Turinys

ElGamalio kriptosistema

1985 metais egiptiečių kilmės kriptografas Taheris ElGamalis (angl. *Taher Elgamal*) pasiūlė asimetrinę kriptosistemą, kuri šiandien žinoma kaip ElGamalio šifravimo schema. Šios sistemos saugumas yra pagrįstas Difio-Helmano raktų mainais ir diskretinio logaritmo problemomis, kurios laikomos itin sudėtingomis matematiniu požiūriu. Algoritmas plačiai taikomas saugiam duomenų perdavimui bei skaitmeniniams parašams, o jo pagrindas – asimetrinė raktų pora, užtikrinanti stiprų šifravimą ir duomenų vientisumą.

Viešieji parametrai **PP**=(***p***, ***g***)

Apskritai sudėtinga užduotis rasti generatorius aibėje $\mathbf{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$, tačiau naudojant stiprų pirminį ***p*** ir *Lagranžo teoremą grupės teorijoje*, generatorių $\mathbf{Z}_p^*$ galima rasti atsitiktine tvarka. Paieška laikoma užbaiga jei galioja dvi sąlygos:

1. jeigu ***p*** ir ***q*** yra stiprūs pirminiai $p = 2 \cdot q + 1 \rightarrow q = (p-1)/2$;
2. jeigu visi $g \in \Gamma$, $g^q \neq 1 \ mod\ p$ ir $g^2 \neq 1 \ mod\ p$. **Tik 40% skaičių yra generatoriai.**

Pavyzdinis generatoriaus radimas (***g*** didinamas po vienetą, kol *ans* $g^q \neq 1$ **mod** ***p*** ir $g^2 \neq 1$ **mod** ***p***):

```
>> p=genstrongprime(28)
p = 187086587
>> isprime(p)
ans = 1
>> q=(p-1)/2
q = 93543293
>> isprime(q)
ans = 1
>> g=2;
g=2
>> mod_exp(g,q,p)
ans = 187086586
>> mod_exp(g,2,p)
ans = 4
```

```
>> p=genstrongprime(28)
p = 241301447
>> q=(p-1)/2
q = 120650723
>> g=2;
>> mod_exp(g,q,p)
ans = 1
>> g=5;
>> mod_exp(g,q,p)
ans = 241301446
>> mod_exp(g,2,p)
ans = 25
```

```
>> p=genstrongprime(28)
p = 224013599
>> q=(p-1)/2
q = 112006799
>> g=111;
>> mod_exp(g,q,p)
ans = 224013598
>> mod_exp(g,2,p)
ans = 12321
```

Toliau naudosime ***p***=int64(241301447); ***g***=5.

Privataus ir viešo raktų poros apskaičiavimas

Raktų generavimas susideda iš šių žingsnių:

1. Sugeneruokite privatų raktą (**PR**) ***x***, pasirinkdami atsitiktinį skaičių $x \leftarrow randi(\mathbf{Z}_p)$, ir patikrinkite ar galioja sąlyga $2 \leq x \leq p$:

   ```
   >> x =int64(randi(p-1))
   x = 927980
   ```

   ```
   >> 2<=x & x<=p
   ans = 1
   ```

2. Apskaičiuokite viešą raktą (**VR**) $a = g^x$ **mod** ***p***:

   ```
   >> a=mod_exp(g,x,p)
   a = 193101372
   ```

3. Konkretaus subjekto privatus raktas **PR** = ***x*** = 927980, viešas raktas **VR** = ***a*** = 193101372.

Toliau naudosime subjektui **Aldona** raktų porą ***x***=927980; ***a***=int64(193101372).

Užduotys privataus ir viešo raktų apskaičiavimui.

Turėdami pirminius skaičius ***p***, ***g*** ir atsitiktinį skaičių (privatų raktą) ***x***, apskaičiuokite viešą raktą ir nustatykite, kuri privataus ir viešo raktų pora iš toliau pateiktų yra teisinga:

1. ***p***=int64(234461687), ***g***=5, ***x***=int64(268829348)
2. ***p***=int64(257175599), ***g***=7, ***x***=int64(15996459)
3. ***p***=int64(235237979), ***g***=2, ***x***=int64(240017859)
4. ***p***=int64(189282707), ***g***=5, ***x***=int64(177275528)

Raktų poros teisingumas ir viešieji raktai (**VR**) ***a***:

1. Neteisinga raktų pora, ***a*** = 10165232;
2. Teisinga raktų pora, ***a*** = 154059003;
3. Teisinga raktų pora, ***a*** = 182304382;
4. Neteisinga raktų pora, ***a*** = 46188149.

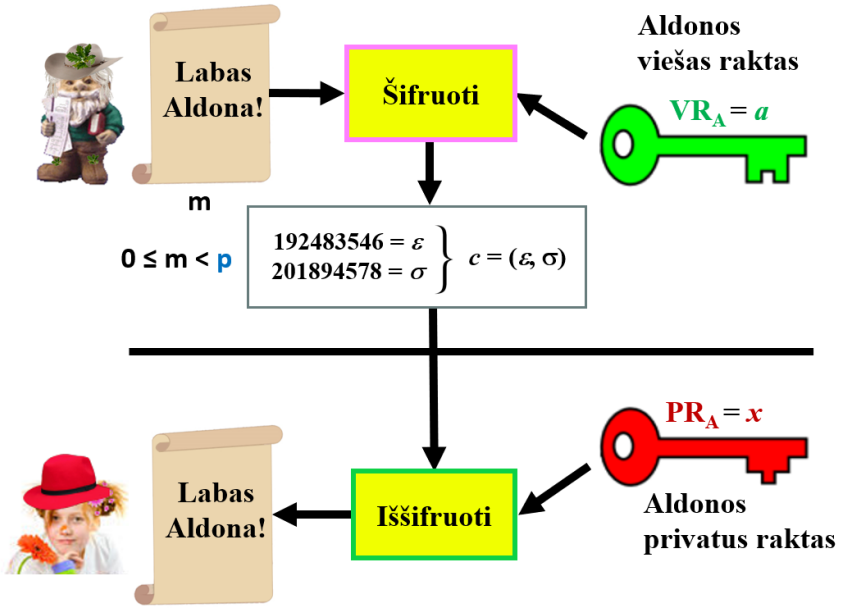
ElGamalio šifravimas

ElGamalio šifravimo algoritmas yra asimetrinio rakto šifravimo schema, kuri remiasi Difio-Helmano raktų mainų mechanizmu. Naudojant šią schemą, viena šalis užšifruoja pranešimą viešuoju raktu, o kita – iššifruoja jį privačiuoju raktu. Algoritmas grindžiamas diskrečiųjų logaritmų radimo ciklinėje grupėje sudėtingumu, t.y., net jei žinome g^a ir g^i, apskaičiuoti g^{ai} yra labai sunku. Dėl šios savybės ElGamalio šifravimo schema užtikrina duomenų saugumą net ir esant dideliam skaičiavimo pajėgumui.

Atsinaujinkime viešuosius parametrus p=int64(241301447); g=5 ir subjektui **Aldona** raktų porą x=927980; a=int64(193101372).

Broniaus pranešimas (tekstograma) m, žymintis pinigų sumą:
>> m=131727
m=131727

Supaprastinta pranešimo šifravimo ir šifrogramos iššifravimo schema pateikiama 1 pav.
c=Šifruoti(VR_A, m)
m=Iššifruoti(PR_A, c)



1 pav. Pranešimo šifravimo ir šifrogramos iššifravimo schema

Bronius šifruoja pranešimą m su **Aldonos** viešuoju raktu (VR_A) a:

1. Patikrinkite ar galioja sąlyga $0 \le m < p$:
   >> 0 <= m & m < p
   ans = 1
2. Sugeneruokite atsitiktinį skaičių $k \leftarrow$ randi(Z_{p-2}), kad galiotų sąlyga $2 \le k \le p$-2:
   >> k=int64(randi(p-2))
   k = 101794605
   >> 2<=k & k<=p-2
   ans = 1
3. Apskaičiuokite enkriptorių $E = m \cdot a^k \bmod p$:
   >> a_k=mod_exp(a,k,p)
   a_k = 68273717
   >> E=mod(m*a_k,p)
   E = 186989569
4. Apskaičiuokite dekriptorių $D = g^k \bmod p$:
   >> D=mod_exp(g,k,p)
   D = 94269996

5. Šifrograma **c = (E,D)** pranešimui ***m***
   Enc(*x*, *m*) = c = (E,D) = (186989569, 94269996).
6. **Bronius** siunčia **Aldonai** šifrogramą **c**.

Svarbu pastebėti, kad kiekvienai tekstogramai ***m*** turi būti generuojamas naujas atsitiktinis skaičius ***k***, antraip žinodamas vieną tekstogramą potencialus piktavališkas veikėjas galėtų apskaičiuoti likusias.

Aldona iššifruoja gautą šifrogramą **c**=(**E,D**) su savo privačiuoju raktu (PR_A) ***x*** ir perskaito pranešimą ***ms***.

1. Apskaičiuokite $\mathbf{D}^{-x \bmod (p-1)} \bmod p$ ir patikrinti ar $\mathbf{D}^{x} \bullet \mathbf{D}^{-x \bmod (p-1)} \bmod p = 1$:
   >> D_mx=mod_exp(D,p-1-x,p)
   D_mx = 58401759
   >> D_x=mod_exp(D,x,p)
   D_x = 68273717
   >> mod(D_x*D_mx,p)
   ans = 1
2. Apskaičiuokite pranešimą $\boldsymbol{m} = \mathbf{E} \bullet \mathbf{D}^{-x} \bmod p$:
   >> ms=mod(E*D_mx,p)
   ms = 131727

Aldona gavus pranešimą jį priima tik tuomet, kai pranešimas gali būti tinkamas perskaitymui, t.y iššifruojamas.

P.S.
Kadangi buvote už **Bronių** ir **Aldoną**, galite palyginti pradinę pranešimo reikšmę su gauta reikšme ir sužinoti ar pranešimas buvo teisingai užšifruotas ir iššifruotas.

>> m==ms
ans = 1 ← jeigu **1** buvo užšifruota ir iššifruota teisingai

Užduotys asimetrinei ElGamalio šifravimo sistemai.

Užduotims naudojami viešieji parametrai p=int64(241301447); g=5.

1. Turėdami viešą raktą (VR_A) a, atsitiktinį skaičių k, pranešimą m, nustatykite, kurioms iš **Broniaus** siųstų **Aldonai** šifrogramų **c** apskaičiavimui buvo panaudotos šios reikšmės:
   1. a=int64(10035139), k=int64(235098085), m=253
   2. a=int64(106468764), k=int64(79793749), m=483
   3. a=int64(187597619), k=int64(208582545), m=693
   4. a=int64(111538491), k=int64(194926519), m=8

   Šifrogramos **c**=(**E**,**D**):
   1. **E** = 17634047, **D** = 109811654;
   2. **E** = 17463370, **D** = 124980846;
   3. **E** = 17463370, **D** = 78762328;
   4. **E** = 230958439, **D** = 109811654;
   5. **E** = 112243115, **D** = 78762328;
   6. **E** = 230958439, **D** = 131896226
   7. **E** = 112243115, **D** = 124980846;
   8. **E** = 17634047, **D** = 131896226.
2. Turėdami privatų raktą (PR_A) x ir šifrogramą **c**=(**E**,**D**), nustatykite, kuris iš toliau esančių pranešimų m buvo **Broniaus** užšifruotas ir perduotas **Aldonai**, naudojantis šiomis pateiktomis reikšmėmis:
   1. x=int64(219010782), **E**=int64(131968784), **D**=int64(33904789)
   2. x=int64(191027938), **E**=int64(16233709), **D**=int64(138032810)
   3. x=int64(128484130), **E**=int64(132019933), **D**=int64(6238080)
   4. x=int64(167376189), **E**=int64(33750902), **D**=int64(17464263)

   Šifruojami pranešimai m:
   1. m = 9;
   2. m = 897;
   3. m = 1453;
   4. m = 36.
3. Gavę dviejų **Broniaus** siunčiamų **Aldonai** šifrogramų $\mathbf{c_1}=(\mathbf{E_1},\mathbf{D_1})$ ir $\mathbf{c_2}=(\mathbf{E_2},\mathbf{D_2})$ enkriptorius $\mathbf{E_1}=m_1 \bullet a^k \bmod p$ ir $\mathbf{E_2}=m_2 \bullet a^k \bmod p$, kurie buvo suformuoti naudojant tą patį viešą raktą a ir atsitiktinį skaičių k ir žinant vieną iš šifruojamų tekstogramų, t.y. pinigų sumą m_1, nustatykite antrą užšifruotą pinigų sumą m_2. Atvirkštiniams skaičiams apskaičiuoti pvz. a^{-1} naudokite funkciją mulinv(a, p).

   Matematinis m_2 apskaičiavimas.

   Turėdami $\mathbf{E_1}$ ir norėdami panaikinti m_1, abi lygties puses padauginame iš $m_1^{-1} \bmod p$:

   $$m_1^{-1} \bullet \mathbf{E_1} \equiv m_1^{-1} \bullet (m_1 \bullet a^k) \bmod p,$$

   Kadangi $m_1^{-1} \bullet m_1 \equiv 1 \bmod p$, lygtis supaprastėja iki:

   $$a^k \equiv \mathbf{E_1} \bullet m_1^{-1} \bmod p.$$

   Turėdami a^k, galime atkurti m_2 iš enkriptoriaus $\mathbf{E_2}$, padaugindami $\mathbf{E_2}$ iš $(a^k)^{-1} \bmod p$:

   $$\mathbf{E_2} \bullet (a^k)^{-1} \bmod p \equiv m_2 \bullet a^k \bullet (a^k)^{-1} \bmod p.$$

   Kadangi $a^k \bullet (a^k)^{-1} \equiv 1 \bmod p$, lygtis supaprastėja iki:

   $$m_2 \equiv \mathbf{E_2} \bullet (a^k)^{-1} \bmod p.$$

   Enkriptoriai $\mathbf{E_1}$ ir $\mathbf{E_2}$ ir pinigų sumos m_1:
   1. **E1**=int64(190056069), **E2**=int64(230168721), m_1=351
   2. **E1**=int64(172122898), **E2**=int64(17463370), m_1=864
   3. **E1**=int64(237265025), **E2**=int64(30729949), m_1=1935
   4. **E1**=int64(126235483), **E2**=int64(103111423), m_1=89

   Užšifruotos pinigų sumos m_2:
   1. m_2 = 483;
   2. m_2 = 1600;
   3. m_2 = 48;
   4. m_2 = 154

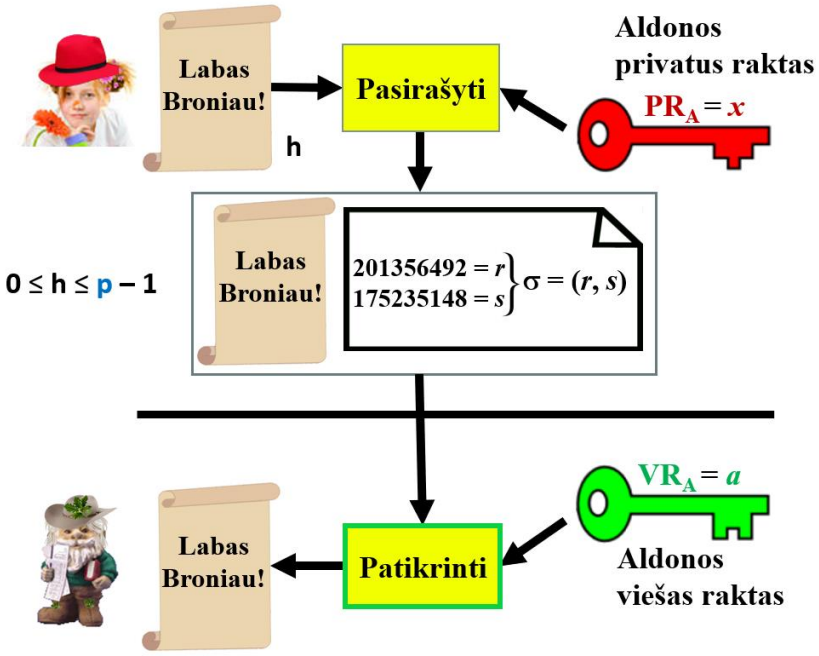
ElGamalio parašas

ElGamalio skaitmeninio parašo schema yra sukurta remiantis diskretinio logaritmo skaičiavimo sudėtingumu ir Difio-Helmano problema. Parašo generavimui naudojamas privatusis raktas, o parašą galima patikrinti naudojant viešąjį raktą. ElGamalio parašo schema užtikrina pranešimo autentiškumą, vientisumą ir neatšaukiamumą. Autentiškumas reiškia, kad gavėjas gali patikrinti siuntėjo tapatybę, vientisumas – kad pranešimas nebuvo pakeistas, o neatšaukiamumas garantuoja, jog siuntėjas negali melagingai teigti, kad nepasirašė pranešimo. Ši schema plačiai naudojama saugiam duomenų perdavimui ir skaitmeninių parašų kūrimui.

Atsinaujinkime subjektui **Aldona** raktų porą x=927980; a=int64(193101372).

Aldonos pranešimas (tekstograma) m:
>> m="Labas Broniau!"
m=Labas Broniau!

Supaprastinta parašo formavimo ir tikrinimo schema pateikiama 2 pav.
Pasirašyti(PR_A, h) = σ = (r, s)
V=Patikrinti(VR_A, h, σ), P∈{*True*, *False*} ≡ {1, 0}



2 pav. Parašo formavimo ir jo patikrinimo schema

Aldona formuoja parašą σ pranešimui m su savo privačiuoju raktu (PR_A) x:

1. Apskaičiuokite pranešimo m santrauką h=H(M) ir patikrinti ar galioja sąlyga $0 \le h \le p$-1:
   >> h=hd28(m)
   h = 4022209
   >> 0<=h & h<=p-1
   ans = 1
2. Sugeneruokite atsitiktinį skaičių $k \leftarrow$ randi(Z_{p-2}), kad didžiausias bendras daliklis tarp k *ir* p-1 būtų 1 ir patikrinkite ar galioja sąlyga $2 \le k \le p$-2:
   >> k=genprime(27)
   k = 233191723
   >> gcd(k,p-1)
   ans = 1
   >> 2<=k & k<=p-2
   ans = 1

3. Apskaičiuokite pirmąją parašo komponentę r=g^k **mod** p:
   >> r=mod_exp(g,k,p)
   r = 226945643
4. Apskaičiuokite k^{-1} **mod** (p-1) ir patikrinkite ar $k \cdot k^{-1}$ **mod** (p-1) = 1:
   >> k_mp1=mulinv(k, p-1)
   k_mp1 = 200116339
   >> mod(k*k_m1,p-1)
   ans = 1
5. Apskaičiuokite antrąją parašo komponentę **s**=(h-x**r**)k^{-1} **mod** (p-1):
   >> hmxr=mod(h-x*r,p-1)
   hmxr = 131859381
   >> s=mod(hmxr*k_mp1,p-1)
   s = 35812335
6. Parašas **σ = (*r*,*s*)** santraukai ***h*** yra
   Pasirašyti(*x*, *h*) = σ = (*r*,*s*) = (226945643, 35812335);
7. **Aldona** siunčia **Broniui** parašą **σ**, pranešimą ***m***.

Bronius tikrina parašą **σ** pranešimui ***m***. Parašas **σ**=(***r***,***s***) pranešimui ***m*** yra patikrinamas naudojant **Aldonos** viešąjį raktą (VR_A) a:

1. Apskaičiuokite pranešimo ***m*** santrauką ***h'*=H(*m*)** ir patikrinti ar galioja sąlyga $0 \le h' \le p-1$:
   >> h=hd28(m)
   h = 4022209
   >> 0<=h & h<=p-1
   ans = 1
2. Patikrinkite ar galioja sąlygos $1 < r < p-1$ ir $1 < s < p-1$:
   >> 1<r & r<p-1
   ans = 1
   >> 1<s & s<p-1
   ans = 1
3. Apskaičiuokite $V_1=g^{h'} \bmod p$ ir $V_2=a^r r^s \bmod p$ ir patikrinkite ar galioja lygybė $V_1=V_2$:

   V1
   >> V1=mod_exp(g,h,p)
   V1 = 157365409

   V2
   >> a_r=mod_exp(a,r,p)
   a_r = 160484328
   >> r_s=mod_exp(r,s,p)
   r_s = 223819162
   >> V2=mod(a_r*r_s,p)
   V2 = 157365409

   >> **V1==V2**
   ans = 1 ← jeigu **1** parašas tikras

Parašas galiojantis (*True*) jeigu: $VR_A = a = F(PR_A) = g^x \bmod p$; $h = h'$.
Patikrinti(a, **σ**, h') = **P**∈{*True*, *False*}≡{**1**, **0**}.

Tikrintojas **Bronius** priima parašą, jeigu galioja visos aukščiau pateiktos sąlygos, kitais atvejais parašą atmeta.

Užduotys ElGamalio parašui.

Užduotims naudojami viešieji parametrai ***p***=int64(241301447); ***g***=5.

1. Turėdami privatų raktą (**PR**) ***x***, atsitiktinį skaičių ***k***, pranešimą ***m***, nustatykite, kuriam iš pokalbio metu tarp **Aldonos** ir **Broniaus** toliau pateiktų parašų **σ = (*r*,*s*)** formavimui buvo panaudotos šios reikšmės:

   1. ***x***=int64(219010782), ***k***=int64(191853097), ***m***="Labas Broniau!"
   2. ***x***=int64(167376189), ***k***=int64(230826165), ***m***="Labas Aldona!"
   3. ***x***=int64(128484130), ***k***=int64(172580663), ***m***="Kada galėtume susitikti."
   4. ***x***=int64(191974619), ***k***=int64(226322045), ***m***="Susitikime vakare."

   Parašai **σ = (*r*,*s*)**:

   1. ***r*** = 119129574, ***s*** = 168692563;
   2. ***r*** = 235701085, ***s*** = 230376317;
   3. ***r*** = 158546630, ***s*** = 230376317;
   4. ***r*** = 9698008, ***s*** = 168692563;
   5. ***r*** = 119129574, ***s*** = 202792434;
   6. ***r*** = 235701085, ***s*** = 120843728;
   7. ***r*** = 158546630, ***s*** = 120843728;
   8. ***r*** = 9698008, ***s*** = 202792434.

2. Turėdami viešą raktą (**VR**) ***a***, pranešimą ***m***, parašą **σ = (*r*,*s*)**, nustatykite, kuriems **Aldonos** ir **Broniaus** pranešimams suformuoti parašai yra galiojantys, panaudojant šias reikšmes:

   1. ***a***=int64(187597619), ***m*** = "Šalia seno ąžuolo.", ***r***=int64(51809372); ***s***=int64(2017893188);
   2. ***a***=int64(106468764), ***m*** = "Šalia didelio kelmo.", ***r***=int64(144624799); ***s***=int64(154268034);
   3. ***a***=int64(111538491), ***m*** = "Iki greito.", ***r***=int64(131317563); ***s***=int64(27038754);
   4. ***a***=int64(106468764), ***m*** = "Iki pasimatymo.", ***r***=int64(70802266); ***s***=int64(189315155).

   Tik du parašai **σ = (*r*,*s*)** galioja.

3. Turėdami viešą raktą (**VR**) ***a*** ir parašą **σ = (*r*,*s*)**, nustatykite, kuriems **Aldonos** ir **Broniaus** pranešimams ***m*** buvo suformuotas parašas, panaudojant pateiktas reikšmes:

   1. ***a***=int64(106468764), ***r***=int64(53154548), ***s***=int64(216781614);
   2. ***a***=int64(10035139), ***r***=int64(108369655), ***s***=int64(60196422);
   3. ***a***=int64(187597619), ***r***=int64(216238345), ***s***=int64(213180469);
   4. ***a***=int64(111538491), ***r***=int64(21803879), ***s***= int64(59527638).

   Pranešimai ***m***:

   1. m_1 = "Kelintą valandą vakare.";
   2. m_2 = "19 valandą.";
   3. m_3 = "Kurioje vietoje.";
   4. m_4 = "Jaukioje parko kavinėje.".

ElGamalio šifravimo homomorfiškumas

Homomorfizmas yra matematinių struktūrų savybė, leidžianti atlikti operacijas su užšifruotais duomenimis taip, kad šios operacijos atitinka tas pačias operacijas, kaip ir su neapdorotais duomenimis pvz. multiplikatyvus homomorfizmas $2 \bullet 3$ užšifravus $\mathbf{c_1}$ ir $\mathbf{c_2} \rightarrow \mathbf{c_{12}} = \mathbf{c_1 \bullet c_2} \rightarrow \mathbf{c_{12}}$ išifravus = 6 (ElGamalio ir kt. šifrai); adityvus homomorfizmas $1 + 2$ užšifravus $\mathbf{c_1}$ ir $\mathbf{c_2} \rightarrow \mathbf{c_{12}} = \mathbf{c_1 \bullet c_2} \rightarrow \mathbf{c_{12}}$ išifravus = 3 (Pailer ir kt. šifrai), $2 + 3$ užšifravus $\mathbf{c_1}$ ir $\mathbf{c_2} \rightarrow \mathbf{c_{12}} = \mathbf{c_1 + c_2} \rightarrow \mathbf{c_{12}}$ išifravus = 5 (Elipsinės kreivės ir kt.). Kitaip tariant, jei turime dvi struktūras (pvz., grupes, žiedus), homomorfiškumas leidžia perkelti operacijas iš vienos struktūros į kitą, išlaikant jų prasmę.

ElGamalio šifravimas yra vienas iš šifravimo metodų, pasižymintis multiplikatyvia homomorfine savybe, kuri leidžia atlikti operacijas su užšifruotais duomenimis taip, kad iššifravus rezultatą gaunamas teisingas atsakymas, tarsi skaičiavimai būtų atlikti tiesiogiai su pradiniais, nešifruotais duomenimis. Naudojantis ElGamalio adityviu homomorfiškumu, sandaugą $1 \bullet 2 \bullet \cdots \bullet n$ galima įgyvendinti dauginant užšifruotų skaičių šifrogramas, o iššifravus rezultatą gaunama teisinga sandauga, pvz. $2 \bullet 3$ užšifravus $\mathbf{c_1}=(\mathbf{E_1},\mathbf{D_1})$ ir $\mathbf{c_2}=(\mathbf{E_2},\mathbf{D_2}) \rightarrow \mathbf{E_1 \bullet E_2}=\mathbf{E_{12}}$ ir $\mathbf{D_1 \bullet D_2}=\mathbf{D_{12}}$ yra $\mathbf{c_{12}}=(\mathbf{E_{12}},\mathbf{D_{12}}) \rightarrow \mathbf{c_{12}}=(\mathbf{E_{12}},\mathbf{D_{12}})$ išifravus = 6.

Homomorfinis šifravimo principas naudojamas elektroniniame balsavime, duomenų debesijos privačiuose skaičiavimuose, finansinėse operacijose, medicininiuose tyrimuose su jautriais duomenimis.

Atsinaujinkime subjektui **Aldona** raktų porą x=927980; a=int64(193101372).

Broniaus sandėlininko ir **Broniaus** pardavėjo pranešimai (tekstogramos) m_1 – prekių kiekis, m_2 – prekių kaina:

```
>> m1=50
m1=50
```

```
>> m2=100
m2=100
```

Broniai šifruoja pranešimus m_1 ir m_2 su **Aldonos** viešuoju raktu (VR$_A$) a:

1. Patikrinkite ar galioja sąlygos $0 \leq m_1 < p$ ir $0 \leq m_2 < p$:

```
>> 0 <= m1 & m1 < p
ans = 1
```

```
>> 0 <= m2 & m2 < p
ans = 1
```

2. Sugeneruokite du atsitiktinius skaičius k_1 ir k_2, kad galiotų sąlygos $2 \leq k_1 \leq p$-2 ir $2 \leq k_2 \leq p$-2:

```
>> k1=int64(randi(p-2))
k1 = 116441089
>> 2<=k1 & k1<=p-2
ans = 1
```

```
>> k2=int64(randi(p-2))
k2 = 120486012
>> 2<=k2 & k2<=p-2
ans = 1
```

3. Apskaičiuokite enkriptorius $\mathbf{E_1}=m_1 \bullet a^{k_1} \bmod p$ ir $\mathbf{E_2}=m_2 \bullet a^{k_2} \bmod p$:

```
>> a_k1=mod_exp(a,k1,p)
a_k1 = 21195669
>> E1=mod(m1*a_k1,p)
E1 = 94577662
```

```
>> a_k2=mod_exp(a,k2,p)
a_k2 = 1311630
>> E2=mod(m2*a_k2,p)
E2 = 131163000
```

4. Apskaičiuokite dekriptorius $\mathbf{D_1}=g^{k_1} \bmod p$ ir $\mathbf{D_2}=g^{k_2} \bmod p$:

```
>> D1=mod_exp(g,k1,p)
D1 = 56164440
```

```
>> D2=mod_exp(g,k2,p)
D2 = 90535279
```

5. Šifrograma $\mathbf{c_1 = (E_1,D_1)}$ pranešimui m_1
   $\mathbf{Enc}(x, m_1) = \mathbf{c_1 = (E_1,D_1)}$ = (94577662, 56164440).
   Šifrograma $\mathbf{c_2 = (E_2,D_2)}$ pranešimui m_2

Enc(x, m_2) = c_2 = (E_2,D_2) = (131163000, 90535279).

6. **Broniai** siunčia **Aldonai** šifrogramas c_1 ir c_2.

Aldona gautas šifrogramas tarpusavyje sudaugina ir gautą naują šifrogramą iššifruoja su savo privačiuoju raktu (PR_A) x ir perskaito pranešimą m_{12}.

1. Padauginkite šifrogramas $c_{12} = (E_1 \bullet E_2, D_1 \bullet D_2) = (E_{12}, D_{12})$:
   >> E12=mod(E1*E2,p)
   E12 = 144541194
   >> D12=mod(D1*D2,p)
   D12 = 136441187
2. Apskaičiuokite $D_{12}^{-x \bmod (p-1)} \bmod p$ ir patikrinkite ar $D_{12}^{x} \bullet D_{12}^{-x \bmod (p-1)} \bmod p = 1$:
   >> D12_mx=mod_exp(D12,p-1-x,p)
   D12_mx = 33238347
   >> D12_x=mod_exp(D12,x,p)
   D12_x = 53018706
   >> mod(D12_x*D12_mx,p)
   ans = 1
3. Apskaičiuokite pranešimą $m_{12} = E_{12} \bullet D_{12}^{-x} \bmod p$:
   >> m12=mod(E12*D12_mx,p)
   m12 = 5000

Užduotys ElGamalio šifravimo homomorfiškumui.

Užduotims naudojami viešieji parametrai p=int64(241301447); g=5.

1. Turėdami viešą raktą (VR_A) a, atsitiktinius skaičius k_1 ir k_2, pranešimus m_1 ir m_2, nustatykite, kuriai iš šifrogramų c_{12}=(E_{12},D_{12}) apskaičiavimui buvo panaudotos šios reikšmės:
   1. a=int64(10035139), k_1=int64(235098085), k_2=int64(235098085), m_1=253, m_2=5
   2. a=int64(187597619), k_1=int64(208582545), k_2=int64(235098085), m_1=693, m_2=453
   3. a=int64(106468764), k_1=int64(79793749), k_2=int64(235098085), m_1=1520, m_2=68
   4. a=int64(111538491), k_1=int64(194926519), k_2=int64(235098085), m_1=8, m_2=1856

   Šifrogramos c_{12}=(E_{12},D_{12}):
   1. E_{12} = 168522036, D_{12} = 130765767;
   2. E_{12} = 126197320, D_{12} = 73021265;
   3. E_{12} = 71988746, D_{12} = 140854530;
   4. E_{12} = 13364725, D_{12} = 174854127;
   5. E_{12} = 71988746, D_{12} = 73021265;
   6. E_{12} = 13364725, D_{12} = 130765767;
   7. E_{12} = 168522036, D_{12} = 174854127;
   8. E_{12} = 126197320, D_{12} = 140854530.
2. Turėdami privatų raktą (PR_A) x ir iš **Broniaus** gautas šifrogramas c_1=(E_1,D_1) ir c_2=(E_2,D_2), nustatykite, kuri iš toliau pateiktų **Aldonos** krepšelio pirkinių suma m_{12} buvo apskaičiuota, naudojantis šiomis pateiktomis reikšmėmis:
   1. x=int64(219010782), E_1=int64(82521182), D_1=int64(128897229), E_2=int64(23828992), D_2=int64(41421797)
   2. x=int64(191027938), E_1=int64(197602529), D_1=int64(17366739), E_2=int64(207984531), D_2=int64(125744489)
   3. x=int64(128484130), E_1=int64(28576818), D_1=int64(237377209), E_2=int64(159184895), D_2=int64(114795507)
   4. x=int64(167376189), E_1=int64(15696388), D_1=int64(135519136), E_2=int64(142651974), D_2=int64(158743422)

   Krepšelio pirkinių suma m_{12}:
   1. m_{12} = 16767;
   2. m_{12} = 4485;
   3. m_{12} = 71197;
   4. m_{12} = 3780.