Turinys

Sąvokos

Kriptografijoje **Aldona** (angl. *Alice*) ir **Bronius** (angl. *Bob*) yra standartizuoti vardai, dažnai naudojami aprašant dviejų subjektų, dalyvaujančių komunikacijoje, veiksmus. **Aldona** paprastai veikia kaip informacijos siuntėja, o **Bronius** – kaip jos gavėjas. Šie vardai plačiai naudojami kriptografinių protokolų ir sistemų paaiškinimui, padedant vizualizuoti saugaus informacijos perdavimo scenarijus.

Papildomai, kriptografiniuose pavyzdžiuose dažnai naudojami ir kiti veikėjai (keletas iš jų):

- **Pasyvi Zosė (**angl. ***Eve*****)** – pasyvus užpuolikas arba stebėtojas, bandantis perimti ar iššifruoti Aldonos ir Broniaus komunikaciją.
- **Aktyvi Zosė (**angl. ***Mallory*****)** – aktyvus užpuolikas, kuris ne tik šnipinėja, bet ir bando pakeisti ar sugadinti komunikaciją.

Ši terminologija naudojama įvairiuose kriptografijos procesuose, pavyzdžiui, šifravime, skaitmeniniuose parašuose ir raktų mainuose, siekiant supaprastinti sudėtingas technines diskusijas.

Difio Helmano raktų apsikeitimo protokolas

(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 tenkinamos dvi sąlygos:

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

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

```
>> p=genstrongprime(28)
p = 187086587
>> isprime(p)
ans = 1
>> q=(p-1)/2
q = 93543293
>> isprime(q)
ans = 1
>> g=2
>> mod_exp(g,q,p)
ans = 187086586
>> g=3;
>> mod_exp(g,q,p)
ans = 1
>> g=4;
>> mod_exp(g,q,p)
ans = 1
```

```
>> 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
```

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

Toliau naudosime p=int64(224013599); g=111.

Bendro simetrinio rakto apskaičiavimas

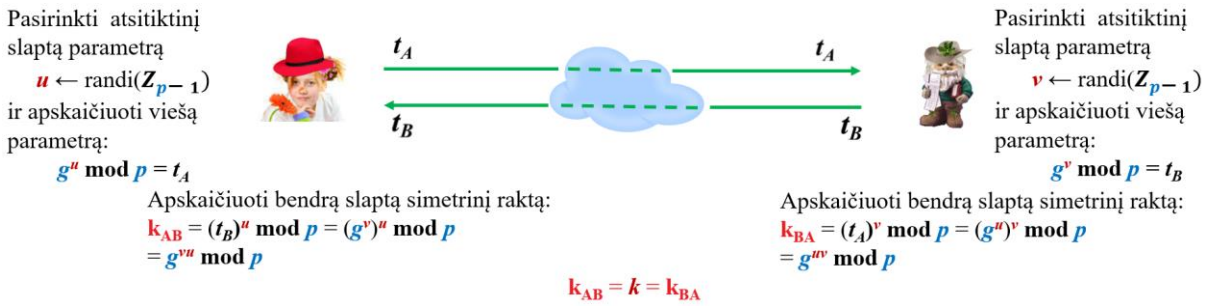
Aldona ir Bronius pasirinkę slaptuosius atsitiktinius parametrus ***u***, ***v***, apskaičiuoja viešus sesijos parametrus $t_A = g^u \bmod p$, $t_B = g^v \bmod p$, kuriuos siunčia per tinklą (žr. 1 pav.) vienas kitam.

1 pav. Aldona ir Bronius apsikeičia viešais sesijos parametrais

Aldona
>> u=int64(randi(2^28-1))
u = 195162450
>> **tA**=mod_exp(g,u,p)
tA = 22053505

Bronius
>> v=int64(randi(2^28-1))
v = 212879876
>> **tB**=mod_exp(g,v,p)
tB = 179573345

Aldona ir Bronius gavę vienas kito viešus sesijos parametrus 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 2 pav.



2 pav. Aldona ir Bronius apskaičiuoja bendrą slaptą simetrinį raktą

Aldona
>> **kAB**=mod_exp(tB,u,p)
kAB = 196960461

Bronius
>> **kBA**=mod_exp(tA,v,p)
kBA = 196960461

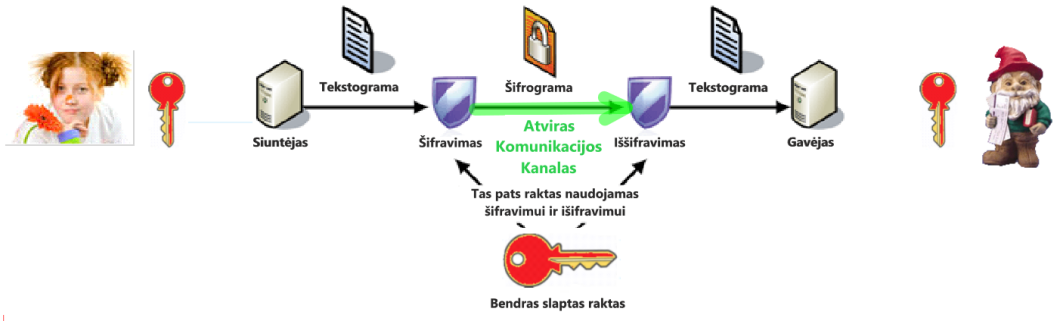
$k_{AB} = 196960461 = k_{BA}$

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

>> **kAB == kBA**
ans=1

Simetrinis šifravimas ir iššifravimas naudojant AES128

Aldona užšifruoja pranešimą *Labas Broniau!* ir siunčia šifrogramą *Ch* Broniui. Bronius gavęs šifrogramą ją iššifruoja ir perskaito pranešimą. Komunikacijos schema naudojant bendrą slaptą simetrinį raktą ***k*** pateikiama 2 pav.



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

Aldona šifruoja

```
>> k=kAB
k = 196960461
>> kh32=dec2hex(k,32)
kh32 = 000000000000000000000000BBD60CD
>> NR=1;
>> fun='e'
fun = e
>> m="Labas Broniau!"
m = Labas Broniau!
>> Ch=AES128(m,kh32,NR,fun)
Ch = 183f15e5d190e4c45756949cda0e5279
```

Bronius iššifruoja

```
>> k=kBA
k = 196960461
>> kh32=dec2hex(k,32)
kh32 = 000000000000000000000000BBD60CD
>> NR=1;
>> fun='d'
fun = d
>> ms = AES128(Ch,kh32,NR, fun)
ms = Labas Broniau!
```

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.

```
>> strcmp(m, ms)
ans = 1 ← jeigu 1 buvo šifruota ir iššifruota teisingai
```

Šifravimui ir iššifravimui naudojamos Octave funkcijos aprašymas pateikiamas 1 lentelėje.

1 lentelė. AES128 Octave funkcija

Funkcija	**Paaiškinimas**	**Pavyzdys**
AES128	Šifruojamas 1 atvirojo teksto 128 bitų ilgio blokas, atitinkantis 16 ASCII simbolių. Parametrai: m(in) – užšifruojama eilutės tipo žinutė; Kh – slaptas simetrinis raktas šešioliktainiu pavidalu; NR – AES128 naudojamų raundų skaičius; fun –"e" eilutės tipo kintamasis, kuriuo iškviečiama šifravimo funkcija, o įvedus "d" iškviečiama dešifravimo funkcija	>> m="Labas Broniau!"; >> Kh=dec2hex(14,32); >> NR=1; >> fun="e" **Šifravimas:** >> C=AES128(m,Kh,NR,fun) C = 018c0376c823368c4e8c82d49b0024f2 **Iššifravimas:** >> fun="d" >> ms=AES128(C,Kh,NR,fun) ms= Labas Broniau!

Octave pateikiamas detalesnis funkcijos **AES128** aprašas:

```
% AES128(in,kh32,NR,fun) Advanced Encryption Standard symmetric cipher with key length of 128 bits
%                 Encryption is performed for 1 block of length 128 bits or 16 ASCII symbols
%
% in - plaintext/ciphertext of string type: maximum 16 symbols or shorter
%
% kh32 - shared secret key in hexadecimal number of length=32 (128 bits)
% kh32 can be obtained when shared decimal key k is given using commands:
%       >> k=int64(randi(2^28))
%       k = 160966896
%       >> kh32=dec2hex(k,32)
%       kh32 = 000000000000000000000000099828F0
%
% NR - Number of Rounds (e.g. Nr = 10)
%      The smaller NR, the lower security of encryption but the speed of encryption is higher
%      The least number of NR is 1 and in this case security lack is evident
```

```
%
% fun - letter determining either encription: fun='e' or decryption: fun='d' functions
%
% Encryption example:
% >> in = 'Hello Bob';
% >> kh32 = '000000000000000000000000099828F0';
% >> NR = 10;
% >> Ch = AES128(in,kh32,NR,'e')
% ASCII_e = ?1~mV                 % ciphertext in ASCII format
% Ch = 0f9a2c08d191310fb27ed16d90f45686   % ciphertext in hexadecimal format
%
% Decryption example:
% >> Dh = AES128(Ch,kh32,NR,'d')
% Dh = 00000000000048656c6c6f7720426f62   % decrypted message in hex format
% D = Hello Bob                   % Decrypted message in ASCII format
```

Žmogaus viduryje ataka

(angl. *Man-in-the-Middle attack, MITM*)

Žmogaus viduryje ataka (*MITM*) yra išpuolis, kai užpuolikas įsiterpia į dviejų šalių (dažniausiai naudotojo ir serverio) komunikaciją be jų žinios. Užpuolikas veikia kaip tarpininkas, perimdamas ir kartais modifikuodamas perduodamus duomenis.

Pagrindiniai etapai:

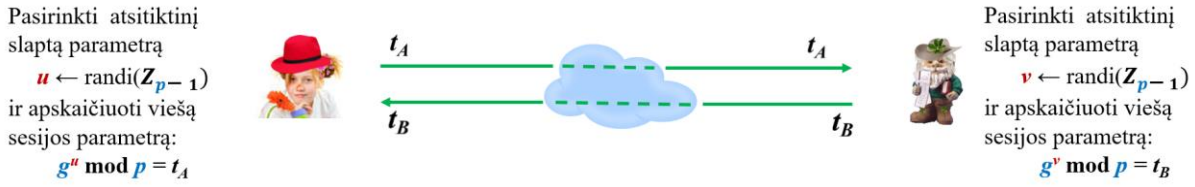
1. **Prisijungimas**. Užpuolikas įsiterpia tarp naudotojo ir serverio, dažnai per nesaugų *Wi-Fi* arba tinklo trūkumus.
2. **Suklastota komunikacija**. Naudotojas ir serveris nežino apie užpuoliką ir mano, kad jie tiesiogiai bendrauja. Tuo metu visi duomenys (pvz., slaptažodžiai, asmeninė informacija) keliauja per užpuoliko įrenginį.
3. **Duomenų perėmimas**. Užpuolikas gali stebėti, perimti, pakeisti, modifikuoti ar pavogti jautrią informaciją.

Ši ataka ypač pavojinga nesaugiuose tinkluose ir kai nėra naudojamas šifravimas, pvz., HTTP vietoje HTTPS.

Toliau naudosime tuos pačius viešuosius parametrus p ir g, kaip ir Difio Helmano raktų apsikeitimo protokole.

Bendro slapto rakto apskaičiavimas

Aldona ir Bronius pasirinkę slaptuosius atsitiktinai sugeneruotus parametrus u, v, apskaičiuoja viešus sesijos parametrus $t_A = g^u \bmod p$, $t_B = g^v \bmod p$, kuriuos siunčia per tinklą (žr. 3 pav.) vienas kitam.



3 pav. Aldona ir Bronius apsikeičia viešais sesijos parametrais

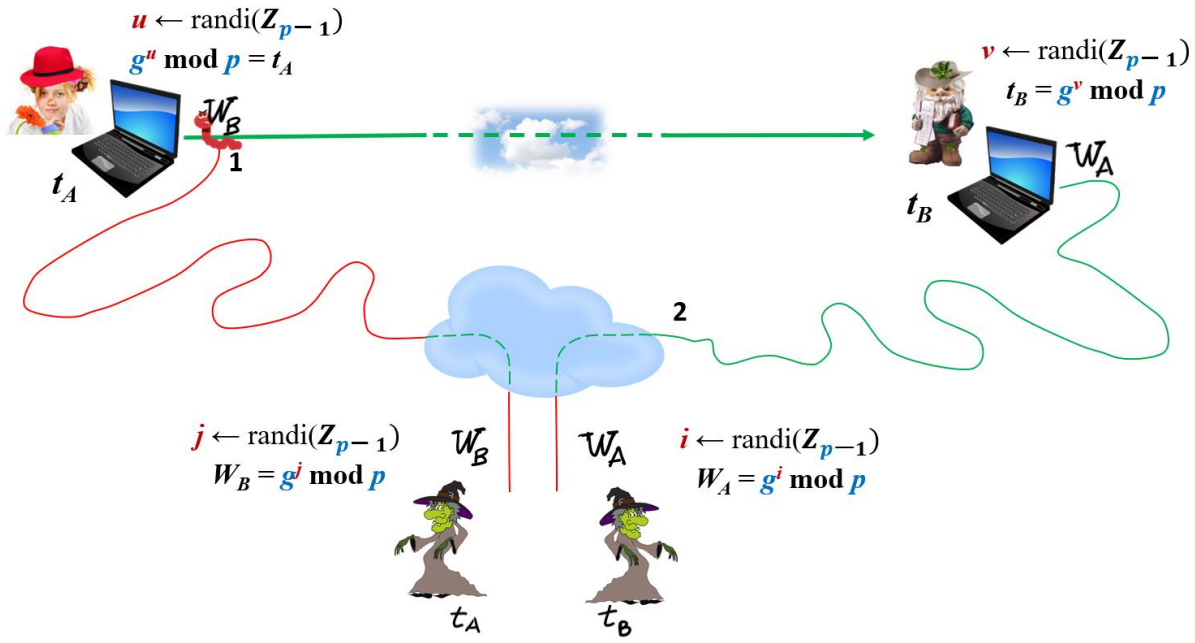
Aldona

```
>> u=int64(randi(2^28-1))
u = 22911896
>> tA=mod_exp(g,u,p)
tA = 27482990
```

Bronius

```
>> v=int64(randi(2^28-1))
v = 52168129
>> tB=mod_exp(g,v,p)
tB = 161452677
```

Aldonai ir Broniui nieko nenumanant į jų komunikaciją įsiterpia ragana Zosė (žr. 4 pav.), prieš tai apkrėtusi kenkėjiška programa Aldonos kompiuterį (kenkėjiška programa vaizduojama, kaip kirmėlė). Ragana Zosė megzdama komunikaciją perima viešus sesijos parametrus t_A ir t_B, atitinkamai pasirenka du slaptus atsitiktinai sugeneruotus parametrus j ir i, apskaičiuoja viešus sesijos parametrus $W_B = g^j \bmod p$ ir $W_A = g^i \bmod p$ ir apsimesdama Broniumi išsiunčia viešą sesijos parametrą W_B Aldonai, o Broniui apsimesdama Aldona išsiunčia viešą sesijos parametrą W_A.

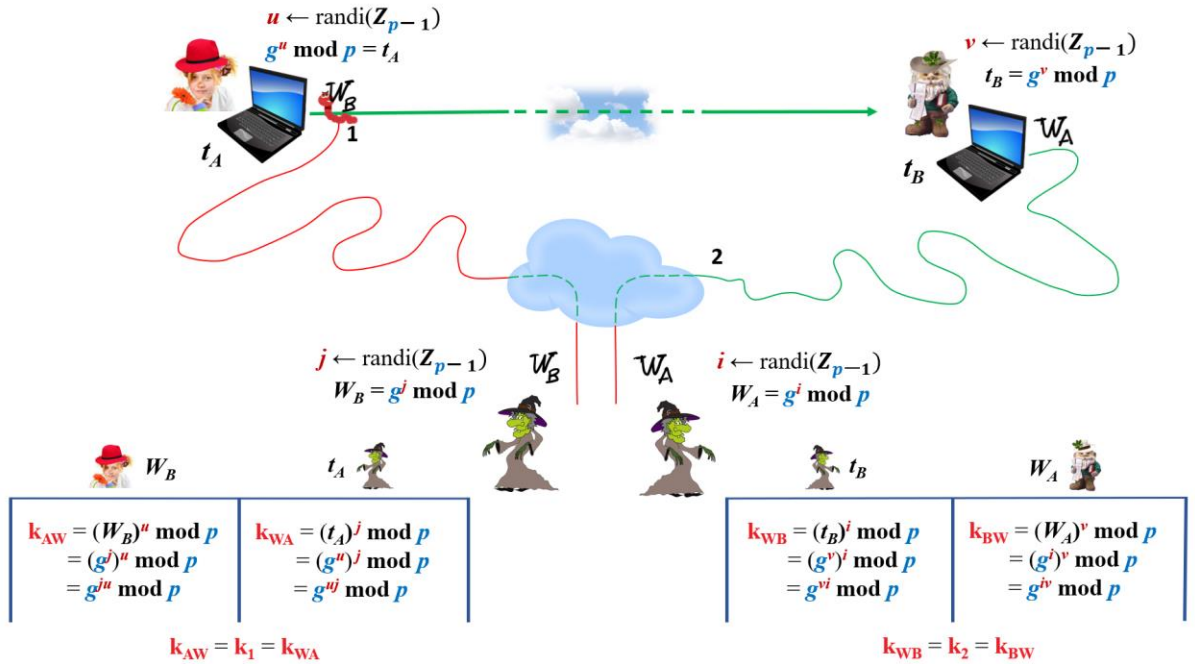


3 pav. Aldona ir Bronius apsikeičia viešais sesijos parametrais su ragana Zose

Ragana Zosė Aldonos pusėje
>> j=int64(randi(2^28-1))
j = 122287213
>> WB=mod_exp(g,j,p)
WB = 15845747

Ragana Zosė Broniaus pusėje
>> i=int64(randi(2^28-1))
i = 233660847
>> WA=mod_exp(g,i,p)
WA = 16659134

Apsikeitę viešais sesijos parametrais Aldona ir ragana Zosė, Bronius ir ragana Zosė, kiekvienas apskaičiuoja bendrą slaptą simetrinį raktą k. Aldona skaičiuoja $k_{AW} = (W_B)^u \bmod p$, ragana Zosė skaičiuoja $k_{WA} = (t_A)^j \bmod p$ ir $k_{WB} = (t_B)^i \bmod p$, Bronius skaičiuoja $k_{BW} = (W_A)^v \bmod p$. Platesni skaičiavimai pateikiami 4 pav.



4 pav. Aldona ir ragana Zosė, Bronius ir ragana Zosė apskaičiuoja bendrą slaptą simetrinį raktą

Aldona
>> kAW=mod_exp(WB,u,p)
kAW = 219711167

Ragana Zosė
>> kWA=mod_exp(tA,j,p)
kWA = 219711167
>> kWB=mod_exp(tB,i,p)
kWB = 37826712

Bronius
>> kBW=mod_exp(WA,v,p)
kBW = 37826712

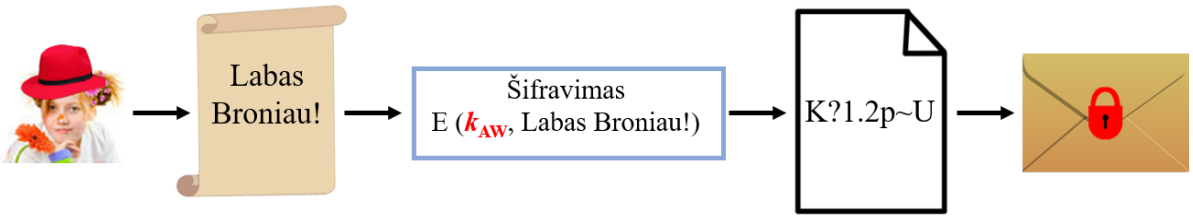
$k_{AW} = 219711167 = k_{WA}$ $k_{WB} = 37826712 = k_{BW}$

P.S
Kadangi buvote už Bronių, Aldoną, raganą Zosę, kad patikrintumėte, ar teisingai apskaičiavote bendrą slaptą simetrinį raktą tarp Aldonos ir Zosės, tarp Broniaus ir Zosės, turi būti tenkinamos sąlygos $k_{AW} = k_1 = k_{WA}$ ir $k_{WB} = k_2 = k_{BW}$:

>> kAW == kWA
ans=1
>> kWB == kBW
ans=1

Simetrinis šifravimas ir iššifravimas

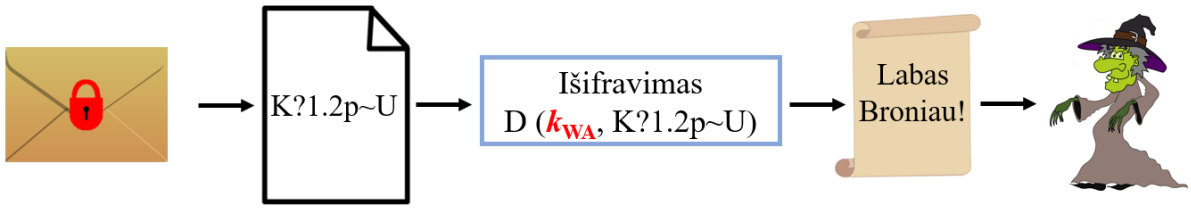
Aldona užšifruoja pranešimą *Labas Broniau!* su slaptu simetriniu raktu k_{AW} ir siunčia šifrogramą Ch_A Broniui. Aldonos pranešimo šifravimo schema pateikiama 5 pav.

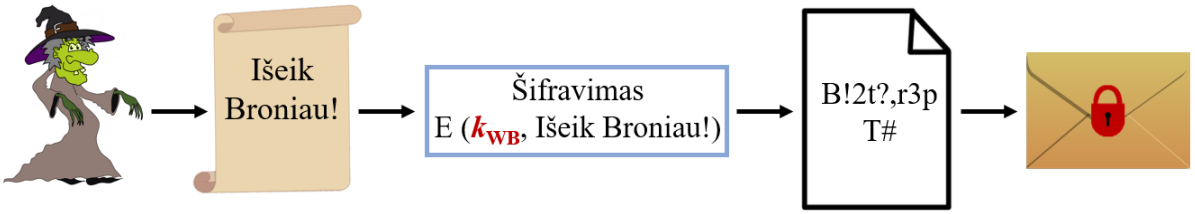


5 pav. Aldona užšifruoja pranešimą ir jį išsiunčia Broniui

Aldona šifruoja pranešimą
>> khAW=dec2hex(kAW,32)
khAW = 0000000000000000000000000D1886BF
>> NR=1;
>> fun='e'
fun = e
>> m="Labas Broniau!"
m = Labas Broniau!
>> ChA=AES128(m, khAW,NR,fun)
ChA = cfaba0dc0604053880f22160e23f01f7

Ragana Zosė perima Aldonos siunčiamą šifrogramą Ch_A, ją iššifruoja su slaptu simetriniu raktu k_{WA} ir perskaito pranešimą. Perskaičius pranešimą, jį modifikuojama pakeisdama tekstą iš *Labas Broniau!* į *Išeik Broniau!* ir užšifruoja su slaptu simetriniu raktu k_{WB} ir siunčia šifrogramą Ch_W Broniui. Raganos Zosės šifravimo ir iššifravimo schema pateikiama 6 pav.





6 pav. Ragana Zosė iššifruoja pranešimą, jį perskaito ir modifikavus užšifruoja naują pranešimą, kurį išsiunčia Broniui

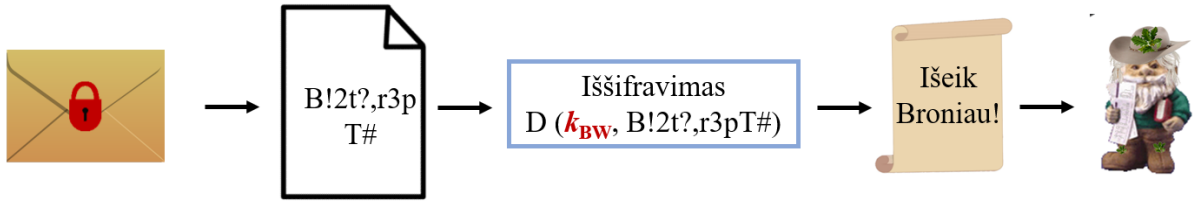
Ragana Zosė perskaito pranešimą

```
>> khWA=dec2hex(kWA,32)
khWA = 000000000000000000000000D1886BF
>> NR=1;
>> fun='d'
fun = d
>> ma = AES128(ChA,khAW,NR, fun)
ma = Labas Broniau!
```

Ragana Zosė keičia pranešimą

```
>> khWB=dec2hex(kWB,32)
khWB = 00000000000000000000000002413098
>> fun='e'
fun = e
>> mw="Išeik Broniau!"
mw = Išeik Broniau!
>> ChW=AES128(mw,khWB,NR,fun)
ChW = e1fdee21cf442845aeb3e0c0ff7e0970
```

Bronius gavęs šifrogramą *Chw* ją iššifruoja su slaptu simetriniu raktu k_{BW} ir perskaito pranešimą. Broniaus pranešimo iššifravimo schema pateikiama 7 pav.



7 pav. Bronius iššifruoja pranešimą ir jį perskaitęs išeina

Bronius perskaito pranešimą

```
>> khBW=dec2hex(kBW,32)
khBW = 00000000000000000000000002413098
>> NR=1;
>> fun='d'
fun = d
>> ms = AES128(ChW, khBW,NR, fun)
ms = Išeik Broniau!
```

P.S.
Kadangi buvote už Bronių, Aldoną, Ragana Zosę, galite palyginti pradinę pranešimo reikšmę su gauta reikšme ir sužinoti ar pranešimas buvo pakeistas.

```
>> strcmp(m, ms)
ans = 0 ← jeigu 0 pranešimas buvo pakeistas
```