9 laboratorinis darbas

Difio Helmano apsikeitimo raktais ir šifravimo algoritmo tyrimas

1. Darbo tikslas

Suprasti kaip perduodami šifravimui reikalingi duomenys ir naudojant Difio Helmano (Diffie–Hellman) algoritmą saugiai perduoti žinutę.

2. Darbo užduotis

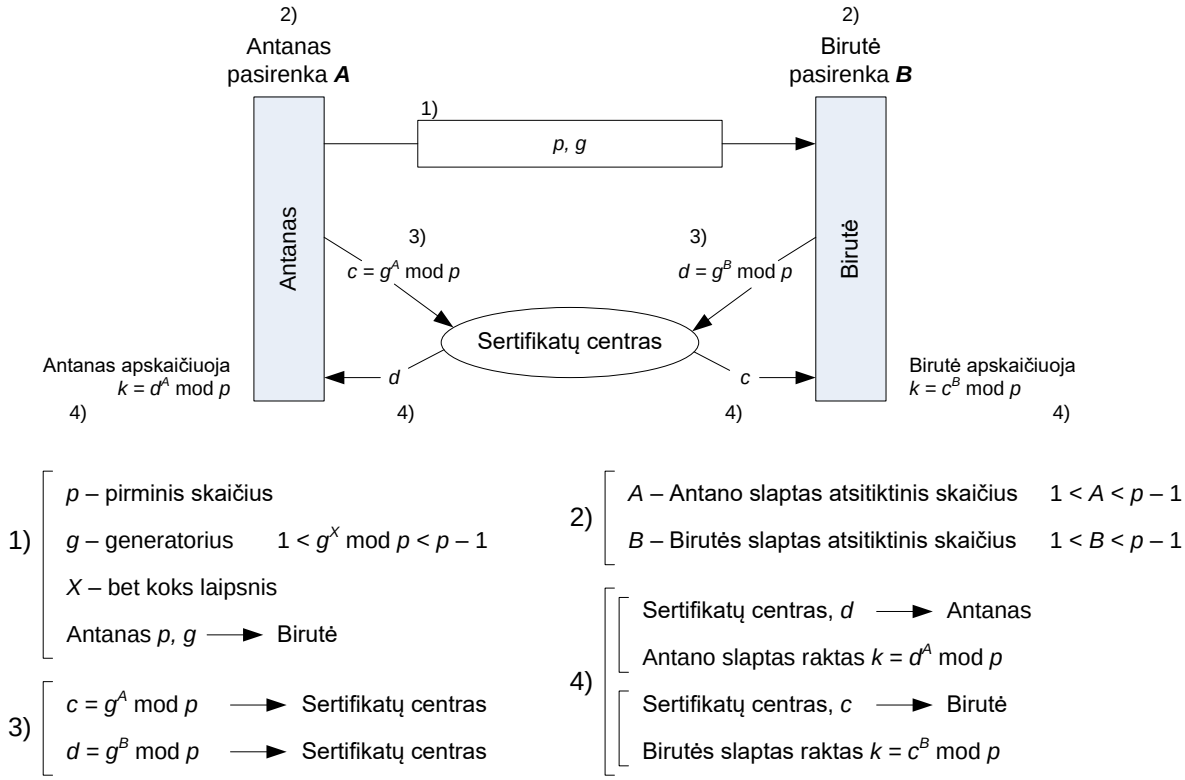
Laboratorijoje susipažinkite su pateikta teorine medžiaga ir naudodami pateiktos formos popieriuje užrašytas žinutes atkartokite procesus būdingus Difio Helmano raktų apsikeitimo bei šifravimo algoritmui.

3. Bendros teorinės žinios

Difio Helmano apsikeitimo raktais algoritmas

Didelį postūmį kriptografijos vystymuisi suteikė 1976 m. W. Diffie ir M. Hellman išspausdintas straipsnis „*New Directions in Cryptography*“. Straipsnyje buvo pateikta tuo metu revoliucinė viešojo rakto (asimetrinės) kriptosistemos idėja ir pasiūlytas originalus raktų apsikeitimo algoritmas.

Apsikeitimas raktais turi būti saugus, kad būtų saugus apsikeitimas šifruotais tekstais. 1 pav. pateiktas Difio Helmano raktų apsikeitimo protokolas.



1 pav. Difio Helmano protokolas raktams apsikeisti

1. Antanas ir Birutė susitaria dėl dviejų sveikų skaičių – *p* ir *g*, kur *p* yra pirminis skaičius. *p* – dažniausiai didelis, *g* – gali būti mažas. *g* yra vadinamas generatoriumi ir yra toks, kad bet kokiu *X*

laipsniu turi būti tenkinama sąlyga: $1 < g^X \bmod p < p-1$. Šie skaičiai perduodami atviru tekstu. Juos parinkti ir perduoti gali kuris nors vienas iš komunikuojančiųjų, pvz. Antanas.

2. Po to, Antanas pasirenka atsitiktinį sveiką skaičių A, $(1<A<p-1)$, ir laiko jį paslaptyje. Birutė taip pat pasirenka atsitiktinį slaptą sveiką skaičių B $(1<B<p-1)$, ir taip pat laiko jį paslaptyje.

3. Antanas apskaičiuoja savo atvirą raktą: $$c=g^A \bmod p, \quad (1)$$ ir pradeda raktų apsikeitimo procedūrą nusiųsdamas Birutei tokio turinio pranešimą: (p, g), o savo atvirą raktą c perduoda sertifikatų centrui.

Birutė apskaičiuoja savo atvirą raktą:

$$d=g^B \bmod p, \quad (2)$$

ir jį nusiunčia sertifikatų centrui.

4. Iš sertifikatų centro gavę vienas kito atvirus raktus c ir d, Antanas ir Birutė gali apskaičiuoti slaptą raktą:

a. Antanas – $k=d^A \bmod p$, (3)

b. Birutė – $k=c^B \bmod p$.

Taigi, atlikę skaičiavimus Antanas ir Birutė gaus tą patį raktą, kurį galės naudoti perduodamos žinutės šifravimui.

4. Darbo eiga

1. Nelyginį variantą atliekantys studentai iš užduoties gautus pirminį skaičių p ir generatorių g, užrašykite lentelėje „Pradiniai vieši šifravimo parametrai“ ir tokią žinutę perduokite savo ryšio partneriui.
2. Pasirinkite atsitiktinį skaičių A arba B tarp 1 ir (p–1), šio skaičiaus partneriui nesakykite, tai bus Jūsų privatus raktas, jį užsirašykite lentelėje „Privatus raktas“.
3. Paleiskite kalkuliatorių, moksliniu (*Scientific*) režimu.
4. Apskaičiuokite savo viešąjį raktą c arba d pagal 1 ar 2 formules.

‘(‘ ‘g’ ‘x^y’ ‘A’ ‘Mod’ ‘p’ ‘)’

5. Viešąjį raktą užrašykite lape „Viešasis raktas” ir atiduokite dėstytojui, jis atlieka sertifikatų centro (CA) vaidmenį (patikima trečioji šalis garantuojanti autentiškumą). Jei Difio Helmano protokolas nenaudoja sertifikatų jis neatsparus nepatikimo subjekto įterpimo (*Man-in-the-Middle* – MIM) atakoms.
6. Sugalvokite trumpą tekstinę žinutę ją užrašykite lentelėje „Siunčiama žinutė“, paverskite ją skaitinėmis vertėmis ir ją užrašykite lentelėje „Skaitinė žinutės forma”.
7. Gaukite savo ryšio parnerio viešąjį raktą iš sertifikatų serverio (šiuo atveju dėstytojo).
8. Apskaičiuokite bendrą slaptą raktą k (3) ir jį užrašykite lentelėje „Slaptas raktas“.

‘(‘ ‘partnerio viešasis raktas’ ‘x^y’ ‘A’ ‘Mod’ ‘p’ ‘)’

9. Užkoduokite savo žinutę naudodami slaptą raktą k (pridėkite k prie kiekvienos skaitinės žinutės formos vertės) ir ją užrašykite.
10. Su ryšio partneriu apsikeiskite šifruotomis žinutėmis.
11. Naudodami slaptą raktą k iššifruokite gautą žinutę ir ją užrašykite.
12. Patikrinkite ar teisingai iššifruota žinutė.

5. Kontroliniai klausimai

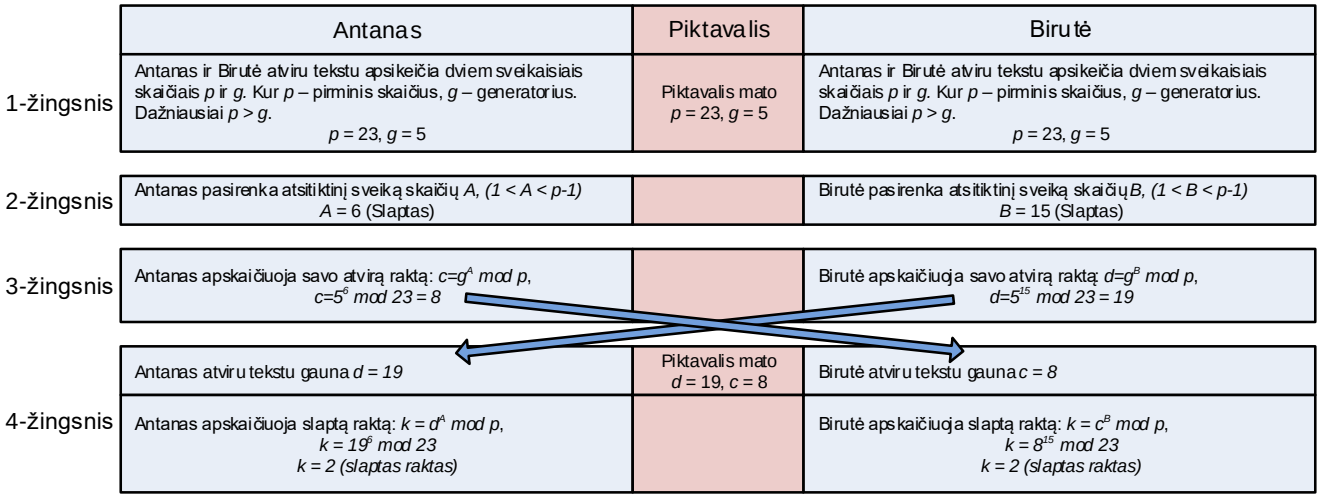
1. Ką daro matematinė *Mod* funkcija?
2. Kokie šifravimo parametrai yra perduodami tarp ryšio partnerių, o kokie ne?
3. Kokie yra kiti saugaus apsikeitimo raktais ir šifravimo algoritmai? Kokie jų pagrindiniai skirtumai nuo minėtojo?

6. Ataskaitos turinys

1. Darbo tikslas;
2. Darbo užduotis;
3. Difio Helmano raktų apsikeitimo ir šifravimo algoritmu pagrįsta šifruotų žinučių apsikeitimo eiga;
4. Naudoti šifravimo parametrai;
5. Siųsta ir iššifruota žinutės;
6. Atsakymai į kontrolinius klausimus, naudota literatūra.

Variantai

Varianto nr.	Pirminis skaičius p	Generatorius g
1	11	3
2		
3	13	4
4		
5	17	5
6		
7	19	6
8		
9	11	7
10		
11	13	8
12		
13	17	9
14		
15	19	3
16		
17	17	4
18		
19	19	5
20		


Antanas
Piktavalis
Birutė
1-žingsnis
Antanas ir Birutė atviru tekstu apsikeičia dviem sveikaisiais skaičiais p ir g. Kur p – pirminis skaičius, g – generatorius. Dažniausiai p > g.
p = 23, g = 5
Piktavalis mato
p = 23, g = 5
Antanas ir Birutė atviru tekstu apsikeičia dviem sveikaisiais skaičiais p ir g. Kur p – pirminis skaičius, g – generatorius. Dažniausiai p > g.
p = 23, g = 5
2-žingsnis
Antanas pasirenka atsitiktinį sveiką skaičių A, (1 < A < p-1)
A = 6 (Slaptas)
Birutė pasirenka atsitiktinį sveiką skaičių B, (1 < B < p-1)
B = 15 (Slaptas)
3-žingsnis
Antanas apskaičiuoja savo atvirą raktą: c=g^A mod p,
c=5^6 mod 23 = 8
Birutė apskaičiuoja savo atvirą raktą: d=g^B mod p,
d=5^15 mod 23 = 19
Antanas atviru tekstu gauna d = 19
Piktavalis mato
d = 19, c = 8
Birutė atviru tekstu gauna c = 8
4-žingsnis
Antanas apskaičiuoja slaptą raktą: k = d^A mod p,
k = 19^6 mod 23
k = 2 (slaptas raktas)
Birutė apskaičiuoja slaptą raktą: k = c^B mod p,
k = 8^15 mod 23
k = 2 (slaptas raktas)