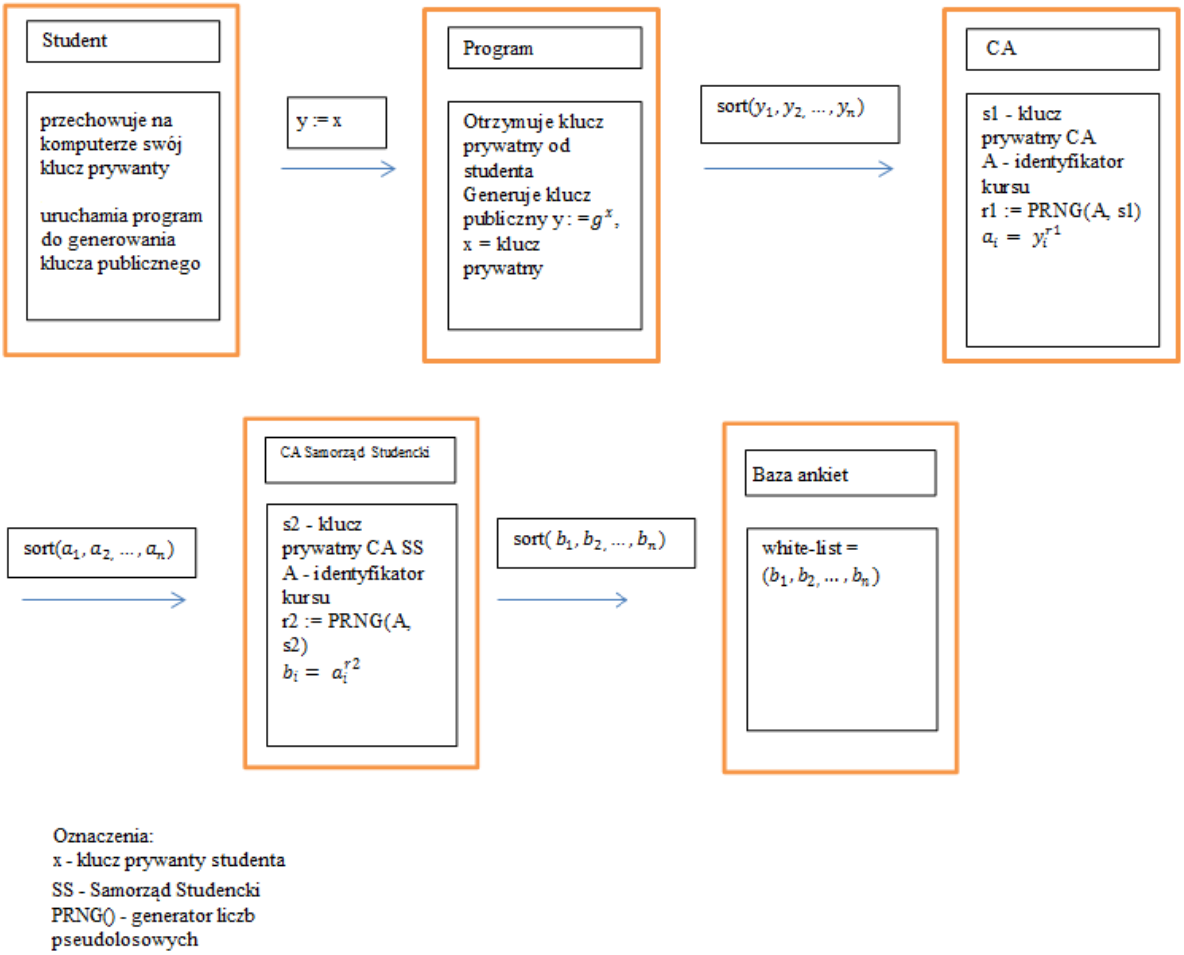
Opis sytemu:
System umożliwia studentom wypełnianie ankiet dotyczących oceny kursów na PWr zapewniając im anonimowość i jednocześnie możliwość weryfikacji, czy student jest zapisany na dany kurs.

Podstawowe założenia:
- jeden student może wypełnić wiele ankiet,
- nie można łatwo zidentyfikować tożsamości studenta mając dostęp do g^x, g^y (problem Diffiego-Hellmana), czy white-list różnych kursów,
- white-listy są generowane po zapisach na kursy.

Podmioty i ich role:
- Student – osoba posiadająca prawa zapisów na kursy,
- PC – osobisty komputer użytkownika na którym przechowywany jest klucz prywatny studenta,
- JSOS (Jednolity System Obsługi Studenta)
- CA - przyjmuje klucze publiczne studentów $y_i^{r_1}$ dla $i = 1,2 \dots n$ od JSOS i podaje je posortowane w postaci $y_i^{r_1}$ do CA Samorząd Studencki,
- CA Samorząd Studencki - przyjmuje y_i^r od CA i wysyła je w postaci $y_i^{(r_1)^{r_2}}$ do Baza Ankiet
- Ankieta –ankieta, która jest wypełniania przez studenaserwer ankiet; daje Studentowi ankiety do wypełnienia; sprawdza, czy student należy do kursu A; wysyła poprawne ankiety do Bazy Ankiet
- BazaAnkiet – serwer przechowujący white-listy studentów zapisanych na kurs, sprawdza czy student należy do kursA i czy jego ma prawo do wypełnienia ankiety

2. Przypadki użycia

a. Generowanie white-lisy.



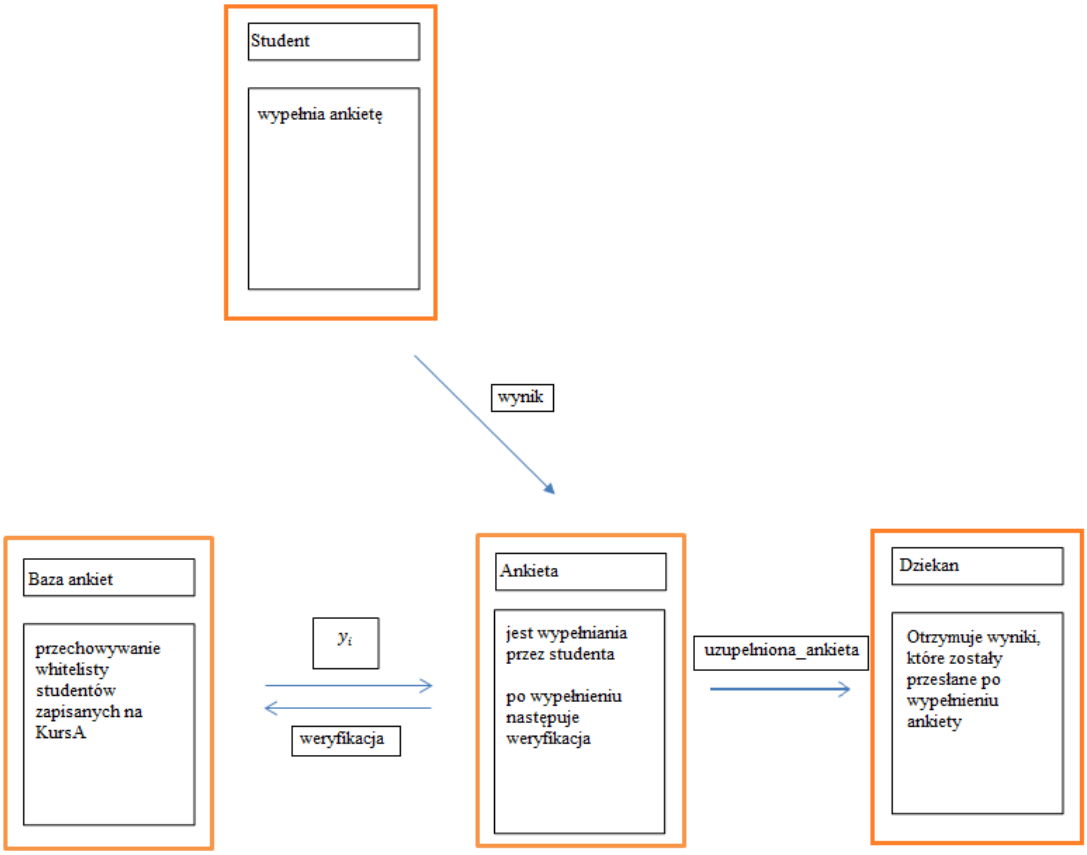
Rys1. Proces generowania whitelisty.

- Student -> Program - student uruchamia program, który generuje z jego klucza prywatnego x generuje jego klucz publiczny $y = g^x$

- Program -> CA – Program wysyła CA posortowany zbiór kluczy publicznych studentów $y_1, y_2, \dots, y_n$
- CA -> CA Samorząd Studencki - dla każdego klucza studenta y_i CA generuje $a_i = y_i^{r1}$, gdzie r1 = PRNG(A, s1), A - identyfikator kursu A, s1 to klucz prywatny CA, a PRNG to generator liczb pseudolosowych. CA sortuje zbiór $a_1, a_2, \dots, a_n$ i wysyła do CA Samorząd Studencki,
- CA Samorząd Studencki -> Baza ankiet – CA Samorząd Studencki otrzymuje posortowanę listę $a_1, a_2, \dots, a_n$. Dla każdego a_i ze zbioru $a_1, a_2, \dots, a_n$ CA Samorząd Studencki generuje $b_i = a_i^{r2}$, gdzie r2 = PRNG(A, s2), gdzie: A - identyfikator kursu A, s2 to klucz prywatny CA Samorząd Studencki, a PRNG to generator liczb pseudolosowych.

- CA Samorząd Studencki -> Baza ankiet – CA Samorząd Studencki sortuje zbiór $b_1, b_2, \dots, b_n$ i wysyła do Baza ankiet gdzie jest przechowywana white-lista osób zapisana na KursA.

b. Wypełnianie ankiety:



Oznaczenia:
wynik - odpowiedzi studenta, które wypłenia w ankiecie
weryfikacja - proces weryfikacji tego, czy klucz publiczny studenta znajduje się na white-liście Bazy ankiet
uzupełniona_ankieta - przesłanie danych z wypełnionych ankiet dla Dziekana

Rys2. Proces wypełniania ankiety

- Baza ankiet – Baza ankiet przechowuje white-liste studentów zapisanych na dany kurs oraz po wypełnieniu ankiety przez studenta sprawdza czy dany student ma prawo do wypełniania ankiety

- Student -> Ankieta -> Baza ankiet – Student wypełnia Ankietę. Wynik *wynik* są to odpowiedzi studenta na poszczególne pytania zawarte w ankiecie. Po wypełnieniu ankiety następuje weryfikacja, czyli proces, który sprawdza czy dany student może uzupełnić ankietę czy nie.

- Ankieta -> Dziekan – Zostają wysłane dane *uzupelniona_ankieta* które zawierają odpowiedzi studentów na pytania zawarte w ankiecie dla dziekana. Dziekan ma możliwość zobaczenia wyników.