Turinys

Ronaldas Rivestas, Adi Shamiras ir Leonardas Adlemanas

(angl. *Rivest–Shamir–Adleman, RSA*)

RSA – viena labiausiai paplitusių viešojo rakto kriptografinių sistemų, kurią 1977 m. Masačusetso technologijos institute (angl. trump. *MIT*) sukūrė Ronaldas Rivestas, Adi Shamiras ir Leonardas Adlemanas. 17 metų RSA sistema buvo saugoma JAV patento, bet 2000 m. rugsėjo mėnesį patento galiojimas baigėsi ir nuo tada RSA sistemą galima naudoti laisvai.

RSA asimetrinės kriptografinės sistemos privalumas tas, kad ji gali būti naudojama ir asimetrinio šifravimo, ir elektroninio parašo sistemose.

Viešo ir privataus rakto apskaičiavimas

RSA sistemos pagrindas yra trys tarpusavyje susiję skaičiai. Du iš jų yra visiems žinomi ir sudaro viešąjį raktą **VR** = (**n**, **e**), trečiasis yra slaptas **PR** = (***d***) ir žinomas tiktai rakto savininkui. Raktų generavimas susideda iš šių žingsnių:

1. Sugeneruokite du pakankamai didelius pirminius skaičius ***p*** ir ***q***, kurie turi būti $p \neq q$:
   >> p=genprime(15) — p = 18911
   >> q=genprime(15) — q = 17027
2. Apskaičiuokite sandaugą **n** = ***pq***. Ši sandauga yra vienas iš viešo rakto parametrų:
   >> n=int64(p*q)
   n = 321997597
3. Apskaičiuokite Eulerio funkciją φ(**n**), kai ***p*** ir ***q*** yra pirminiai, tai φ(**n**) = (***p*** – 1)(***q*** – 1):
   >> fy=int64((p-1)*(q-1))
   fy = 321961660
4. Parinkite tokį sveikąjį skaičių **e** (1 < **e** < φ(**n**)), kad **e** ir φ(**n**) būtų reliatyviai pirminiai skaičiai, t. y. **e** ir φ(**n**) ir bendras didžiausias daliklis būtų 1. **e** yra antrasis viešo rakto parametras:
   >> e=genprime(14) — e = 17977
   1 < e < fy — ans = 1
   gcd(e, fy) — ans = 1
5. Raskite privatų raktą/slaptąjį parametrą, kuris dažniausiai randamas naudojant išplėstinį Euklido algoritmą ***d*** = **e**$^{-1}$ **mod** φ(**n**), kad **e*****d*** **mod** φ(**n**) = 1:
   >> d=mulinv(e,fy) ← geriau už eeuklid() — d = 204277393
   >> mod(e*d,fy) — ans = 1
6. Konkretaus subjekto (toliau bus Aldonos) RSA raktų pora yra **PR** = (***d***) ir **VR** = (**n**, **e**), **PR** = (***d***) = (204277393) ir **VR** = (**n**, **e**) = (321997597, 17977)

RSA saugumas remiasi tuo, kad turint tik **n**, ***p*** ir ***q***, jų atkūrimas per priimtiną laiką yra praktiškai neįmanomas. Šiuo metu rekomenduojamas minimalus raktų ilgis yra 2048 bitai.

Užduotys RSA raktų apskaičiavimui.

Turėdami pirminius skaičius ***p***, ***q*** ir reliatyviai pirminį skaičių **e**, nustatykite, kurioms iš toliau pateiktų RSA privataus ir viešojo raktų porų apskaičiavimui buvo panaudotos šios reikšmės:

1. ***p***=27449, ***q***=22189, **e**=17669;
2. ***p***=21407, ***q***=26053, **e**=20353;
3. ***p***=18701, ***q***=30803, **e**= 23627;
4. ***p***=18367, ***q***=17431, **e**= 31019.

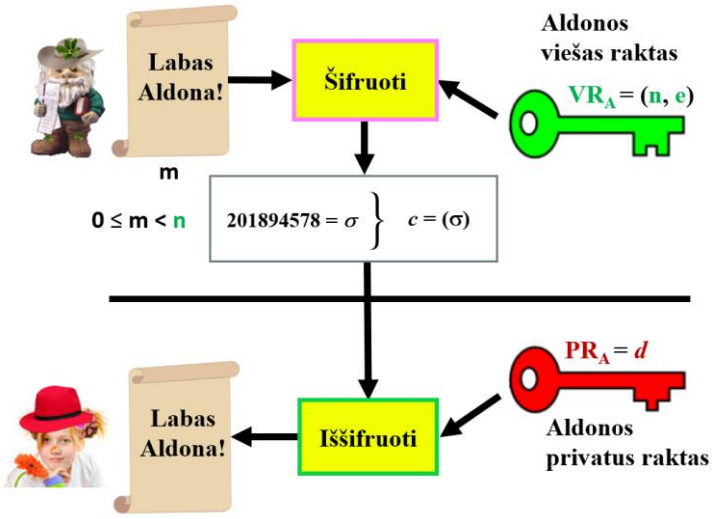
RSA raktų poros:

1. **PR** = (596642189) ir **VR** = (609065861, 17669);
2. **PR** = (553983363) ir **VR** = (576046903, 23627);
3. **PR** = (191974619) ir **VR** = (320155177, 31019);
4. **PR** = (92282689) ir **VR** = (557716571, 20353).

Asimetrinis RSA šifravimas ir iššifravimas

Broniaus pranešimas ***m***, žymintis pinigų sumą:
>> m=800
m=800

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$_A$ = (**n**, **e**):

1. Patikrinkite ar $0 \le m < n$:
   >> 0<=m & m<n
   ans = 1
2. Apskaičiuokite šifrogramą $c = m^e \bmod n$.
   >> c=mod_exp(m,e,n)
   c = 277078937
3. Šifrograma **c** pranešimui ***m***
   Enc(e, n, *m*) = c = (277078937).
4. **Bronius** siunčia **Aldonai** šifrogramą **c**.

Aldona iššifruoja šifrogramą **c** su savo privačiuoju raktu PR$_A$ = (***d***) ir perskaito pranešimą $M = c^d \bmod n$:
>> ms=mod_exp(c,d,n)
ms = 800

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 tas pats pranešimas buvo teisingai užšifruotas ir iššifruotas:

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

Užduotys Asimetriniam RSA šifravimui.

1. Turėdami viešą raktą **VR** = (**n**, **e**) ir pranešimą ***m***, nustatykite, kurioms iš **Broniaus** siųstų **Aldonai** šifrogramų **c** apskaičiavimui buvo panaudotos šios reikšmės:

   1. **n**=int64(609065861), **e**=17669, ***m***=253;
   2. **n**=int64(557716571), **e**=20353, ***m***=483;
   3. **n**=int64(576046903), **e**=23627, ***m***=693;
   4. **n**=int64(320155177), **e**=31019, ***m***=8.

   Šifrogramos **c**:

   1. **c** = 428674001;
   2. **c** = 306986504;
   3. **c** = 530699522;
   4. **c** = 296593473.

2. Turėdami privataus **PR** = (***d***) ir viešo **VR** = (**n**, **e**) raktų porą, šifrogramą **c**, nustatykite, kuris iš toliau esančių pranešimų ***m*** buvo **Broniaus** užšifruotas ir perduotas **Aldonai**, naudojantis šiomis pateiktomis reikšmėmis:

   1. ***d***=int64(92282689), **n**=int64(557716571), **e**=20353, **c**=int64(442140803);
   2. ***d***=int64(596642189), **n**=int64(609065861), **e**=17669, **c**=int64(164478220);
   3. ***d***=int64(553983363), **n**=int64(576046903), **e**=23627, **c**=int64(233885819);
   4. ***d***=int64(191974619), **n**=int64(320155177), **e**=31019, **c**=int64(31947984).

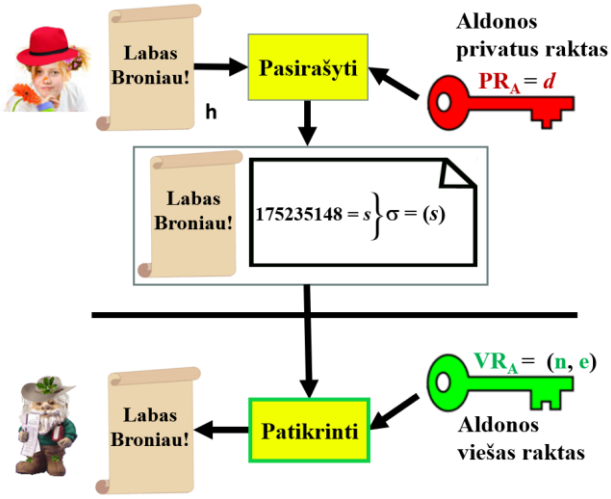
   Šifruojami pranešimai ***m***:

   1. ***m*** = 9;
   2. ***m*** = 897;
   3. ***m*** = 1453;
   4. ***m*** = 36.

RSA parašas

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

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



2 pav. Parašo formavimo ir jo patikrinimo schema

Aldona formuoja parašą **ϭ** pranešimui ***m*** su savo privačiuoju raktu PR_A = (*d*):

1. Apskaičiuokite pranešimo ***m*** santrauką ***h*=H(*m*)** ir patikrinti ar galioja sąlyga ***h*** < **n**:
   >> h=hd28(m)
   h = 4022209
   >> h<n
   ans=1
2. Apskaičiuoti parašą $s=h^d$ **mod n**:
   >> s=mod_exp(h,d,n)
   s = 62451040
3. Parašas **ϭ = (*s*)** santraukai ***h*** yra
   Pasirašyti(*d*, *h*) = ϭ = (*s*) = (62451040);
4. **Aldona** siunčia **Broniui** pranešimą ***m*** ir parašą **ϭ**.

Bronius tikrina parašą **ϭ** pranešimui ***m***. Parašas **ϭ**=(*s*) pranešimui ***m*** yra patikrinamas naudojant **Aldonos** viešąjį raktą VR_A = (**n**, **e**):

1. Apskaičiuokite pranešimo ***m*** santrauką ***h*=H(*m*)** ir patikrinti ar galioja sąlyga ***h*** < **n**:
   >> hA=hd28(m)
   hA = 4022209
   >> hA<n
   ans=1
2. Apskaičiuokite **V=s^e mod n** ir patikrinti ar galioja lygybė **V=*h*'**:
   >> V=mod_exp(s,e,n)
   V = 4022209
   >> **V==hA**
   ans = 1 ← jeigu **1** parašas tikras

Parašas galiojantis (*True*) jeigu: VR_A = (**n**, **e**); ***h* = *h'*.**
Patikrinti(VR_A, ϭ, *h'*) = P∈{*True*, *False*}≡{1, 0}.

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

Užduotys RSA parašui.

1. Turėdami privataus **PR** = (***d***) ir viešo **VR** = (**n**, **e**) raktų porą ir pranešimą ***m***, nustatykite, kuriam iš pokalbio metu tarp **Aldonos** ir **Broniaus** toliau pateiktų parašų **ϭ = (*s*)** formavimui buvo panaudotos šios reikšmės:

   1. ***d***=int64(596642189), **n**=int64(609065861), **e**=17669, ***m***="Labas Broniau!";
   2. ***d***=int64(92282689), **n**=int64(557716571), **e**=20353, ***m***="Labas Aldona!";
   3. ***d***=int64(553983363), **n**=int64(576046903), **e**=23627, ***m***="Kada galėtume susitikti.";
   4. ***d***=int64(191974619), **n**=int64(320155177), **e**=31019, ***m***="Susitikime vakare.".

   Parašai **ϭ = (*s*)**:

   1. ***s*** = 555799686;
   2. ***s*** = 193913095;
   3. ***s*** = 173140478;
   4. ***s*** = 321388681.

2. Turėdami viešą raktą **VR** = (**n**, **e**), pranešimą ***m***, parašą **ϭ = (*s*)**, nustatykite, ar **Aldonos** ir **Broniaus** pranešimams suformuoti parašai yra galiojantys, panaudojant pateiktas reikšmes:

   1. **n**=int64(576046903), **e**=23627, ***m*** = "Šalia seno ąžuolo.", ***s***=int64(425264870);
   2. **n**=int64(320155177), **e**=31019, ***m*** = "Šalia didelio kelmo.", ***s***=int64(225053345);
   3. **n**=int64(609065861), **e**=17669, ***m*** = "Iki greito.", ***s***=int64(26802311);
   4. **n**=int64(557716571), **e**=20353, ***m*** = "Iki pasimatymo.", ***s***=int64(346491286).

   Tik du parašai **ϭ = (*s*)** galioja.

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

   1. **n**=int64(576046903), **e**=23627, ***s***=int64(135267870);
   2. **n**=int64(320155177), **e**=31019, ***s***=int64(181799738);
   3. **n**=int64(609065861), **e**=17669, ***s***=int64(56902511);
   4. **n**=int64(557716571), **e**=20353, ***s***= int64(232857800).

   Pranešimai ***m***:

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

Simetrinis šifravimas ir iššifravimas naudojant Difio Helmano autentifikuotą raktų apsikeitimo protokolą su RSA parašais ir Vernamo šifrą

Šiame skyriuje aprašoma, kaip naudoti Difio Helmano raktų apsikeitimo protokolą, kad būtų sugeneruotas slaptas raktas, kuris vėliau naudojamas Vernamo šifravimui. Pirmiausia, naudojant DH protokolą, apsikeičiama viešaisiais parametrais, kad būtų apskaičiuotas bendras slaptas simetrinis raktas. Šis raktas vėliau naudojamas Vernamo šifravimui, kad būtų užšifruota ir iššifruota žinutė, užtikrinant saugią komunikaciją.

Autentifikuotas Difio Helmano raktų apsikeitimo protokolas su RSA parašais

(angl. *Diffie Helman Key agreement protocol, DH KAP*)

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

Difio Helmano raktų apsikeitimas (DH KAP) – tai matematinis metodas saugiai keistis kriptografiniais raktais vykdant komunikaciją viešaisiais kanalais. Be to, tai vienas pirmųjų viešojo rakto protokolų, kurį sugalvojo Ralfas Merkle (angl. *Ralph Merkle*) ir pavadino Vitfildo Difio (angl. *Whitfield Diffie*) ir Martino Helmano (angl. *Martin E. Hellman*) vardu. DH yra vienas pirmųjų praktinių viešojo rakto apsikeitimo pavyzdžių kriptografijos srityje. 1976 m. paskelbtame Difio ir Helmano darbe anksčiausiai iš viešai žinomų darbų pasiūlyta privataus rakto ir atitinkamo viešojo rakto idėja.

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 $g \in \Gamma$, $g^q \neq 1 \bmod p$ ir $g^2 \neq 1 \bmod p$. **Tik 40% skaičių yra generatoriai.**

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

```
>> p=genstrongprime(28)
p = 268435019
>> isprime(p)
ans = 1
>> q=(p-1)/2
q = 93543293
>> isprime(q)
ans = 1
>> g=2
>> mod_exp(g,q,p)
ans = 268435018
>> mod_exp(g,2,p)
ans = 4
```

```
>> p=genstrongprime(28)
p = 144668519
>> q=(p-1)/2
q = 72334259
>> g=2;
>> mod_exp(g,q,p)
ans = 1
>> g=7;
>> mod_exp(g,q,p)
ans = 144668518
>> mod_exp(g,2,p)
ans = 49
```

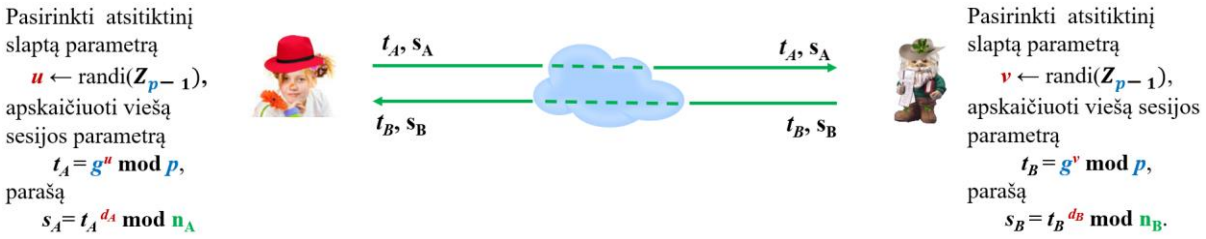
```
>> p=genstrongprime(28)
p = 224013599
>> q=(p-1)/2
q = 112006799
>> g=111;
>> mod_exp(g,q,p)
ans = 224013598
>> mod_exp(g,2,p)
ans = 12321
```

Aldona ir **Bronius** kartu su viešais parametrais iš anksto turi žinoti vienas kito RSA viešą raktą. **Viešieji parametrai** p=268435019 ir g=2, **Aldonos** RSA raktų pora $PR_A = (d_A)$ = (204277393) ir $VR_A = (n_A, e_A)$ = (321997597, 17977), o **Broniaus** $PR_B = (d_A)$ = (293620919) ir $VR_B = (n_A, e_A)$ = (361195337, 17123):

```
>> p=int64(268435019); g=2;
>> dA=int64(204277393); nA=int64(321997597); eA=17977;
>> dB=int64(293620919); nB=int64(361195337); eB=17123;
```

Bendro slapto simetrinio rakto apskaičiavimas

Aldona ir Bronius pasirinkę slaptus atsitiktinius parametrus u, v, apskaičiuoja viešus sesijos parametrus $t_A=g^u \bmod p$, $t_B=g^v \bmod p$, kuriems suformuoja parašus $\text{б}_A=s_A=t_A^{d_A} \bmod n_A$ ir $\text{б}_B=s_B=t_B^{d_B} \bmod n_B$ ir vienas kitam išsiunčia viešus sesijos parametrus kartu su parašais per tinklą (žr. 3 pav.) vienas kitam.



3 pav. Aldona ir Bronius apsikeičia viešais sesijos parametrais ir parašais

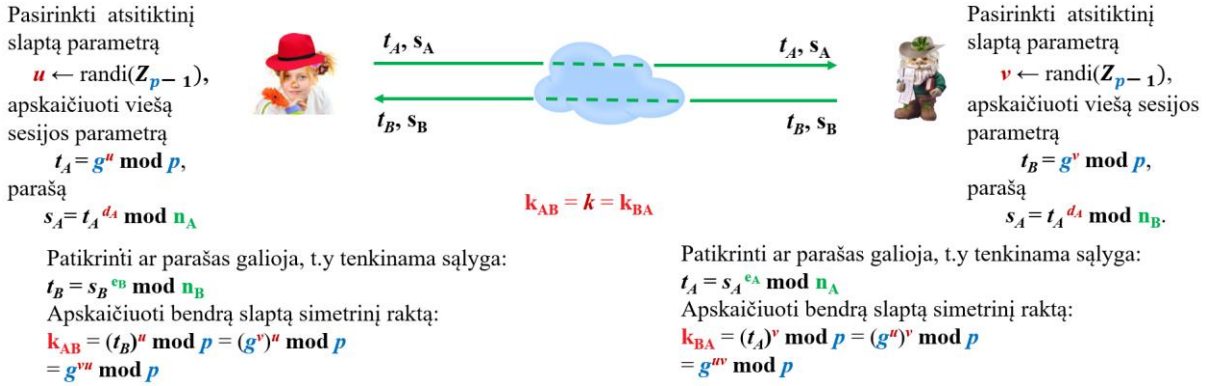
Aldona

```
>> u=int64(randi(2^28-1))
u = 195162450
>> tA=mod_exp(g,u,p)
tA = 234887359
>> sA=mod_exp(tA,dA,nA)
sA=236295026
```

Bronius

```
>> v=int64(randi(2^28-1))
v = 212879876
>> tB=mod_exp(g,v,p)
tB = 67527455
>> sB=mod_exp(tB,dB,nB)
sB = 57678530
```

Aldona ir Bronius gavę vienas kito viešus sesijos parametrus t_A, t_B ir parašus б_A, б_B, pirmiausia patikrina ar parašai galioja t.y ar $t_B=s_B^{e_B} \bmod n_B$ ir $t_A=s_A^{e_A} \bmod n_A$, ir parašams galiojant apskaičiuoja bendrą slaptą simetrinį raktą k, apskaičiuodami $k_{AB}=(t_B)^u \bmod p$ ir $k_{BA}=(t_A)^v \bmod p$, platesni skaičiavimai pateikiami 4 pav.



4 pav. Aldona ir Bronius patikrina parašus ir apskaičiuoja bendrą slaptą simetrinį raktą

Aldona
>> **VB**=mod_exp(sB,eB,nB)
VB=67527455
>> tB==VB
ans = 1 ← jeigu **1** parašas galioja
>> **kAB**=mod_exp(tB,u,p)
kAB = 215173946

Bronius
>> **VA**=mod_exp(sA,eA,nA)
VA=234887359
>> tA==VA
ans = 1 ← jeigu **1** parašas galioja
>> **kBA**=mod_exp(tA,v,p)
kBA = 215173946

$$k_{AB} = 215173946 = k_{BA}$$

P.S
Kadangi buvote už Bronių ir Aldoną, kad patikrintumėte, ar teisingai apskaičiavote bendrą slaptą simetrinį raktą, įsitikinkite, kad galioja sąlyga $k_{AB} = k = k_{BA}$:

>> **kAB == kBA**
ans=1 ← jeigu **1** bendras slaptas simetrinis raktas teisingas

Užduotys Autentifikuotam KAP su RSA parašais.

Žemiau esančioms užduotims naudokite šiuos viešus parametrus ir Aldonos ir Broniaus RSA raktų poras.

1. Turėdami **Aldonos** slaptą parametrą u, apskaičiuokite viešą sesijos parametrą t_A ir jam suformuokite parašą $\sigma_A = (s_A)$, naudojant pateiktas reikšmes:

   1. u=int64(171749124);
   2. u=int64(108124069);
   3. u=int64(137026270);
   4. u=int64(182373318).

   Vieši sesijos parametrai t_A ir jiems suformuoti parašai $\sigma_A = (s_A)$:

   1. t_A = 263715831, s_A = 55728759;
   2. t_A = 235392929, s_A = 232894451;
   3. t_A = 123902632, s_A = 263673968;
   4. t_A = 104068868, s_A = 83689066.

2. Turėdami **Aldonos** slaptą parametrą u, patikrinkite gautą iš **Broniaus** sesijos viešo parametro t_B parašą $\sigma_B = (s_B)$ ir apskaičiuokite bendrą slaptą simetrinį raktą, naudojant pateiktas reikšmes:

   1. u=int64(146684763), t_B=int64(103524719), s_B=int64(27663509);
   2. u=int64(104009295), t_B=int64(47576070), s_B=int64(202332120);
   3. u=int64(78700710), t_B=int64(164286595), s_B=int64(234874849);
   4. u=int64(131537269), t_B=int64(44144238), s_B=int64(42051258).

   Parašų galiojimas ir bendri slapti simetriniai raktai k:

   1. Parašas negalioja, k = 176675006;
   2. Parašas galioja, k = 160369819;
   3. Parašas galioja, k = 50051930;
   4. Parašas negalioja, k = 236209858.

Vernamo šifras

(angl. Vernam cipher)

Vernamo šifras (taip pat žinomas kaip vienkartinė juosta, angl. *One-Time Pad*) yra srautinio šifravimo metodas, kuris tam tikromis sąlygomis gali būti absoliučiai saugus. Šis šifravimo metodas naudoja bitų XOR (mod 2 sudėtis) operaciją tarp pradinio teksto bitų ir atsitiktinės bitų sekos, vadinamos šifravimo gama. Pagrindiniai principai:

1. **Šifravimas.** Kiekvienas pradinio teksto bitas t_i yra šifruojamas XOR (žr. 1 lentelę) operacija su atitinkamu atsitiktinės gamos bitu γ_i. Rezultatas yra šifrograma $c_i=t_i \oplus \gamma_i$.
2. **Dešifravimas.** Atlikus tą pačią XOR operaciją tarp šifrogramos ir gamos, galima atkurti pradinį tekstą $t_i=c_i \oplus \gamma_i$.

Vernamo šifras yra absoliučiai saugus, jei galioja šios Klodo Šenono (angl. *Claude Shannon*) suformuluotos sąlygos:

1. Šifravimo gamos (rakto) ilgis turi būti lygus pradinio teksto ilgiui.
2. Šifravimo gama turi būti atsitiktinė, tolygiai pasiskirsčiusi ir statistiškai nepriklausoma.
3. Šifravimo gama turi būti naudojama tik vieną kartą.

Jei šios sąlygos yra išpildytos, turint tik šifrogramą, neįmanoma atkurti pradinio teksto, nes jis neturi jokios atpažįstamos struktūros. Vis dėlto, praktinis šifro įgyvendinimas turi tam tikrų trūkumų, ypač sunkumų generuojant ir saugiai perduodant atsitiktinę gamą, kuri turi būti tokio paties ilgio kaip šifruojamas pranešimas.

1 lentelė. XOR($\oplus$) griežtosios disjunkcijos teisingumo lentelė

A	B	Y
0	0	0
0	1	1
1	0	1
1	1	0

Pavyzdys. Jeigu turime pranešimą **m**=010111010101 ir bendrą slaptą simetrinį raktą ***k***=101101001111, tai atliekant XOR operaciją

$$\begin{array}{rl} & 010111010101 \leftarrow \boldsymbol{m} \\ \oplus & 101101001111 \leftarrow \boldsymbol{k} \\ & 111010011010 \end{array}$$

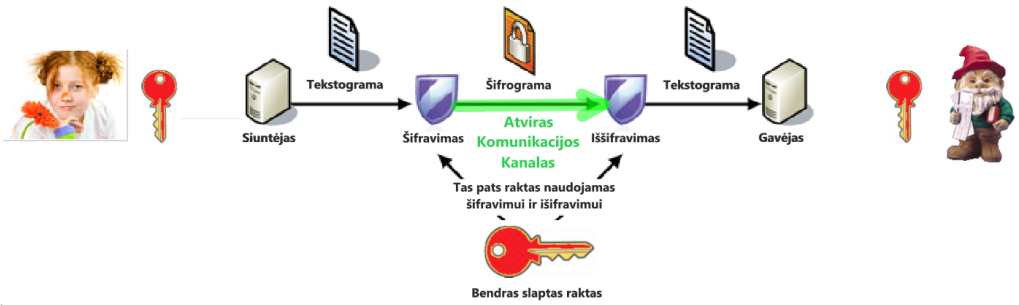
gaunama šifrograma **c**=111010011010.

Simetrinis šifravimas ir iššifravimas naudojant Vernamo šifrą

Aldona užšifruoja pranešimą, kuriame pateikiama pinigų suma ***m***=500 ir siunčia šifrogramą *Ch* Broniui. Bronius gavęs šifrogramą ją iššifruoja ir perskaito pranešimą. Komunikacijos schema naudojant bendrą slaptą simetrinį raktą ***k*** pateikiama 5 pav.

Broniaus pranešimas ***m***:

```
>> m = 500
m = 500
```



5 pav. Aldonos ir Broniaus komunikacija naudojant bendrą slaptą simetrinį raktą

Bronius šifruoja pranešimą ***m*** su bendru slaptu simetriniu raktu ***k***.

1. Paverskite pranešimą į dvejetainę formą:
   >> mb = dec2bin(m)
   mb = 111110100
2. Konvertuoti bendrą slaptą simetrinį raktą ***k*** į dvejetainę formą:
   >> k=kBA
   k=215173946
   >> kb=dec2bin(k)
   kb = 11001101001101001011001110 10
3. Apskaičiuokite dvejetainę šifrogramą **c** atliekant XOR operaciją su dvejetainiu pranešimu ***m*** ir slaptu simetriniu dvejetainiu raktu ***k*** (dvejetainio skaičių ilgis $m_{ilgis} \leq k_{ilgis}$):
   >> c1b = binaryxor(mb, kb)
   c1b = 11001101001101001010110011 10
4. Konvertuoti šifrogramą **c** į dešimtainę formą:
   >> c = int64(bin2dec(c1b))
   c = 215173838
5. Šifrograma **c** pranešimui ***m***:
   Enc(*k*, *m*) = c = 215173838
6. **Bronius** siunčia **Aldonai** šifrogramą **c**.

Aldona iššifruoja gautą šifrogramą **c** su savo bendru slaptu simetriniu raktu ***k*** ir perskaito pranešimą ***ms***.

1. Paverskite šifrogramą **c** į dvejetainę formą:
   >> c2b = dec2bin(c)
   c2b = 11001101001101001010110011 10
7. Paverskite bendrą slaptą simetrinį raktą ***k*** į dvejetainę formą:
   >> k=kAB
   k=215173946
   >> kb=dec2bin(k)
   kb = 11001101001101001011001110 10
2. Apskaičiuokite pranešimą ***m*** dvejetaine forma atliekant XOR operaciją su dvejetaine šifrograma **c** ir slaptu dvejetainiu simetriniu raktu ***k***:
   >> m2b = binaryxor(c2b, kb)
   m2b = 111110100
3. Atkurkite pradinį pranešimą konvertuojant dvejetainį pranešimą į dešimtainę formą:
   ms = bin2dec(m2b)
   ms = 500

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

>> m==ms

ans = 1 ← jeigu **1** buvo užšifruota ir iššifruota teisingai

Užduotys Vernamo šifrui.

1. Turėdami bendrą slaptą simetrinį raktą ***k*** ir šifrogramą **c**, nustatykite, kuris iš toliau esančių pranešimų ***m***, atitinkančių siunčiamą pinigų sumą, **Broniaus** buvo užšifruotas, naudojant pateiktas reikšmes:

   1. ***k***=int64(264221733), **c**=int64(264221912);
   2. ***k***=int64(215173946), **c**=int64(215173913);
   3. ***k***=int64(140522101), **c**=int64(140522423);
   4. ***k***=int64(91379786), **c**= int64(91381142).

   Šifruojami pranešimai ***m***:

   1. ***m*** = 1500;
   2. ***m*** = 253;
   3. ***m*** = 35;
   4. ***m*** = 450.

2. Turėdami bendrą slaptą simetrinį raktą ***k*** ir pranešimą ***m***, atitinkantį pinigų sumą, nustatykite, kuriai iš **Aldonos** gautų šifrogramų **c** apskaičiavimui buvo panaudotos šios reikšmės:

   1. ***k***=int64(154451104), ***m***=253;
   2. ***k***=int64(94037749), ***m***=35;
   3. ***k***=int64(131504832), ***m***=450;
   4. ***k***=int64(21814380), ***m***=1500.

   Šifrogramos **c**:

   1. **c** = 94037718;
   2. **c** = 154451037;
   3. **c** = 131504898;
   4. **c** = 21813680.

3. Kenkėjišku būdu gavę dvi **Broniaus** siunčiamas **Aldonai** šifrogramas $\mathbf{c}_1$ ir $\mathbf{c}_2$, kurios buvo suformuotas naudojant tą patį bendrą slaptą simetrinį raktą ***k*** ir žinant vieną iš šifruojamų tekstogramų, t.y. piniginę sumą $\boldsymbol{m}_1$ dešimtainiame pavidale, nustatykite antrą užšifruotą pinigų sumą $\boldsymbol{m}_2$, naudodamiesi formule $\boldsymbol{m}_2=\mathbf{c}_1\oplus\mathbf{c}_2\oplus\boldsymbol{m}_1$ ir šiomis reikšmėmis:

   1. $\mathbf{c}_1$=int64(21814517), $\mathbf{c}_2$=int64(21814579), $\boldsymbol{m}_1$=351;
   2. $\mathbf{c}_1$=int64(151673848), $\mathbf{c}_2$=int64(151673000), $\boldsymbol{m}_1$=864;
   3. $\mathbf{c}_1$=int64(126161973), $\mathbf{c}_2$=int64(126161478), $\boldsymbol{m}_1$=1936;
   4. $\mathbf{c}_1$=int64(239858008), $\mathbf{c}_2$=int64(239859521), $\boldsymbol{m}_1$=89.

   Užšifruotos pinigų sumos $\boldsymbol{m}_2$:

   1. $\boldsymbol{m}_2$ = 483;
   2. $\boldsymbol{m}_2$ = 1600;
   3. $\boldsymbol{m}_2$ = 48;
   4. $\boldsymbol{m}_2$ = 153.