

Turinys

ElGamalio kriptosistema.....	2
Privataus ir viešo rakto apskaičiavimas	2
Asimetrinė ElGamalio šifravimo sistema	4
ElGamalio parašas.....	7
ElGamalio šifravimo homomorfiškumas	10

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 $Z_p^* = \{1, 2, 3, \dots, p-1\}$, tačiau naudojant stiprų pirminį p ir *Lagranžo teoremą grupės teorijoje*, generatorių Z_p^* galima rasti atsitiktine tvarka. Paieška laikoma užbaigta jei tenkinamos dvi sąlygos:

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

Pavyzdinis generatoriaus radimas (g didinamas po vieną, kol ans nelygus 1 ir neviršija p):

```
>>p=genstrongprime(28)      >>p=genstrongprime(28)      >> p=genstrongprime(28)
p = 187086587              p = 241301447              p = 224013599
>> isprime(p)              >> q=(p-1)/2                >> q=(p-1)/2
ans = 1                    q = 120650723             q = 112006799
>> q=(p-1)/2              >> g=2;                    >> g=111;
q = 93543293              >> mod_exp(g,q,p)          >> mod_exp(g,q,p)
>> isprime(q)              ans = 1                     ans = 224013598
ans = 1                    >> g=5;
>> g=2                    >> mod_exp(g,q,p)
>> mod_exp(g,q,p)          ans = 241301446
ans = 187086586
>> g=3;
>> mod_exp(g,q,p)
ans = 1
>> g=4;
>> mod_exp(g,q,p)
ans = 1
```

Toliau naudosime $p=\text{int64}(241301447)$; $g=5$.

Privataus ir viešo rakto apskaičiavimas

Raktų generavimas susideda iš šių žingsnių:

1. Sugeneruoti privatų raktą (**PR**) x , pasirenkant atsitiktinį skaičių x ir patikrinti ar tenkinama sąlyga $2 \leq x \leq p$:

```
>> x =int64(randi(p-1))      >> 2<=x & x<=p
x = 927980                  ans = 1
```

2. Apskaičiuoti viešą raktą (**VR**) $a = g^x \pmod p$:

```
>> 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 $x=927980$; $a=\text{int64}(193101372)$.

Užduotys privataus ir viešo raktų skaičiavimui.

Turėdami pirminius skaičius p , g ir atsitiktinį skaičių x , nustatykite, kuri privataus ir viešo raktų pora iš toliau pateiktų buvo apskaičiuota tinkamai:

1. $p=\text{int64}(234461687)$, $g=5$, $x=\text{int64}(268829348)$;
2. $p=\text{int64}(257175599)$, $g=7$, $x=\text{int64}(15996459)$;
3. $p=\text{int64}(235237979)$, $g=2$, $x=\text{int64}(240017859)$;
4. $p=\text{int64}(189282707)$, $g=5$, $x=\text{int64}(177275528)$.

Raktų poros suderinamumas 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, $a = 46188149$.

Asimetrinė ElGamalio šifravimo sistema

ElGamalio šifravimo algoritmas yra asimetrinio raktų šifravimo schema, kuri remiasi Difio-Helmana 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^j , apskaičiuoti g^{aj} yra labai sunku. Dėl šios savybės ElGamalio šifravimo schema užtikrina duomenų saugumą net ir esant dideliame skaičiavimo pajėgumui.

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

Broniaus pranešimas (tekstograma) m , žymintis pinigų sumą:

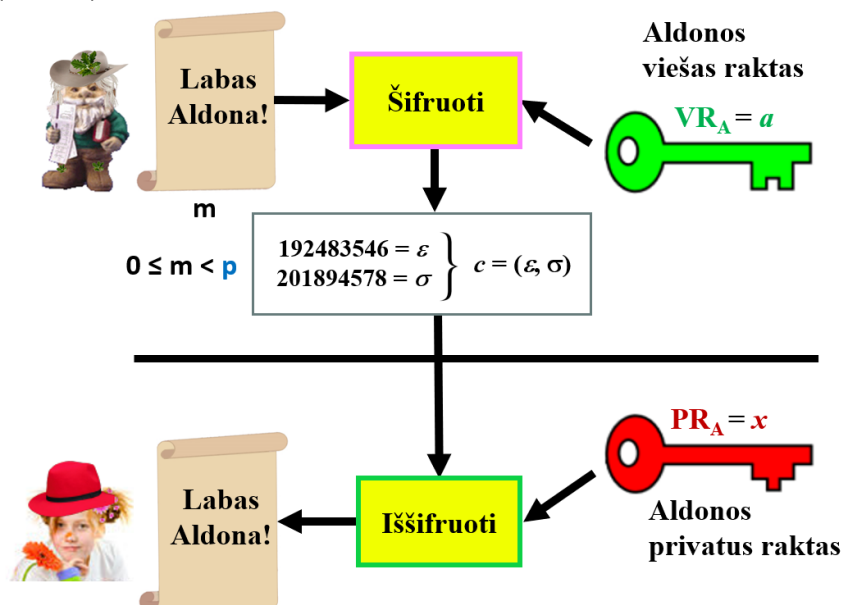
```
>> m=131727
```

```
m=131727
```

Supaprastinta pranešimo šifravimo ir šifrogramos iššifravimo schema pateikiama 1 pav.

$c = \text{Šifruoti}(VR_A, m)$

$m = \text{Iššifruoti}(PR_A, c)$



1 pav. Pranešimo šifravimo ir šifrogramos iššifravimo schema

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

- Patikrinti ar tenkinama sąlyga $0 \leq m < p$:

```
>> 0 <= m & m < p
```

```
ans = 1
```
- Sugeneruoti atsitiktinį skaičių k , kad tenkintų sąlygą $2 \leq k \leq p-2$:

```
>> k=int64(randi(p-1))
```

```
k = 101794605
```

```
>> 2 <= k & k <= p-2
```

```
ans = 1
```
- Apskaičiuoti 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
```
- Apskaičiuoti 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. Apskaičiuoti $D^{-x \bmod (p-1)} \bmod p$ ir patikrinti ar $D^x \cdot D^{-x \bmod (p-1)} \bmod p = 1$:

```
>> 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. Apskaičiuoti pranešimą $m = E \cdot D^{-x} \bmod p$:

```
>> 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 $p=\text{int64}(241301447)$; $g=5$.

1. Turėdami viešą raktą (VRA) a , atsitiktinį skaičių k , pranešimą m , nustatykite, kurioms iš **Broniaus** siųstų **Aldonai** šifrogramų c apskaičiavimui buvo panaudotos šios reikšmės:

1. $a=\text{int64}(10035139)$, $k=\text{int64}(235098085)$, $m=253$;
2. $a=\text{int64}(106468764)$, $k=\text{int64}(79793749)$, $m=483$;
3. $a=\text{int64}(187597619)$, $k=\text{int64}(208582545)$, $m=693$;
4. $a=\text{int64}(111538491)$, $k=\text{int64}(194926519)$, $m=8$.

Šifrogramos $c=(E,D)$:

- | | |
|--|--|
| 1. $E = 17634047$, $D = 109811654$; | 5. $E = 112243115$, $D = 78762328$; |
| 2. $E = 17463370$, $D = 124980846$; | 6. $E = 230958439$, $D = 131896226$ |
| 3. $E = 17463370$, $D = 78762328$; | 7. $E = 112243115$, $D = 124980846$; |
| 4. $E = 230958439$, $D = 109811654$; | 8. $E = 17634047$, $D = 131896226$. |

2. Turėdami privatų raktą (PRA) x ir šifrogramą $c=(E,D)$, nustatykite, kuris iš toliau esančių pranešimų m buvo **Broniaus** užšifruotas ir perduotas **Aldonai**, naudojantis šiomis pateiktomis reikšmėmis:

1. $x=\text{int64}(219010782)$, $E=\text{int64}(131968784)$, $D=\text{int64}(33904789)$;
2. $x=\text{int64}(191027938)$, $E=\text{int64}(16233709)$, $D=\text{int64}(138032810)$;
3. $x=\text{int64}(128484130)$, $E=\text{int64}(132019933)$, $D=\text{int64}(6238080)$;
4. $x=\text{int64}(167376189)$, $E=\text{int64}(33750902)$, $D=\text{int64}(17464263)$.

Šifruojami pranešimai m :

- | | |
|----------------|-----------------|
| 1. $m = 9$; | 3. $m = 1453$; |
| 2. $m = 897$; | 4. $m = 36$. |

3. Gavę dviejų **Broniaus** siunčiamų **Aldonai** šifrogramų $c_1=(E_1,D_1)$ ir $c_2=(E_2,D_2)$ enkriptorius $E_1=m_1 \cdot a^k \bmod p$ ir $E_2=m_2 \cdot a^k \bmod p$, 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 . Atvirkštiniais skaičiams apskaičiuoti pvz. a^{-1} naudokite funkciją $\text{mulinv}(a, p)$.

Matematinis m_2 apskaičiavimas.

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

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

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

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

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

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

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

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

Enkriptoriai E_1 ir E_2 ir pinigų sumos m_1 :

1. $E_1=\text{int64}(190056069)$, $E_2=\text{int64}(230168721)$, $m_1=351$;
2. $E_1=\text{int64}(172122898)$, $E_2=\text{int64}(17463370)$, $m_1=864$;
3. $E_1=\text{int64}(237265025)$, $E_2=\text{int64}(30729949)$, $m_1=1935$;
4. $E_1=\text{int64}(126235483)$, $E_2=\text{int64}(103111423)$, $m_1=89$.

Užšifruotos pinigų sumos m_2 :

- | | |
|-------------------|-----------------|
| 1. $m_2 = 483$; | 3. $m_2 = 48$; |
| 2. $m_2 = 1600$; | 4. $m_2 = 154$ |

ElGamalio parašas

ElGamalio skaitmeninio parašo schema yra sukurta remiantis diskretinio logaritmo skaičiavimo sudėtingumu ir Difio-Helmana 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 $x=927980$; $a=\text{int64}(193101372)$.

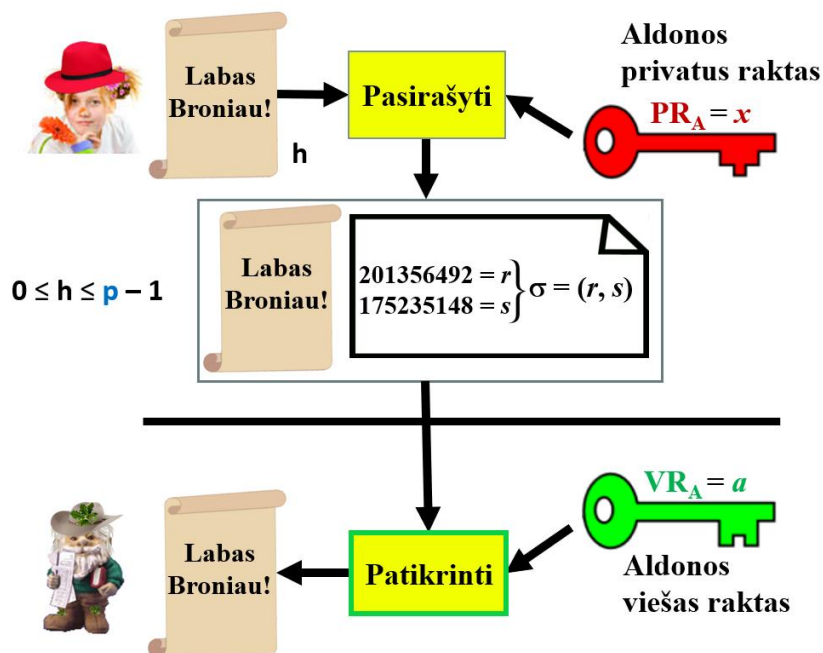
Aldonos pranešimas m :

```
>> m="Labas Broniau!"
m=Labas Broniau!
```

Supaprastinta parašo formavimo ir tikrinimo schema pateikiama 2 pav.

Pasirašyti(PR_A, h) = $\sigma = (r, s)$

V=Patikrinti(VR_A, h, σ), $P \in \{\text{True}, \text{False}\} \equiv \{1, 0\}$



2 pav. Parašo formavimo ir jo patikrinimo schema

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

1. Sugeneruoti atsitiktinį skaičių k , kad didžiausias bendras daliklis tarp k ir $p-1$ būtų 1 ir patikrinti ar galioja sąlyga $2 \leq k \leq p-2$:

```
>> k=genprime(28)
k = 233191723
```

```
>> gcd(k,p-1)
ans = 1
>> 2<=k & k<=p-2
ans = 1
```

2. Apskaičiuoti $k^{-1} \bmod (p-1)$ ir patikrinti ar $k \cdot k^{-1} \bmod (p-1) = 1$:

```
>> k_m1=mulinv(k, p-1)
k_m1 = 200116339
```

```
>> mod(k*k_m1,p-1)
ans = 1
```

3. Apskaičiuoti pirmąją parašo komponentę $r=g^k \bmod p$:
 $\gg r=\text{mod_exp}(g,k,p)$
 $r = 226945643$
4. Apskaičiuoti pranešimo m santrauką $h=H(M)$ ir patikrinti ar tenkinama sąlyga $0 \leq h \leq p-1$:
 $\gg h=\text{hd28}(m)$ $\gg 0 \leq h \ \& \ h \leq p-1$
 $h = 4022209$ $\text{ans} = 1$
5. Apskaičiuoti antrąją parašo komponentę $s=(h-xr)k^{-1} \bmod (p-1)$:
 $\gg \text{hmxr}=\text{mod}(h-x*r,p-1)$ $\gg s=\text{mod}(\text{hmxr}*k_m1,p-1)$
 $\text{hmxr} = 131859381$ $s = 35812335$
6. Parašas h santraukai yra $\sigma = (r,s)$
Pasirašyti(x, h) = $\sigma = (r,s) = (226945643, 35812335)$;
7. **Aldona** siuncia **Broniui** parašą σ , pranešimą m .

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

1. Apskaičiuoti pranešimo m santrauką $h'=H(m)$ ir patikrinti ar tenkinama sąlyga $0 \leq h' \leq p-1$:
 $\gg hA=\text{hd28}(m)$ $\gg 0 \leq h \ \& \ h \leq p-1$
 $hA = 4022209$ $\text{ans} = 1$
2. Patikrinti ar tenkinamos sąlygos $1 < r < p-1$ ir $1 < s < p-1$:
 $\gg 1 < r \ \& \ r < p-1$ $\gg 1 < s \ \& \ s < p-1$
 $\text{ans} = 1$ $\text{ans} = 1$
3. Apskaičiuoti $V_1=g^{h'} \bmod p$ ir $V_2=a^r r^s \bmod p$ ir patikrinti ar tenkinama lygybė $V_1=V_2$:

V1	V2
$\gg V1=\text{mod_exp}(g,hA,p)$	$\gg a_r=\text{mod_exp}(a,r,p)$
$V1 = \underline{157365409}$	$a_r = 160484328$
	$\gg r_s=\text{mod_exp}(r,s,p)$
	$r_s = 223819162$
	$\gg V2=\text{mod}(a_r*r_s,p)$
	$V2 = \underline{157365409}$

$\gg V1==V2$
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') = $P \in \{\text{True}, \text{False}\} \equiv \{1, 0\}$.

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

Užduotys ElGamalio parašui.

Užduotims naudojami viešieji parametrai $p = \text{int64}(241301447)$; $g = 5$.

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

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

Parašai $\sigma = (r,s)$:

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

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

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

Tik du parašai $\sigma = (r,s)$ galioja.

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

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

Pranešimai m :

- | | |
|---|--|
| 1. $m = \text{"Kelintą valandą vakare."}$; | 3. $m = \text{"Kurioje vietoje."}$; |
| 2. $m = \text{"19 valandą."}$; | 4. $m = \text{"Jaukioje parko kavinėje."}$. |

ElGamalio šifravimo homomorfiškumas

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

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

ElGamalio adityviai homomorfinis šifravimo principas naudojamas elektroniniame balsavime, duomenų debesijos privačiuose skaičiavimuose, finansinėse transakcijose ir auditui, medicininiuose tyrimuose su jautriais duomenimis.

Atsinaujinkime subjektui **Aldona** raktų porą $x=927980$; $a=\text{int64}(193101372)$.

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

```
>> m1=50 >> m2=100
m1=50 m2=100
```

Broniai šifruoja pranešimus m_1 ir m_2 su **Aldonos** viešuoju raktu (VR_A) a :

- Patikrinti ar tenkinamos sąlygos $0 \leq m_1 < p$ ir $0 \leq m_2 < p$:

```
>> 0 <= m1 & m1 < p >> 0 <= m2 & m2 < p
ans = 1 ans = 1
```
- Sugeneruoti du atsitiktinius skaičius k_1 ir k_2 , kad tenkintų sąlygas $2 \leq k_1 \leq p-2$ ir $2 \leq k_2 \leq p-2$:

```
>> k1=int64(randi(p-1)) >> k2=int64(randi(p-1))
k1 = 116441089 k2 = 120486012
>> 2 <= k1 & k1 <= p-2 >> 2 <= k2 & k2 <= p-2
ans = 1 ans = 1
```
- Apskaičiuoti enkriptorius $E_1 = m_1 \cdot a^{k_1} \bmod p$ ir $E_2 = m_2 \cdot a^{k_2} \bmod p$:

```
>> a_k1=mod_exp(a,k1,p) >> a_k2=mod_exp(a,k2,p)
a_k1 = 21195669 a_k2 = 1311630
>> E1=mod(m1*a_k1,p) >> E2=mod(m2*a_k2,p)
E1 = 94577662 E2 = 131163000
```
- Apskaičiuoti dekriptorius $D_1 = g^{k_1} \bmod p$ ir $D_2 = g^{k_2} \bmod p$:

```
>> D1=mod_exp(g,k1,p) >> D2=mod_exp(g,k2,p)
D1 = 56164440 D2 = 90535279
```
- Šifrograma $c_1 = (E_1, D_1)$ pranešimui m_1
 $\text{Enc}(x, m_1) = c_1 = (E_1, D_1) = (94577662, 56164440)$.
Šifrograma $c_2 = (E_2, D_2)$ pranešimui m_2
 $\text{Enc}(x, m_2) = c_2 = (E_2, D_2) = (131163000, 90535279)$.
- 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. Padaugininti šifrogramas $c_{12} = (E_1 \cdot E_2, D_1 \cdot D_2) = (E_{12}, D_{12})$:

```
>> E12=mod(E1*E2,p)           >> D12=mod(D1*D2,p)
E12 = 144541194                D12 = 136441187
```
2. Apskaičiuoti $D_{12}^{-x \bmod (p-1)} \bmod p$ ir patikrinti ar $D_{12}^x \cdot D_{12}^{-x \bmod (p-1)} \bmod p = 1$:

```
>> D12_mx=mod_exp(D12,p-1-x,p) >> D12_x=mod_exp(D12,x,p)
D12_mx = 33238347              D12_x = 53018706
                                >> mod(D12_x*D12_mx,p)
                                ans = 1
```
3. Apskaičiuoti pranešimą $m_{12} = E_{12} \cdot D_{12}^{-x} \bmod p$:

```
>> m12=mod(E12*D12_mx,p)
m12 = 5000
```

Užduotys ElGamalio šifravimo homomorfiškumui.

Užduotims naudojami viešieji parametrai $p = \text{int64}(241301447)$; $g = 5$.

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. $a = \text{int64}(10035139)$, $k_1 = \text{int64}(235098085)$, $k_2 = \text{int64}(235098085)$, $m_1 = 253$, $m_2 = 5$;
2. $a = \text{int64}(187597619)$, $k_1 = \text{int64}(208582545)$, $k_2 = \text{int64}(235098085)$, $m_1 = 693$, $m_2 = 453$;
3. $a = \text{int64}(106468764)$, $k_1 = \text{int64}(79793749)$, $k_2 = \text{int64}(235098085)$, $m_1 = 1520$, $m_2 = 68$;
4. $a = \text{int64}(111538491)$, $k_1 = \text{int64}(194926519)$, $k_2 = \text{int64}(235098085)$, $m_1 = 8$, $m_2 = 1856$.

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 pirkinų suma m_{12} buvo apskaičiuota, naudojantis šiomis pateiktomis reikšmėmis:

1. $x = \text{int64}(219010782)$, $E_1 = \text{int64}(82521182)$, $D_1 = \text{int64}(128897229)$,
 $E_2 = \text{int64}(23828992)$, $D_2 = \text{int64}(41421797)$;
2. $x = \text{int64}(191027938)$, $E_1 = \text{int64}(197602529)$, $D_1 = \text{int64}(17366739)$,
 $E_2 = \text{int64}(207984531)$, $D_2 = \text{int64}(125744489)$;
3. $x = \text{int64}(128484130)$, $E_1 = \text{int64}(28576818)$, $D_1 = \text{int64}(237377209)$,
 $E_2 = \text{int64}(159184895)$, $D_2 = \text{int64}(114795507)$;
4. $x = \text{int64}(167376189)$, $E_1 = \text{int64}(15696388)$, $D_1 = \text{int64}(135519136)$,
 $E_2 = \text{int64}(142651974)$, $D_2 = \text{int64}(158743422)$;

Krepšelio pirkinų suma m_{12} :

1. $m_{12} = 16767$;
2. $m_{12} = 4485$;
3. $m_{12} = 71197$;
4. $m_{12} = 3780$.