ISSN 1392 - 1215 ELEKTRONIKA IR ELEKTROTECHNIKA. 2004. Nr. 7(56)

T 180 TELEKOMUNIKACIJŲ INŽINERIJA

Kriptografijos seanso iniciacijos protokolas

S. Japertas
Krašto apsaugos ministerija
Šv. Ignoto g. 8/29, LT-01120 Vilnius, Lietuva
P. Nefas,
Vyriausybinių ryšių centras prie valstybės Saugumo departamento Kauno sk.
Laisvės al. 14, LT-44001 Kaunas, Lietuva
R. Jankūnienė
Telekomunikacijų katedra, Kauno technologijos universitetas
Studentų g. 50, LT-51368 Kaunas, Lietuva

Įvadas

Lietuvai įsijungus į europines ir tarpatlantines organizacijas, kyla klausimas, kaip keistis slapta valstybine ir tarnybine informacija tiek su Lietuvos, tiek su užsienio institucijomis. Vienas iš būdų saugiam informacijos perdavimui užtikrinti yra kriptografinių metodų taikymas.

Kriptografinę sistemą (KS) suprantame kaip lokaliai, teritoriškai ar globaliai pasiskirsčiusią informacinę sistemą, sudarytą iš atvirų ryšio linijų ir aptarnaujančią didelę grupę kriptografinių subjektų.

Nagrinėsime tam tikrą subjektų grupę, kurios nariai turi šiuos kriptografinius raktus: uždarą raktą (UR) ir atvirą (grupinį) raktą (AR). Kartu įvedama seansinio rakto (SR), kurį subjektai sukuria tarpusavyje iniciacijos protokolo metu ir kuris yra skirtas informacijai šifruoti, sąvoka. Kalbant apie UR ir AR sąvokas, nenagrinėjami skirtumai tarp simetrinės ir asimetrinės kriptografijų, ypač, kai pabrėžiama, kad geroje KS gali būti naudojamos abi kriptografijos rūšys [1]. Todėl šiame darbe naudojamos abiejų kriptografijų metodologinės galimybės, kuriant KS elementus. Pateikta vieno iš KS elemento – iniciacijos protokolo schema. Iniciacijos protokolas skirtas kriptografinio ryšio seansui pradėti tarp kriptografinių subjektų. Šiam protokolui realizuoti būtina, kad kiekvienas subjektas turėtų po UR ir AR porą. Tokias poras generuoja raktų paskirstymo centras (RPC) [2, 3], kuris yra KS sudėtinė dalis. Būtent RPC, paskirstydamas raktus, atlieka svarbią užduotį, užtikrinant saugų KS funkcionavimą. Šiame darbe aprioriškai laikoma, kad grupės subjektai jau turi UR ir AR poras. Tariama, kad nagrinėjamos grupės viduje AR jau padalyti, todėl teigiama, kad AR yra atviras raktas tik konkrečioje grupėje.

Iniciacijos protokolo fazės

Vyksta seansas tarp dviejų subjektų *A* ir *B*. Tarkim, *A* pradeda kriptografinį seansą, vykdydamas iniciacijos protokolą, ir jo tikslas yra nusiųsti šifruotą informaciją subjektui *B*. Siūloma įvesti tris iniciacijos protokolo fazes.

Subjektų tarpusavio sinchronizacija OSI (Open Systems Interconnect) protokolų lygmenyje. Paprastai tai atliekama fiziniame, kanaliniame ir transporto lygmenyse. Priklausomai nuo protokolo yra įvairių sinchronizacijos variantų, neatsižvelgiant į tai, koks informacijos srauto padalijimas: paketinis, laikinis ar dažninis. Todėl sinchronizacija šiuo atveju suprantama apibendrinta prasme. Sinchronizacijos fazė iniciacijos protokole reiškia subjekto *A* pasiųstą sinchronizacijos signalą subjektui *B* ir tai, kad subjektas *B* gauna šį signalą.

Autentifikavimo - autorystės nustatymo protokolas (Entity Autentification) [1, 2, 3]. Subjektas *A* subjektui *B* įrodo, kad jis išties yra subjektas *A*, o subjektas *B* įsitikina, kad taip yra iš tiesų. Galima tvirtinti, kad autentifikavimo protokolas šiuolaikinėje kriptografijoje yra vienas iš svarbiausių, todėl skiriama ypač daug dėmesio, siekiant efektyviai naudoti jį informacinėse sistemose. Autentifikavimo atsparumui kriptografiniu požiūriu naudojamos tiek organizacinės, tiek techninės priemonės. Techninėms priemonėms priklausytų specialiai kuriami protokolai, vadinami nulinio atskleidimo įrodymais (ZKP – Zero Knowledge Proof) [1, 4, 5]. Efektyviausia ir praktikoje pasitvirtinusia organizacine priemone yra laikoma trečiosios patikimos šalies (TTP – Third Trusted Party) tarnyba [1, 2, 3]. Pasinaudodamas TTP, subjektas *B* įsitikina, kad subjektas *A* išties yra subjektas *A* ir atvirkščiai.

Raktų apsikeitimas, kada abu subjektai apsikeičia seansiniais kriptografiniais raktais informacijai šifruoti ir dešifruoti. Apsikeičiama tiek pasinaudojus TTP paslaugomis, tiek tiesiogiai tarp pačių subjektų *A* ir *B*. Kriptografiniam atsparumui padidinti rekomenduojama taikyti abu apsikeitimo būdus.

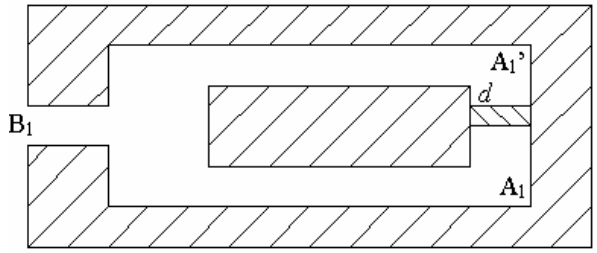
Autentifikavimo protokolas

Kaip anksčiau sakėme, šis protokolas sudaromas panaudojant pagalbinį ZKP protokolą, kuris savo ruožtu laikomas svarbiu kriptografiniu primityvu, naudojamu ne

tik subjektams autentifikuoti, bet ir kitiems autentifikavimo uždaviniams spręsti [1, 4, 5].

Pateiktas formalizuotas ir apibendrintas šio protokolo aprašymas, tinkantis daugeliui įrodymo uždavinių atliekant kriptografinę analizę. Atskiras ZKP uždavinys - pagal pateiktą protokolo aprašymą įrodyti diskretinio logaritmo reikšmės žinojimą, neatskleidžiant pačios tos reikšmės. Ši reikšmė asimetrinėje kriptografijoje naudojama kaip UR.

Norint geriau suvokti autentifikavimo uždavinį, tikslinga pateikti ZKP schemos interpretaciją, kurią pirmą kartą paskelbė grupė Prancūzijos kriptografų konferencijoje CRYPTO 89.



1 pav. Labirinto modelis

Tarkime, subjektas *A* žino kodą, kuriuo atidaromos labirinto durys *d* (1 pav.). Sakykime, *A* pageidauja įrodyti subjektui *B*, kad jis žino tą kodą, tačiau nenori jo atskleisti. Tam įrodyti pasirenkama schema: pradiniu laiko momentu *A* ir *B* subjektai užima pozicijas. Tada *A* atsitiktinai pasirenka arba kairįjį, arba dešinįjį koridorių ir nueina prie durų *d* iš kairės – į poziciją A_1' arba iš dešinės - į poziciją A_1. Tarkim, *A* pasirinko poziciją A_1. Tada *B* ateina į poziciją B_1 ir atsitiktinai (tą pasirinkimą galima koduoti vienu bitu *b* su reikšmėmis {0,1}) nurodo *A* eiti pas jį kairiuoju ($b=0$) arba dešiniuoju ($b=1$) koridoriumi. Jei $b=1$, tai A, net nežinodamas kodo, grįš pas *B* tuo pačiu keliu, kaip ir buvo nuėjęs. Tačiau jei $b=0$, tai tuo atveju *B* galės grįžti pas *B* tik tada, jei žinos duris *d* atidarantį kodą. Jei *A* nežino kodo, tai tikimybė, kad *A* sumeluos, yra 1/2. *B*, norėdamas turėti didesnes garantijas, kad *A* žino kodą, lieps subjektui *A* kartoti tą eksperimentą *n* kartų. Tada subjektas *A* kiekvieno eksperimento metu užims po vieną iš dviejų skirtingų pozicijų: $\{A_2, A_2'\}, \{A_3, A_3'\}, \ldots, \{A_n, A_n'\}$. Po *n* bandymų tikimybė, kad *A* apgaus *B*, yra lygi 1/2.

Pateikta interpretacija vadinama iteracine ZKP schema. Ši schema nepatogi tuo, kad tarp *A* ir *B* turi būti daug kreipčių. Todėl sukurtos tokios ZKP schemos, kurios naudoja tik vieną iteraciją. Tokios schemos pavyzdžiu galėtų būti schema, pateikta [4]. Šiame darbe nagrinėjama apibendrinta neiteracinė ZKP schema ir pagal tą schemą sudaromas apibendrintas autentifikavimo protokolas. Protokolas sudaromas keliais etapais.

I etapas. Tai protokolo pradinių sąlygų etapas. Tarkim, *A* turi UR, sudarytą iš dviejų parametrų – $UR=\{u_0,u_1\}$ ir AR, susidedančio iš trijų parametrų – $AR=\{a_0,a_1,f\}$. Funkcija *f* apibrėžiama kaip vienkryptė funkcija, kuri vektorinę erdvę V^n atvaizduoja ja pačia, t.y. *f*: $V^n \to V^n$, kai bet kuriam a V^n egzistuoja toks a_0 V^n, kad $a_0 = f(a)$. Be to, į funkciją *f* įterpiamas parametrų vektorius $p=\{p_1, p_2 p_3\}$, nuo kurio priklausys funkcijos $f(a_0)$ vertė. Tada galima užrašyti $a_0 = f(p,a)$. Norint pabrėžti faktą, kad *f* reikšmės apskaičiuojamos, esant tam tikroms nustatytoms *p* komponentėms, pvz., p_1 ir p_3, naudojamas užrašas $a_{13} = f(p_1, p_3, a_0)$. Laikoma, kad $a_0 = f(p_1, p_2, u_0) = a_{12}$, kai $p_1 = \varphi(a_1, u_1)$, o φ – abipusiškai vienareikšmė funkcija. Parametras p_1 nusakomas iš anksto.

II etapas. Šiame etape nustatoma, kokį žinojimo lygį turi įrodyti subjektas *A*. Autentifikuojant, *A* turi įrodyti savo tapatumą. Kriptografiniu požiūriu tai galima suformuluoti taip: *A* turi įrodyti, kad jis žino savo UR, pateikdamas subjektui *B* savo SR ir įrodymo metu neatskleisdamas savojo UR.

III etapas. Tai ZKP schemos sudarymas. Informacijos siuntimas iš *A* į *B* žymimas $A \to B$, o siunčiami parametrai pavaizduojami laužtiniuose skliaustuose. Atliekami šie žingsniai:

$$A \to B \ [u_2 = f(p_2, u_0)], \tag{1}$$

$$B \to A \ [p_3], \tag{2}$$

$$A \to B \ [a_{123} = f(p_1, p_2, p_3, a_0)]. \tag{3}$$

čia *A, B* – sugeneruoti atsitiktiniai skaičiai.

Po trečiojo žingsnio *B* turi patikrinti *A* autentiškumą, t. y. ar *A* subjekto AR atitinka jo UR. Tam tikslui *B* turi apskaičiuoti $f(p_3, a_{123})$. Funkcija φ turi „neprieštarauti“ alternatyvoms. Jei

$$f(p_3, a_{123}) = f(p_2, u_0) = u_2, \tag{4}$$

B įsitikino *A* autentiškumu, jei:

$$f(p_3, a_{123}) \neq f(p_2, u_0) = u_2, \tag{5}$$

B nustatė, kad $AR=\{a_0, a_1, f\}$ neatitiko $UR=\{u_0, u_1\}$ ir todėl subjektas *A* nebuvo autentifikuotas.

Autentifikavimo protokolo analizė

Autentifikavimo protokolo kriptografinis atsparumas kriptoanalizei priklauso nuo funkcijos *f* savybių. Jei, pvz., ši funkcija *f* yra rodyklinė funkcija moduliui *p*, tai pirmojo žingsnio metu įsibrovėlis *X*, perrinkdamas įvairias galimas atsitiktines p_2 reikšmes, turi atlikti diskretinį logaritmavimą. Tai matematiškai sudėtinga. Pateikta ZKP apibendrinta schema aptariamu požiūriu yra pakankamai kriptografiškai atspari.

Analizuojamos galimos situacijos, kai tarp *A* ir *B* subjektų yra įsibrovėlis *X*, kuris gali registruoti ir retransliuoti šių subjektų informacijos srautus. *X* gali būti aktyvus arba pasyvus įsibrovėlis. Esant aktyviam įsibrovimui, ir pakeitus bent vieną iš perimtų signalų u_2, p_3 ar a_{123}, subjektas *B* nustatys antrą alternatyvą ir subjektas *A* nebus autentifikuotas. Taip *X* atliks sabotažo funkcijas, t. y. neleis subjektui *A* autentifikuotis. Pasyvaus įsibrovimo atveju *X* gali nieko nekeisdamas retransliuoti protokolą tarp *A* ir *B*. Kaip buvo minėta, bet koks jo

įsikišimas į protokolo eigą bus neišvengiamai identifikuotas. Tačiau, retransliuodamas protokolą, *X* gali prisistatyti subjektui *B* kaip subjektas *A* ir subjektas *B* turės jį autentifikuoti, nes tai atitiks pirmąją alternatyvą. Sulaukęs protokolo pabaigos, *X* galės įsiterpti į kitą iniciacijos protokolo fazę – seansinio rakto tarp *A* ir *B* generavimą. Kaip to galima išvengti, aptariama toliau.

Seansinių raktų protokolas

Nagrinėjamas klasikinis seansinių raktų apsikeitimo protokolas, kuris remiasi Diffie ir Hellman [1,2,3,4] protokolu arba jo modifikacijomis (pvz., [4]).

Subjektai *A* ir *B* parenka pakankamai didelius pirminius skaičius *p* ir *g*. Nuo šių skaičių dydžio priklauso protokolo kokybė, t. y. kriptografinis atsparumas. Pirminis skaičius *p* apibrėžia baigtinį Galua lauką $GF(p)$, o *g* yra to lauko generatorius, kuris gali sugeneruoti visus lauko elementus $p \cdot g$ kartų. Diffie ir Hellman protokolas remiasi *g* kėlimu sveikuoju laipsniu, kai rezultatas yra apskaičiuojamas *p* moduliu:

$$A \to B \quad \left[a = g^{\alpha} (\mathrm{mod}\, p)\right], \tag{6}$$

$$B \to A \quad \left[b = g^{\beta} (\mathrm{mod}\, p)\right]; \tag{7}$$

čia α yra *A* subjekto generuotas atsitiktinis skaičius,

β yra *B* subjekto generuotas atsitiktinis skaičius.

A apskaičiuoja:

$$SR_{AB} = b^{\alpha} (\mathrm{mod}\, p) = g^{\alpha\beta} (\mathrm{mod}\, p). \tag{8}$$

B apskaičiuoja:

$$SR_{BA} = a^{\beta} (\mathrm{mod}\, p) = g^{\alpha\beta} (\mathrm{mod}\, p). \tag{9}$$

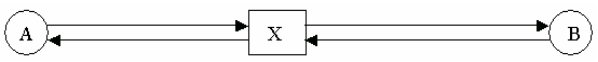
Kadangi $SR_{AB} = SR_{BA} = g^{\alpha\beta} (\mathrm{mod}\, p)$, tai subjektai *A* ir *B* nustatė tarpusavio SR.

Seansinių raktų protokolų analizė

SR protokolo atsparumą kriptoanalizei nusako sudėtingas diskretinio logaritmavimo uždavinys. Todėl galima teigti, jog jo kriptografinis atsparumas priklauso nuo to, kokie naudojami protokolo parametrai, ir nuo naudojamų diskretinio logaritmavimo algoritmų efektyvumo.

Tarkime, *X* – pasyvus įsibrovėlis tarp *A* ir *B*, norintis nustatyti jų SR. Šiuo atveju *X* gali turėti tik skaičius (6) ir (7). Norint rasti (8), reikia spręsti vieną iš dviejų diskretinio logaritmavimo uždavinių: $\alpha = \lg a$ arba $\beta = \lg b$. Tačiau tikimybė, kad *X* sugebės tą uždavinį išspręsti per laiko tarpą, kol SR_{AB} šifruota informacija yra aktuali, nedidelė. Laikome, kad surasti SR generavimo parametrai yra pakankamai geri. Tad pasyvusis *X* negalės pasiekti savo tikslų.

Kai įsibrovėlis *X* aktyvus, tai, kaip minėta anksčiau, antrojo žingsnio metu būdamas tiktai pasyvus, jis galėtų subjektui *B* prisistatyti kaip subjektas *A*. Tada III žingsnyje jis galėtų pasiekti tam tikrų rezultatų. Šie rezultatai reiškia, kad *X* galėtų dešifruoti pranešimus, subjekto *A* pasiųstus subjektui *B*, pastarajam nusiųsdamas savo užšifruotą informaciją. Tokio pobūdžio įsibrovimą įprasta vadinti „žmogumi viduryje“ (angliškai „Man in the Middle“). Šio įsibrovimo schema parodyta 2 pav.



2 pav. Įsibrovimo „žmogus viduryje“ modelis

Įsibrovimo algoritmas toks:

$$A \to X \quad \left[a = g^{\alpha} (\mathrm{mod}\, p)\right], \tag{10}$$

$$X \to B \quad \left[x = g^{\alpha} (\mathrm{mod}\, p)\right], \tag{11}$$

$$B \to X \quad \left[b = g^{\beta} (\mathrm{mod}\, p)\right], \tag{12}$$

$$X \to A \quad SR_{AX} = a^{X} (\mathrm{mod}\, p) = g^{\alpha X} (\mathrm{mod}\, p), \tag{13}$$

$$X \to B \quad SR_{BX} = b^{X} (\mathrm{mod}\, p) = g^{bX} (\mathrm{mod}\, p); \tag{14}$$

čia *x* yra įsibrovėlio *X* sugeneruotas skaičius.

Vietoj bendrojo rakto (8) ryšio tarp *A* ir *B* subjektų seanso metu atsiranda du raktai $SR_{AX} = g^{\alpha X} (\mathrm{mod}\, p)$ ir $SR_{BX} = g^{\beta X} (\mathrm{mod}\, p)$. Nei *A*, nei *B* nežino, kad jie turi skirtingus SR, kuriuos jiems sugeneravo *X*. Nuo to momento *X* gali visiškai kontroliuoti šifravimo ir dešifravimo procesą tarp *A* ir *B*. Kai *A* siunčia subjektui *B* raktu SR_{AX} šifruotą informaciją, *X* ją dešifruoja. Po to *X* paruošia dezinformaciją, užšifruoja ją raktu SR_{BX} ir pasiunčia subjektui *B*. Subjektas *B* dešifruoja dezinformaciją su SR_{BX} ir priima ją kaip tikrą.

Įsibrovimo prevencija

Panagrinėkime aktyvaus įsibrovimo prevenciją II ir III žingsnių metu. Kaip minėta, jei autentifikavimo fazėje įsibrovėlis *X* yra tik pasyvus, jo galima žala gali pasireikšti tik trečiajame žingsnyje – SR protokolo metu. Prevencijai galima panaudoti šias priemones:

1. Subjektas *A* papildo AR komponentę u_0 papildoma komponente u_X, skirta kovai su *X*. Pastarąją subjektas *A* perduoda subjektui *B* kokiu nors kitu būdu ar slaptu kanalu, kuriame tuo momentu nėra įsibrovėlio *X*. Kitaip sakant, parametro u_X įsibrovėlis *X* nežino.

2. Įsteigiama trečioji šalis (TTP), kuria pasitiki abu subjektai *A* ir *B*. Be to laikoma, kad *X* negali įsibrauti tarp *A* - TTP ir tarp *B* - TTP. Šiais TTP saugiais kanalais yra perduodamas komponentas u_X.

Aktyvaus įsibrovimo atveju II žingsnyje subjektas *B* nustato, kad *A* nėra autentiškas. Tada *B* kreipiasi į TTP. Pastarasis nustato, kad *A* nori užmegzti seansą su *B* ir kad *A* yra autentiškas. Apie įsibrovėlį *X* informuojama tinklo apsaugos tarnyba.

Trečiajame žingsnyje *A* ir *B* turi nustatyti, kad SR protokolo metu pas juos atsirado skirtingi raktai SR_{AX} ir SR_{BX}. Arba, atvirkščiai, *A* ir *B* turi įsitikinti, kad jie turi vieną ir tą patį raktą SR_{AB}. Tuo tikslu SR protokolas turi apimti šiuos papildomus veiksmus:

$$\begin{cases} A \to B\left[\mathrm{u}_X(SR_{AB})\right] \\ B \to A\left[\mathrm{u}_X(SR_{BA})\right] \end{cases}; \tag{15}$$

čia $u_X(SR)$ reiškia SR šifravimo operaciją su papildomu atviru raktu u_X.

Jeigu *A* nustato, kad $u_X(SR_{AB}) \neq u_X(SR_{BA})$, tai akivaizdu, kad *B* nustato tą patį. Tuo atveju abu subjektai kreipiasi į TTP, informuodami apie susidariusią situaciją ir tolesnis kriptografinis seansas nutraukiamas.

Išvados

1. Pasiūlytas kriptografinio seanso iniciacijos protokolas, susidedantis iš trijų organiškai susijusių fazių (žingsnių).
2. Pateikti kriptografiniai primityvai, leidžiantys realizuoti II ir III iniciacijos protokolo fazes (žingsnius).
3. Atlikta II ir III fazių bei įsibrovimo prevencijos analizė, kuri leidžia pagrįsti šių fazių įtraukimą į iniciacijos protokolą ir jų organišką sąsają.
4. Iniciacijos protokolo kriptografinis atsparumas paremtas reikalavimais, kad:

a) egzistuoja papildomas saugus informacijos kanalas;

b) funkcionuoja TTP;

c) įsibrovėlis *X* negali įsiterpti tarp *A* - TTP bei *B* - TTP.

Literatūra

1. **Шнайер Б.** Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Изд. ТРИУМО, 2002. – 816 с.
2. **Чмора А.** Современная прикладная криптография. – М.: Гелиос АРВ, 2002. – 256 с.
3. **Бернет С., Пэйн С.** Криптография. Официальное руководство RSA Security. – М.: Бином-Пресс, 2002 – 384 с.
4. **Menezes A., P van Oorschot, Vanstone S.** Handbook of Applied Cryptography. – CRC Press, 1996. – 780 p.
5. **Fiat A., Shamir A.** How to prove yourself: Practical Solutions to Identification and Signature Problems// Advances in Cryptology // CRYPTO'89 Proceedings, Springer – Verlag. – P. 186–194.

Pateikta spaudai 2004 09 14

S. Japertas, P. Nefas, R. Jankūnienė. Kriptografijos seanso iniciacijos protokolas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2004. – Nr. 7(56). – P. 80-83.

Nagrinėjami aktualūs kriptografinių metodų taikymo, keičiantis slapta informacija, klausimai. Pasiūlytas iš trijų organiškai susijusių fazių susidedantis kriptografinio seanso iniciacijos protokolas, kurio atsparumas yra paremtas tam tikrais reikalavimais: yra papildomas saugus informacijos kanalas; funkcionuoja trečioji – patikima šalis bei įsibrovėlis negali įsiterpti tarp sąveikaujančių subjektų ir trečiosios – patikimosios šalies. Pateikti kriptografiniai primityvai, leidžiantys realizuoti II ir III iniciacijos protokolo fazes (žingsnius). Atlikta II ir III fazių bei įsibrovimo prevencijos analizė, kuri leidžia pagrįsti šių fazių įtraukimą į iniciacijos protokolą. Il. 2, bibl. 5 (lietuvių kalba; santraukos lietuvių, anglų ir rusų k.).

S. Japertas, P. Nefas, R. Jankūnienė. A Initiation Protocol for Crypto Graphical Session // Electronics and Electrical Engineering. – Kaunas: Technologija, 2004. – No. 7(56). – P. 80-83.

This article presents the analysis of using cryptographic methods for sensitive information interchanging. It is proposed the initiation protocol for crypto graphical session that security is based on certain demands: the channel must exist, which is additional and save, the functioning of trusted third party must be and adversary can't interfere between subjects interact and the third, i.e. trusted party. The cryptography primitives are proposed, that allow realizing the second and third phases of initiation protocol. Besides, the analysis of second and third protocol phases and prevention of cracking is done. That permits motivated involving of these phases on to initiation protocol. Ill. 2, bibl. 5 (in Lithuanian; summaries in Lithuanian, English and Russian).

С. Япертас, П. Нефас, Р. Янкунене. Протокол инициации криптографического сеанса // Электроника и электротехника. – Каунас: Технология, 2004. – № 7(56). – С. 80-83.

Анализируются актуальные вопросы использования криптографических методов для обмена актуальной секретной информации. Предъявлен протокол инициации криптографического сеанса, который составляется из трех органично связанных фаз и устойчивость которого основана на оговоренных требованиях: существует дополнительный безопасный канал информации; функционирует третья – надежная сторона и взломщик не может внедрится между взаимодействующими сторонами и третьей – надежной стороной. Даны криптографические примитивы, позволяющие выполнить II и III фазы (шаги) протокола. Сделан анализ II и III фаз и превенций взлома, который позволяет обосновать включение этих фаз в протокол инициации. Ил. 2, библ. 5 (на литовском языке; рефераты на литовском, английском и русском яз.).