ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
КІЛТТЕРДІ БАСҚАРУ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ
2-бөлім
Симметриялы әдістерді қолданатын тетіктер

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УПРАВЛЕНИЕ КЛЮЧАМИ
Часть 2
Механизмы, использующие симметричные методы

ҚР СТ ИСО/МЭК 11770-2-2008

ИСО/МЭК 11770-2:1996 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Кілттерді басқару. 2-бөлім. Симметриялы әдістерді қолданатын тетіктер.

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитеті (Мемстандарт)

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

КІЛТТЕРДІ БАСҚАРУ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ

2-бөлім
Симметриялы әдістерді қолданатын тетіктер

ҚР СТ ИСО/МЭК 11770-2-2008
ИСО/МЭК 11770-2:1996 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Кілттерді басқару. 2-бөлім. Симметриялы әдістерді қолданатын тетіктер.

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігінің
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

Алғысөз

1 «Инфосистемы Джет» ЖАҚ **ӘЗІРЛЕДІ**

Қазақстан Республикасы Ақпараттандыру және байланыс жөніндегі агенттігі **ЕНГІЗДІ.**

2 Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитетінің 2008 жылғы 25 ақпандағы № 107-од бұйрығымен **БЕКІТІЛІП ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

3 Осы стандарт мәтінде Қазақстан Республикасының экономикалық қажеттіліктерін көрсететін қосымша талаптар көлбеу қаріппен бөліп көрсетіліп «Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Кілттерді басқару. 2-бөлім. Симметриялы әдістерді қолданатын тетіктер» («Information technology. Security techniques. Entity authentication. Part 2. Mechanisms using symmetric encipherment algorithms»), IDT ИСО/МЭК 11770-2:1996 халықаралық стандартына балама

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ
КІЛТТЕРДІ БАСҚАРУ
2-бөлім
Симметриялық әдістерді қолданатын тетіктер

Енгізілген күні 2008.07.01

1. Қолданылу саласы

Кілттерді басқарудың мақсаты қолданыстағы қауіпсіздік саясатына сәйкес симметриялық немесе ассиметриялық криптограммалық алгоритмдерде қолданылатын бастапқы материалдармен жұмыс істеу үшін арналған рәсімдер беру болып табылады. Осы *ҚР СТ ИСО/МЭК 11770-2* стандарты симметриялық криптографиялық әдістерді қолдана отырып кілтті құру тетіктерін анықтайды.

Ақпаратты криптографиялық қорғаудың нақты құралдарын таңдау және қолдану Қазақстан Республикасының заңнамасымен регламенттеледі және ҚР СТ ИСО/МЭК 11770-2 осы стандарт қарастыратын заты болып табылмайды.

Симметриялық криптографиялық әдістерді қолданылатын кілтті құру тетіктері *ҚР СТ ИСО/МЭК 9798-2* мен [8] стандартында сипатталған осы тетіктерде қарастырылған мәтіндік жиектерді қолдану тәртібін анықтау арқылы сәйкестендіру тетігінен құрылуы мүмкін. Кілтті құрудың басқа да тетіктері өзіне тән ортада қолданылады (ИСО 8732 қараңыз). Кілттерді құрудан басқа бұл тетіктер өзара әрекет ететін мәндерді бір тараптан немесе өзара сәйкестендіру үшін, сондай-ақ кілттің бүтіндігін және кілтті растау мүмкіндігін қамтамасыз ету үшін қолданылуы мүмкін.

Осы *ҚР СТ ИСО/МЭК 11770-2* стандартында кілттерді құрудың үш ортасы қарастырылады: Кілттерді тарату орталығын (КТО) және Кілттерді трансляциялау орталығын (КТрО) қолданатын «нүкте – нүктені» қосқан кезде. Осы *ҚР СТ ИСО/МЭК 11770-2* стандарты бастапқы материалдарды берген кезде және бастапқы материалдарды құру үшін қажетті шарттарды қамтамасыз еткен кезде қолданылатын хабарлама мазмұнына талаптар қояды. Осы құжатта осы тәріздес хабарларда болуы мүмкін басқа ақпарат, сондай-ақ қателіктер туралы хабарлар тәрізді хабарлардың басқа түрлері қарастырылмайды. Қарастырылатын хабардың толық форматы осы *ҚР СТ ИСО/МЭК 11770-2* стандартының қарауына кірмейді.

Осы *ҚР СТ ИСО/МЭК 11770-2* стандарты кілттерді доменаралық басқару мәселелерін тікелей қарастырмайды, сондай-ақ кілттерді басқару тетігін іске асыруды анықтамайды. Осы *ҚР СТ ИСО/МЭК 11770-2*

стандартының талаптарына сәйкес келетін, алайда өзара қабыспайтын әр түрлі өнімдердің болуына жол беріледі.

2 Нормативтік сілтемелер

Осы стандартта мынадай стандарттарға сілтемелер пайдаланылды:

ҚР СТ ИСО/МЭК 9798-1 – 1991 Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сәйкестендіру тетіктері. 1-бөлім. Жалпы ережелер.

ҚР СТ ИСО/МЭК 9798-2:1994 Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сәйкестендіру тетіктері. 2-бөлім. Симметриялық шифрлей алгоритмдерін қолданатын тетіктер.

ҚР СТ ИСО/МЭК 11770-1:1996 Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Кілттерді басқару. 1-бөлім. Негізгі ережелер.

3 Терминдер, анықтамалар мен белгілеулер

Осы стандартта сәйкес анықтамаларымен мынадай терминдер қолданылады.

3.1 Терминдер мен анықтамалар

Осы *ҚР СТ ИСО/МЭК 11770-2 стандартында ҚР СТ ИСО/МЭК 11770-1 стандартында сипатталған терминдер мен анықтамалар қолданылады.*

3.1.1 **Мәнді сәйкестендіру (entity authentication):** Мән өзін кім деп көрсетсе сол болатынын растау.

3.1.2 **Кілтті екі нүктелі құру (point-to-point key establishment):** Үшінші тарапты қатыстырмай кілттерді мәндермен тікелей құру.

3.1.3 **Артықшылық (redundancy):** Мәлім және тексерілген болуы мүмкін кез-келген ақпарат.

3.1.4 **Кілтті бақылау (key control):** Кілтті есептеп тапқан кезде қолданылатын параметрлерді немесе кілттерді таңдау мүмкіндігі.

3.1.5 **Айырмашылықты идентификатор (distinguishing identifier)**: Мәнді тура анықтауға болатын ақпарат.

3.1.6 **Уақытында ауысатын шама (time variant parameter):** Хабардың екінші қайтара қолданылмайтындығын тексеру үшін қолданылатын кездейсоқ сан, дәйекті сан немесе уақыт таңбасы сияқты деректердің элементтері.

3.1.7 **Кілтті растау (key confirmation):** Мәндердің біреуінің басқа мәннің нақты кілтті иеленетінінің кепілдігін алуы.

3.1.8 **Дәйекті сан (sequence number):** Мағынасы белгіленген дәйектіліктен алынатын, және белгілі бір уақыт барысында тексерілмейтін, уақытында ауысып тұратын шама.

3.1.9 **Кездейсоқ сан (random number):** Мағынасын алдын ала болжау мүмкін емес, уақытында ауысып тұратын шама.

3.1.10 **Кілтті генерациялау функциясы (key generating function):** Кірерде бірнеше параметрлерді қабылдайтын функция, олардың ішінде ең аз дегенде біреуі құпия болып табылады, және кірерде алгоритм мен өзінің тағайындалуына сәйкес кілтті береді. Бұл функция кірерде құпия параметрлерді білмей нәтижелі кілтті есептеп тауып алуы мүмкін емес болатындай қасиетке ие болуы тиіс.

3.2 Белгілеулер

Осы *ҚР СТ ИСО/МЭК 11770-2* стандартында мынадай белгілеулер қолданылады:

X	X мәнінің айырмашылықты идентификаторы
ЦРК	Кілттерді тарату орталығы
ЦТК	Кілттерді трансляциялау орталығы
T	Кілттерді тарату орталығының немесе Кілттерді трансляциялау орталығының айырмашылықты идентификаторы
F	бастапқы материал
$К_{XY}$	X және Y мәндеріне байланысты құпия кілт
R	кездейсоқ сан
R_X	X мәнімен құрылған кездейсоқ сан
T/N	уақыт таңбасы немесе дәйекті сан
T_X/N_X	X мәнімен жасалған уақыт таңбасы немесе дәйекті сан
TVP	уақытында өзгеріп тұратын шама
TVP_X	X мәнімен жасалған уақытында өзгеріп тұратын шама
eK(Z)	симметриялы алгоритмдер мен К кілтінің көмегімен Z деректерін шифрлау нәтижелері
dK(Z)	симметриялы алгоритм мен К кілтінің көмегімен Z деректерін ашып көрсету нәтижелері

vK(Z) К. vK(Z) кілтін қолданатын Z деректері үшін есептеп табылған соңғы криптографиялық функцияның нәтижесі, сондай-ақ хабарды сәйкестендіру коды (ХАК) аталады және macK(Z) белгіленуі мүмкін.

f Кілтті генерациялау функциясы

X || Y X және Y деректерінің элементтерін белгіленген тәртіпте дәйекті түрде қосу нәтижелері.

Тетіктерде анықталған *Мәтін1*, *Мәтін2* жиектерінде қосымшада қолдану үшін қажетті қосымша деректер болуы мүмкін және олар осы стандартта қарастырылмайды (аталған жиектер бос болуы мүмкін), олардың қатыстығы және мазмұны нақты қосымшаларға байланысты. Аталған жиектерді қолдану әдістерінің бірі хабарды сәйкестендіру болып табылады (Б қосымшасын қараңыз).

Шифрланбаған қосымша мәтіндік жиектер ұқсас түрде кез-келген хабардың басына немесе соңына қосылуы мүмкін. Олар қауіпсіздікке ықпал етпейді және айқын түрде осы стандартта сипатталған тетіктерге енгізілген жоқ.

Деректердің міндетті емес элементтері *көлбеу қаріппен* көрсетілген.

4 Симметриялық әдістерді пайдаланатын тетіктерге қойылатын талаптар

Осы стандартта сипатталған кілттерді құру тетіктері симметриялы криптографиялық әдістерді қолданады, атап айтқанда – шифрлаудың симметриялық алгоритмі және/немесе кілтті генерациялау қызметі. Криптографиялық алгоритмдер және кілттің өмір сүру уақыты оның өмір сүру уақыты барысында кілтті есептеп тауып ала алмайтындай түрде таңдап алынуы тиіс. Егер бұдан әрі келтірілген шарттар орындалмаған болса, кілтті құру процесінің беделі түсуі мүмкін, немесе іске асырылмауы мүмкін.

Шифрлаудың симметриялық алгоритмін қолданатын тетіктер келесі талаптардың біреуін қанағаттандыруы тиіс:

а) шифрлаудың алгоритмі, оның жұмыс істеу тәртібі және ашық мәтіннің артықтығы жасандылықты немесе деректердің өзгеруін анықтау үшін тиісті құралдары бар алушыға мүмкіндік беруі тиіс;

б) шифрланған деректердің бүтіндігі деректердің бүтіндігін қамтамасыз ететін тетіктермен кепілдендірілуі тиіс. Егер осы мақсат үшін хэш-функция қолданылса, онда хэш-код не шифрлау алдында қосылуы мүмкін, не шифрланбаған мәтіндік жиектерге орналастырылған болуы тиіс.

Ескертпе

1 *ҚР СТ ИСО/МЭК 10116* стандартында шифрлаудың блоктік алгоритмдерінің жұмыс істеу тәртібі стандартталған.

2 Деректердің бүтіндігін қамтамасыз ету тетіктері *[2]*-де стандартталған.

3 Егер КТО немесе КТрО қолданылатын болса, онда а) және б) талаптары шабуылға ұрынған байланыс каналын анықтау мүмкіндігі бөлігінде әрқашан баламалы бола бермейді (Б қосымшасындағы мысалды қараңыз).

5, 6 және 7-бөлімдерде сипатталған тетіктердегі әрбір алмасуда алушы оны құрушының мәлімделген мәнін білуі тиіс. Егер бұл контексте орындалмаған болса, онда бұны, мысалға, кейбір хабардың шифрланбаған қосымша мәтіндік жиектеріне идентификаторларды енгізу арқылы іске асыруға болады.

Бастапқы материал қорғанған және қорғанбаған коммуникациялық каналдар бойынша құрылуы мүмкін. Егер тек қана симметирялы криптографиялық әдістер қолданылатын болса, онда ең аз дегенде мәндер арасында бірінші кілтпен алмасу қорғанылған алмасуды орнату үшін қорғанған каналдар бойынша өтуі тиіс.

Осы стандартта сипатталған кілтті құру тетіктерін қолдану үшін уақыт таңбасы, дәйекті немесе кездейсоқ сандар сияқты уақытында өзгеретін шамаларды қолдану қажет. Аталған контексте кездейсоқ сандар терминін қолдануға алдын ала болжамдалмайтын жалған кездейсоқ сандар кіреді. Сол тәрізді шамалардың қасиеттері, әсіресе, мағыналардың қайталанбауы, қаралатын кілттерді құрудың тетіктерін қорғау үшін қажетті маңызды. Уақытында өзгеретін шамалар туралы қосымша ақпарат *ҚР СТ ИСО/МЭК 9798-2* стандартының В қосымшасында келтірілген.

5. Кілттерді «нүкте-нүктені» қосқан кезде құру

Кілтті «нүкте-нүктені» қосқан кезде құру кілтті құрудың кез-келген тәсілінің базалық тетігі болып табылады. Бұл жағдайда өзара әрекет ететін мәндердегі бастапқы жалпы кілттің болуы талап етіледі, бұл оларға келесі кілттерді құруға тікелей мүмкіндік береді.

Осы бөлімде сипатталған тетіктерді іске асырған жағдайда төмендегілер тұспалданады:

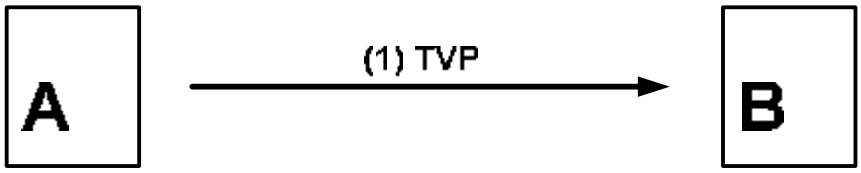
– А және В мәндерінің жалпы K_{AB} кілті бар;

– ең аз дегенде мәндердің біреуі нақты тетіктерде сипатталғандай К құпия кілтін ала алады, генерациялай алады және оны генерациялауға қатыса алады;

– К кілтінің құпиялылығын қамтамасыз ету, оның өзгеруі мен жаңғыруын табу бөлігінде барлық қауіпсіздік талаптары ескерілген.

5.1 №1 кілтті құру тетігі

№1 кілтті құру тетігінде К кілті уақытында өзгеретін TVP шамаларынан құралады, мысалға, кілтті генерациялау функциясы қолданылатын кездейсоқ R саны, Т уақыт таңбасы немесе дәйекті N саны. №1 кілтті құру тетігі оның көмегімен құрылған К кілтін сәйкестендіруді қамтамасыз етпейді. Бұл тетік А мәнінің TVP-ны генерациялауын қажет етеді.



1-сурет – №1 тетік

Қадамдар:

(1) А мәні кездейсоқ R санын, Т уақыт таңбасын немесе дәйекті N санын генерациялайды және оны В мәніне тапсырады.

(1а) А және В екі мәндер f кілтін генерациялау функциясы арқылы К кілтін алады, оның кіруіне жалпы құпия K_{AB} кілті және уақытында өзгеретін TVP шамасы беріледі:

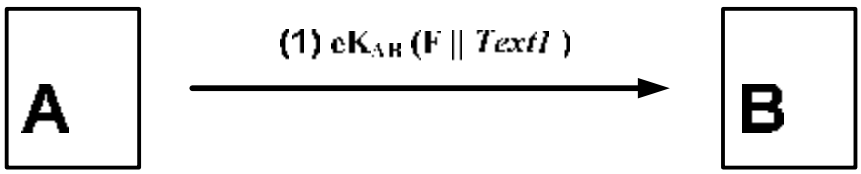
$$K = f(K_{AB}, TVP). \qquad (1)$$

Кілтті генерациялау функциясының мысалдары Б қосымшасында келтірілген.

Ескертпе – Сәйкестендіруді қамтамасыз ету үшін №1 кілтті құру тетігі *ҚР СТ ИСО/МЭК 9798-2* немесе *[8]*-де сипатталғандай сәйкестендіру тетігімен араластырылуы мүмкін (Б қосымшасын қараңыз).

5.2 № 2 кілтті құру тетігі

№2 кілтті құру тетігінде К кілті А мәнімен беріледі. Бұл тетік оның көмегімен құрылған не К кілтінің сәйкестендірілуін, не мәнді сәйкестендіруді да қамтамасыз етпейді.



2-сурет – №2 тетік

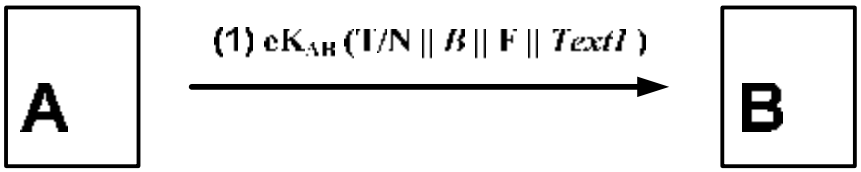
Қадамдар:

(1) А мәні В мәніне K_{AB} кілтін қолдана отырып шифрланған F бастапқы материалын (К кілті және қосымша деректер) жібереді.

(1а) Хабар ала отырып, В шифрланған бөлікті ашып көрсетеді және К кілтін алады.

5.3 № 3 кілтін құру тетігі

№3 кілтін құру тетігі *ҚР СТ ИСО/МЭК 9798-2* стандартының 5.1.1. бөлігінде сипатталған мәндерді сәйкестендірудің бір өткелекті тетігінен құрылған. Бұл тетікте К кілті А мәнімен беріледі. №3 кілтті құру тетігі бір тараптан сәйкестендіруді қамтамасыз етеді, яғни, тек А мәні ғана осы тетікпен анық түрде сәйкестендірілуі мүмкін. Бірегейлік пен мерзімділік уақыт таңбасы мен дәйекті сандар көмегімен қамтамасыз етіледі. Бұл тетік А және В екі мәндердің Т уақыт таңбасының немесе N дәйекті сандарының шынайылығын тексеру және генерациялау мүмкіндігінің болуын талап етеді.



3-сурет – №3 тетік

Қадамдар:

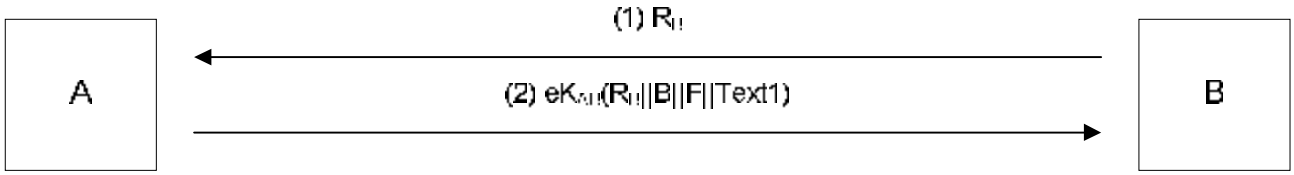
(1) А мәні В мәніне уақыт таңбасын немесе T/N дәйекті санын, В айырмашылықты идентификаторын және В және F бастапқы материалын (К кілті және қосымша деректер) жібереді. Айырмашылықты В идентификаторын қосу міндетті емес. Деректер жиегі $К_{АВ}$ кілтінің көмегімен шифрланады.

(1а) Хабарды алған соң В, егер болған болса, айырмашылықты идентификаторды ашып көрсетеді, уақыт таңбасын немесе дәйекті санды тексереді және К кілтін алады.

Ескертпе – В айырмашылықты идентификаторының жібергені ауыстырып алу мүмкіндіктерінің алдын алу үшін (1) қадамға қосылады, яғни өзін В ретінде атаған қиянат жасаушының аталған хабарды жаңғыртуы (А қосымшасын қараңыз). Осындай шабуыл жасау мүмкін емес ортада идентификаторды қоспауға да болады.

5.4 № 4 кілтті құру тетігі

№4 кілтті құру тетігі *ҚР СТ ИСО/МЭК 9798-2*, 5.1.2.-бөлімінде сипатталған мәндерді сәйкестендірудің екі өткелекті бір тараптық тетігінен құрылған. Бұл тетікте К кілті А мәнімен беріледі. №4 кілтті құру тетігі бір тарапты сәйкестендіруді қамтамасыз етеді, яғни тек А мәні осы тетік арқылы анық сәйкестендірілуі мүмкін. Бірегейлігі және мерзімділігі кездейсоқ R_B санының көмегімен қамтамасыз етіледі. Бұл тетік В мәнінің кездейсоқ сандарды генерациялауға мүмкіндігінің болуын талап етеді.



4-сурет – №4 тетік

Қадамдар:

(1) В мәні А мәніне R_B кездейсоқ санын жібереді.

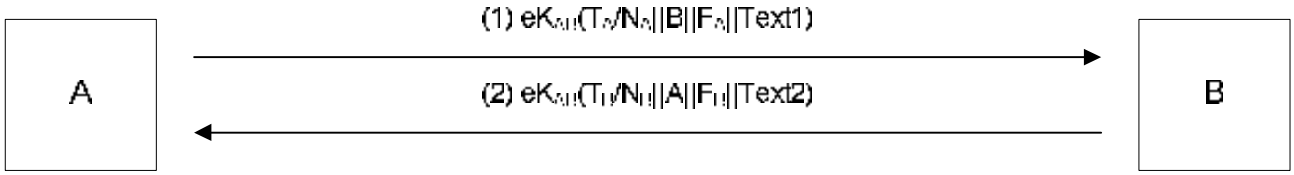
(2) А мәні В мәніне алынған R_B кездейсоқ санын, айырмашылықты В идентификаторы мен F бастапқы материалын (К кілті және қосымша деректер) жібереді. Айырмашылықты В идентификаторын қосу міндетті емес. Деректер жиегі K_{AB} кілті арқылы шифрланады.

(2а) (2) Хабарды ала отырып, В мәні егер болған болса шифрланған бөлікті ашады, өз бөлігінің дұрыстығын тексереді, А мәніне жіберілген кездейсоқ R_B саны (1) қадамда (2) хабарда қолданылғанын тексереді және К кілтін алады.

Ескертпе – В айырмашылықты идентификаторының жібергені ауыстырып алу мүмкіндіктерінің, яғни өзін В ретінде атаған қиянат жасаушының аталған хабарды жаңғыртуының (А қосымшасын қараңыз) алдын алу үшін (2) қадамға қосылады. Осындай шабуыл жасау мүмкін емес ортада идентификаторды қоспауға да болады.

5.5 №5 кілтін құру тетігі

№5 кілтін құру тетігі *ҚР СТ ИСО/МЭК 9798-2*, 5.2.1.-бөлімінде сипатталған мәндерді өзара сәйкестендірудің екі өткелекті тетігінен құралған. Аталған тетік А және В екі мәндердің де К кілтін құру процесіне қатысуына мүмкіндік береді. №5 кілтті құру тетігі өзара сәйкестендіруді қамтамасыз етеді, яғни екі өзара әрекет ететін мәндерді сәйкестендіру жүргізіледі. Бірегейлігі және мерзімділігі не уақыт таңбасы, не дәйекті сандар арқылы қамтамасыз етіледі. Аталған тетік үшін екі А және В мәндерінің де генерациялау және Т уақыт таңбасының немесе N дәйекті санының шынайылығын тексеру мүмкіндігінің болуы қажет.



5-сурет – №5 тетік

Қадамдар:

(1) А мәні В мәніне уақыт таңбасын немесе T_A/N_A дәйекті санын, В айырмашылықты идентификаторын және F_A бастапқы материалды жібереді. В идентификаторын қосу міндетті емес. Деректер жиектері K_{AB} кілтінің көмегімен ашып көрсетіледі.

(1a) (1) Хабарды алып, В шифрланған бөлікті ашып көрсетеді, егер болған болса өзінің айырмашылықты идентификаторының дұрыстығын тексереді, және уақыт таңбасын немесе дәйекті санды тексереді.

(2) В мәні А мәніне уақыт таңбасын немесе T_B/N_B кездейсоқ санын, айырмашылықты А идентификаторын және F_B бастапқы материалын жібереді. Айырмашылықты А идентификаторын қосу міндетті емес. Деректер жиектері K_{AB} кілтінің көмегімен шифрланады.

(2a) (2) Хабарды алып, А шифрланған бөлікті ашып көрсетеді, егер болған болса, өзінің айырмашылықты идентификаторының дұрыстығын тексереді, және уақыт таңбасын немесе дәйекті санды тексереді.

(2b) А және В екі мәні де кірерде F_A және F_B құпия бастапқы материалы бар f кілтін генерациялау функциясы арқылы К кілтін алады:

$$K = f(F_A, F_B). \qquad (2)$$

Кілтті генерациялау функциясының мысалдары Б қосымшасында берілген.

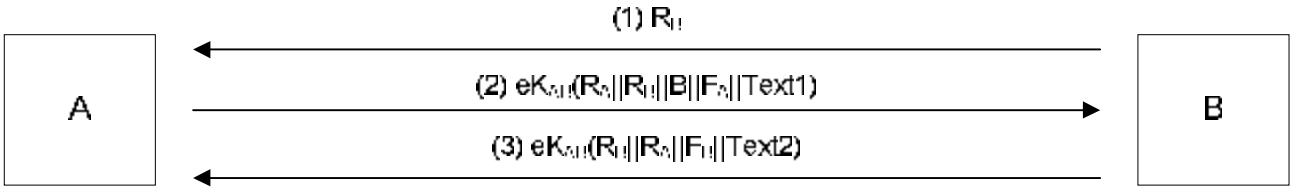
Ескертпе

1 №5 кілтті құру тетігінде F_A и F_B бастапқы материалдары қолданылатын екі жиектің кез-келгені бос болуы мүмкін, алайда екеуі бір уақытта емес.

2 В айырмашылықты идентификаторы ауыстырып алу, яғни өзін В деп атаған қиянат жасаушының аталған хабарды жаңғырту мүмкіндіктерінің алдын алу үшін (1) қадамға қосылады. Осы себептермен (2) қадамында А айырмашылықты идентификаторы қолданылады. Осындай шабуыл болуы мүмкін емес ортада бір немесе екі идентификатор іске қосылуы мүмкін.

5.6 №6 кілттерді құру тетігі

№ 6 кілтті құру тетігі *ҚР СТ ИСО/МЭК 9798-2* стандартының 5.2.2.-бөлімінде сипатталған үш өткелекті сәйкестендіру тетігінен құрылған. Бұл тетік А және В екі мәнінің де К кілтін құруға қатысуына мүмкіндік береді. №6 кілтті құру тетігі өзара аутентификацияны қамтамасыз етеді, яғни екі өзара әрекет ететін мәндер осы тетікпен сәйкестендіріле алады. Бірегейлігі және мерзімділігі кездейсоқ сандар арқылы қамтамасыз етіледі. Бұл тетік А және В мәндерінің кездейсоқ сандарды генерациялауға мүмкіндіктерінің болуын талап етеді.



6-сурет – №6 тетік

Қадамдар:

(1) В мәні А мәніне R_B кездейсоқ санын жібереді.

(2) А мәні В мәніне R_A кездейсоқ санын, алынған R_B кездейсоқ санын, В айырмашылықты идентификаторын және F_A бастапқы материалын жібереді. В айырмашылықты идентификаторын қосу міндетті емес. Деректер жиектері K_{AB}- кілтінің көмегімен шифрланады.

(2a) (2) хабарды алып, В мәні шифрланған бөлігін ашып көрсетеді, егер болса өзінің айырмашылықты идентификаторының дұрыстығын тексереді, А мәніне жіберілген R_B кездейсоқ саны (1) қадамында (2) хабарда қолданылғандығын анықтайды.

(3) В мәні А мәніне R_B және R_A кездейсоқ сандарын және F_B бастапқы материалын жібереді. Деректер жиектері K_{AB} кілтімен шифірленеді.

(3a) (3) хабарды алып, А мәні шифрланған бөлікті ашып көрсетеді және В кездейсоқ санына жіберілген R_A кездейсоқ саны (2) қадамда (3) хабарда қолданылғанын тексереді.

(3b) А және В екі мәндері кірерде F_A және F_B бастапқы құпия материалдары бар f кілтін генерациялау қызметін қолдана отырып, К кілтін құрады:

$$K = f(F_A, F_B). \qquad (3)$$

Кілтті генерациялау қызметінің мысалдары Б қосымшасында келтірілген.

Ескертпе

1 №6 кілтті құру тетігінде FA және FB бастапқы материалдары қолданылатын екі жиектің бірі бос болуы мүмкін, алайда бір уақытта емес.

2 В айырмашылықты идентификаторы «тойтарыс беру» түріндегі шабуыл жасау мүмкіндіктерінің (reflection attacks) алдын алу үшін (2) қадамға қосылады. Осындай шабуыл жасау мүмкін емес ортада бұл идентификатор іске қосылуы мүмкін.

3 №6 кілтті құру тетіктерінің нысандарының бірі №4 кілтін құрудың екі қатарлас тетіктерінен құрылуы мүмкін, олардың біреуі А мәнімен, ал басқасы – В мәнімен бастамашылық етеді.

6 Кілттерді тарату орталығы

Кілттерді тарату орталығының (КТО) міндеті КТО-мен ортақ кілті бар мән үшін кілттерді тарату мен генерациялау/құру болып табылады.

Бұл бөлімде кілттерді құрудың төрт мәні анықталады. Бірінші үш тетіктерде мәндердің екеуінің бірі бұдан әрі басқа мәнді беру үшін КТО-дан К кілтін сұратады. Кілттерді тарату орталығы К кілтін генерациялайды немесе басқалай түрде К кілтін алады және мәнді сұратқан, кілтпен қорғалған, Кілттерді пайдалану орталығына және екінші мәнге ортақ пайдаланылған мәнді жібереді және содан кейін ол сұратқан мәнмен соңғы алушыға жіберілуі мүмкін. КТО соңғы тетікте К кілтін генерациялайды немесе басқаша түрде К кілтін алады және оны тікелей өзара әрекет ететін мәндердің әр қайсысына жібереді. Егер қажет жағдайда сұралған мәнді сәйкестендіру Кілттерді тарату орталығының алдында хабарды (МАС) сәйкестендіру кодын сұранысы бар хабардың шифрланбаған мәтіндік жиектеріне қосу арқылы қамтамасыз етілуі мүмкін.

Осы барлық тетіктерде тек КТО кілтті генерациялау немесе басқаша алғанда кілтті алу мүмкіндігін иемденуі тиіс. КТО кілтті таратқаннан кейін екі мән «нүкте–нүкте» режимінде жұмыс істей алады.

Осы бөлімде сипатталған тетіктерді іске асырған кезде мыналар ескеріледі:

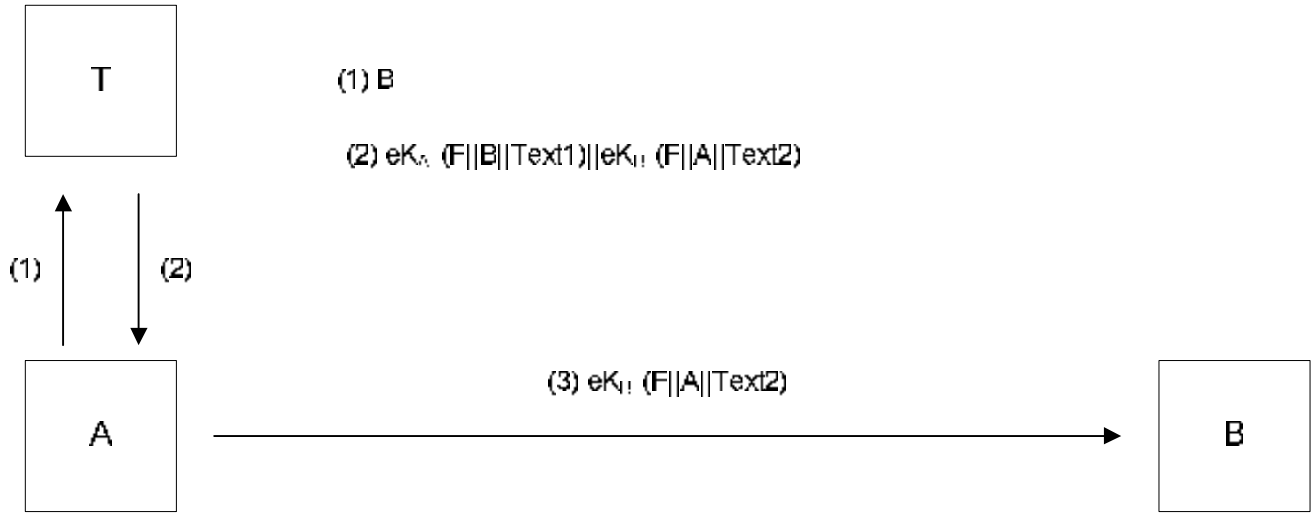
– сенім білдірілген Т үшінші тарапы (Кілттерді тарату орталығы) бар, онымен А және В мәндерінің сәйкесінше $К_{АТ}$ және $К_{ВТ}$ ортақ кілттері бар. Кілттерді тарату орталығының К кілтін генерациялауға немесе басқалай алғанда К кілтін алуға мүмкіндігі бар;

– Кілттерді тарату орталығы кілтті сұратқан мәндер үшін интерактивті режимде(on-line) қол жеткізімді.

– К кілтінің құпиялылығын қамтамасыз ету, оның өзгеруін, қайтара қолданылуын және ауыстырып алу шабуылын анықтау бөлігінде барлық қауіпсіздік талаптары ескерілді.

6.1 №7 кілтті құру тетіктері

№7 кілтті құру тетігінде К кілті Кілттерді тарату орталығымен беріледі. Аталған тетік оның көмегімен құрылған К кілтін сәйкестендіруді қамтамасыз етпейді.



7-сурет – №7 тетік

Қадамдар:

(1) А мәні В мәнінің айырмашылықты идентификаторы бар хабарды КТО-ға жібере отырып КТО-дан бастапқы материалды сұратады.

(2) Кілтті тарату орталығы А мәнінің F қосымша материалы (К кілті мен қосымша деректер) бар қорғанылған хабарын жібереді. Бұл хабар 2 негізгі бөліктен тұрады:

(а) eK_{AT}(F || B || *Мәтін1*)

(б) eK_{BT}(F || A || *Мәтін2*)

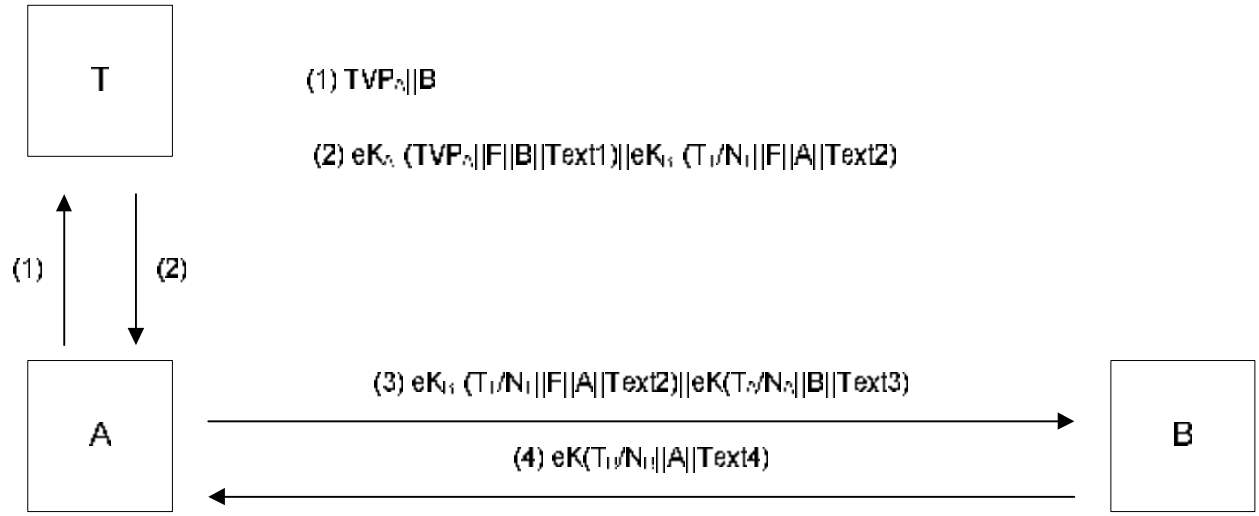
(2а) (2) хабарды алып, А (а) бөлігін ашып көрсетеді, айырмашылықты идентификатордың дұрыстығын тексереді және К кілтін алады.

(3) А (2) хабардың (б) бөлігін В мәніне қайта жібереді.

(3а) (3) хабарды алып, В шифрланған бөлікті ашып көрсетеді, айырмашылықты идентификатордың дұрыстығын тексереді және К кілтін алады.

6.2 №8 кілтті құру тетіктері

№8 кілтті құру тетігі *ҚР СТ ИСО/МЭК 9798-2* стандартының 6.1. бөлімінде сипатталған төрт өткелекті сәйкестендіру тетігінен құралды. Аталған тетікте К кілті Кілттерді тарату орталығымен беріледі. №8 кілтті құру тетігі өзара сәйкестендіруді қамтамасыз етуі мүмкін, яғни екі өзара әрекет ететін мәндер осы тетіктің көмегімен сәйкестендірілуі мүмкін. Бірегейлігі мен мерзімділігі уақыт таңбасы мен дәйекті сан арқылы қамтамасыз етіледі. Бұл тетік А, В мәндерінің және КТО-ның Т уақыт таңбасының немесе N дәйекті санының немесе Т уақыт белгісінің дұрыстығын тексеретін мүмкіндігінің болуын талап етеді.



8-сурет – № 8 тетік

Қадамдар:

(1) А мәні уақытында өзгеретін TVP_A шамасы (кездейсоқ сан, уақыт таңбасы немесе дәйекті сан) мен В мәнінің айырмашылықты идентификаторы бар хабарды КТО-ға жіберіп, КТО-дан бастапқы материалды сұратады.

(2) Кілттерді тарату орталығы F бастапқы материалы (К кілті мен қосымша деректер) бар А мәнінің қорғалған хабарын жібереді. Бұл хабар 2 негізгі бөліктен тұрады:

(a) $eK_{AT}(TVP_A \parallel F \parallel B \parallel$ *Мәтін1*)

(b) $eK_{BT}(T_T/N_T \parallel F \parallel A \parallel$ *Мәтін2*)

(2a) (2) хабарды алып, А (a) бөлігін ашып көрсетеді, КТО жіберілген TVP_A уақытында өзгеретін шама (1) қадамда (2) хабарда қолданылғанын тексереді, айырмашылықты идентификатордың дұрыстығын тексереді және К кілтін алады.

(3) А мәні (2) хабардың (b) бөлігін В мәніне қайта жібереді. (3) хабарда қосымша ретінде В мәніне F-тен құрылған кілтті тексеруге мүмкіндік беретін $eK(T_A/N_A \parallel F \parallel B \parallel$ *Text3*) деректер жиектері болуы мүмкін.

(3a) (3) хабарды алып, В бірінші бөлігін ашып көрсетеді, уақыт таңбасының немесе дәйекті санның дұрыстығын тексереді және К кілтін алады. Айырмашылықты идентификатор В-ға кілттің А мәнімен сұратылғанын көрсетеді.

(3b) В мәні, егер болған болса, (3) хабардың екінші бөлігін ашып көрсетеді, және уақытында өзгеретін шаманың және айырмашылықты идентификатордың дұрыстығын тексереді.

Қосымша міндетті емес қадамдар:

Келесі қадамдар, егер тек бір тараптық сәйкестендіру талап етілетін болса, іске қосылуы мүмкін немесе ол мүлде талап етілмейді.

(4) В мәні eK(T_B/N_B || A || *Text4*) А мәніне ол К кілтін алғандығын растай отырып қайтарады.

(4a) (4) хабарды алып, А оны ашып көрсетеді және уақытында өзгеретін шаманың және айырмашылықты идентификатордың дұрыстығын тексереді.

Ескертпе

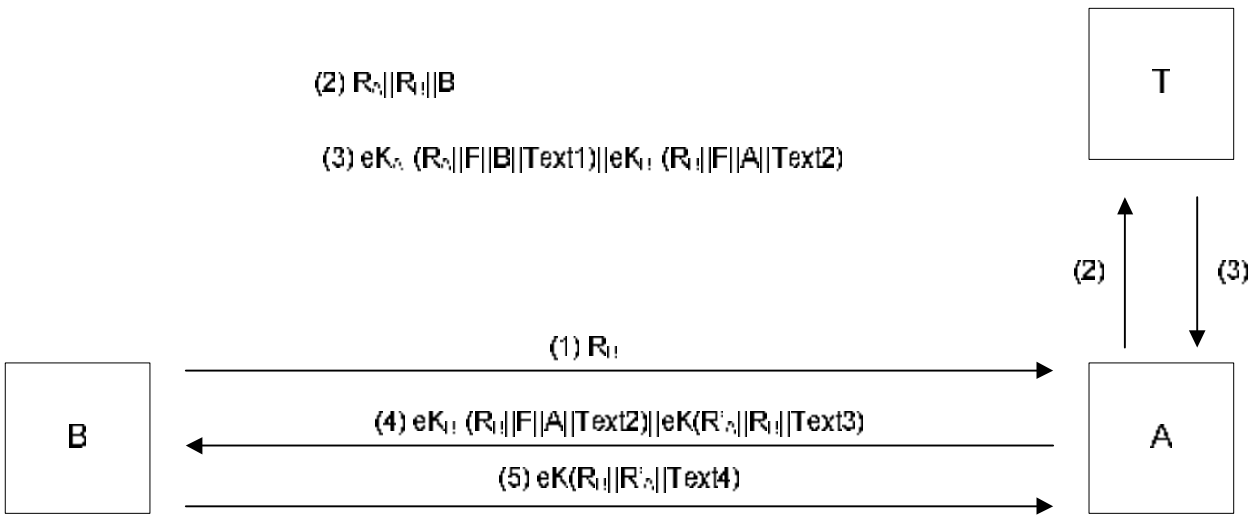
1 Кілтті растаудың міндетті емес процесінде қолданылған е шифрлау алгоритмі кілттерді тарату үшін қолданылған шифрлаудың алгоритмінен (е деп белгіленген) ерекшеленуі мүмкін.

2 Өзара сәйкестендіруге және *ҚР СТ ИСО/МЭК 9798-2* стандартында анықталған төрт өткелекті сәйкестендіру тетігіне сәйкестігіне қол жеткізу үшін (3) және (3b) қадамдарындағы қосымша шамаларды және міндетті емес (4) және (4a) қадамдарын қолдану қажет.

6.3 №9 кілтті құру тетіктері

№9 кілтті құру тетігі *ҚР СТ ИСО/МЭК 9798-2* стандартының 6.2.-бөлімінде сипатталған бес өткелекті сәйкестендіру тетігінен құралған. Аталған тетікте К кілті Кілттерді тарату орталығымен беріледі. №9 кілтті құру тетігі өзара аутентификацияны қамтамасыз етеді, яғни екі өзара аутентификацияланған мәндер осы тетіктің көмегімен сәйкестендірілуі мүмкін.

Бірегейлік пен мерзімділік кездейсоқ сандардың көмегімен қамтамасыз етіледі. Бұл тетік А, В мәндерінің және КТО-ның кездейсоқ сандарды генерациялауға мүмкіндігінің болуын талап етеді.



9-сурет – №9 тетік

Қадамдар:

(1) В мәні R_B кездейсоқ санын А мәніне жіберумен тетікке бастамашылық етеді.

(2) А мәні КТО-на R_A кездейсоқ саны, R_B кездейсоқ саны мен В айырмашылықты идентификаторы бар хабарды жібере отырып, КТО-дан бастапқы материалды сұратады.

(3) Кілтті тарату орталығы А мәнінің F бастапқы материалы (К кілті және қосымша деректері) бар қорғанылған хабарын жібереді. Бұл хабар 2 негізгі бөліктен тұрады:

(a) $eK_{AT}(R_A \parallel F \parallel B \parallel$ *Мәтін1*$)$

(b) $eK_{BT}(R_B \parallel F \parallel A \parallel$ *Мәтін2*$)$

(3a) (3) хабарды алып, А мәні (a) бөлігін ашып көрсетеді, (2) қадамда КТО жіберілген R_A кездейсоқ саны (3) хабарда қолданылғанын тексереді, айырмашылықты идентификатордың дұрыстығын тексереді және К кілтін алады.

(4) А мәні хабардың (b) бөлігін В мәніне жібереді. (4) хабарда R_B және R'_A кездейсоқ сандары енгізілген $eK(R'_A \parallel R_B \parallel$ *Text3*$)$ деректердің қосымша жиектері болуы мүмкін және В мәніне F кілтінен құралған К кілтінің бүтіндігін тексеруге мүмкіндік береді.

(4a) (4) хабарды алып, В мәні бірінші бөлікті ашып көрсетеді, (1) қадамда А мәніне жіберілген R_B кездейсоқ саны (4) хабарда қолданылғанын тексереді және К кілтін алады. Айырмашылықты идентификатор кілттің А мәнімен сұралғанын В-ға көрсетеді.

(4b) В мәні, егер болған болса, (4) хабардың екінші бөлігін ашып көрсетеді, А мәніне жіберілген R_B кездейсоқ саны (1) қадамда (4) хабардың екінші бөлігінде қолданылғандығын тексереді.

Қосымша міндетті емес қадамдар:

Келесі қадамдар, егер тек бір тараптық аутентификация талап етілсе, немесе ол мүлде талап етілмейтін болса, іске қосылуы мүмкін.

(5) В мәні А мәніне $eK(R_B \parallel R'_A \parallel$ *Мәтін4*$)$ қайтарады, сонысымен ол да К кілтін алғандығын растайды. (5) қадам (4) қадамда қосымша деректерді қолдануды талап етеді.

(5a) (5) хабарды алып, А мәні оны ашып көрсетеді және (4) қадамда В мәніне жіберілген R'_A кездейсоқ саны (5) хабарда қолданылғанын тексереді.

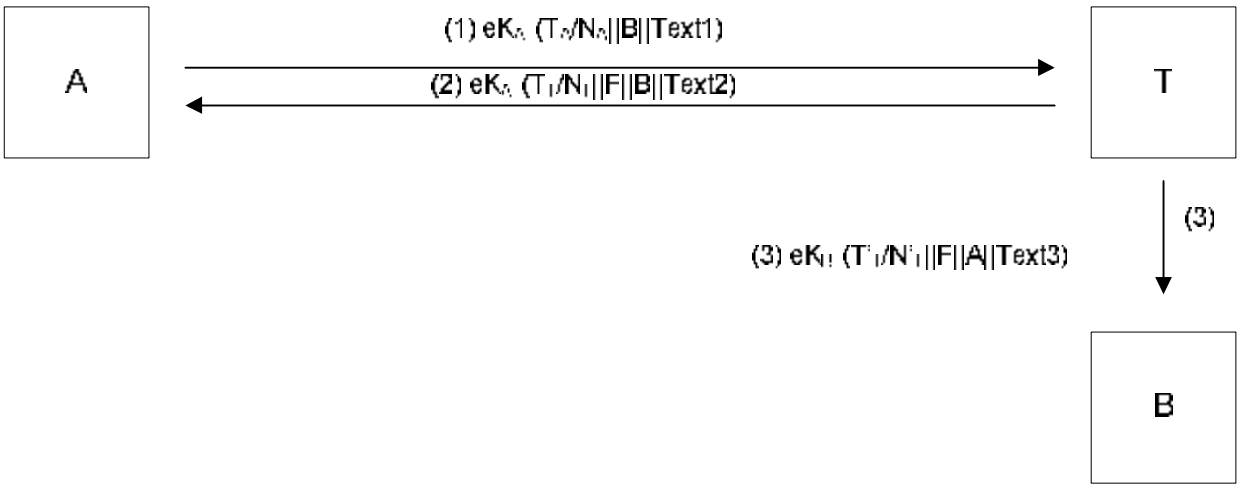
Ескертпе

1 Кілтті растаудың міндетті емес процесінде қолданылған е шифрлау алгоритмі кілттерді тарату үшін қолданылған шифрлаудың алгоритмінен (е деп белгіленген) ерекшеленуі мүмкін.

2 Өзара сәйкестендіруге және *СТ РК ИСО/МЭК 9798-2* стандартында анықталған бес өткелекті сәйкестендіру тетігіне сәйкестігіне қол жеткізу үшін (4) және (4b) қадамдарындағы қосымша шамаларды және міндетті емес (5) және (5a) қадамдарын қолдану қажет.

6.4 №10 кілтті құру тетіктері

№10 кілтті құру тетігінде КТО тікелей екі мәнге бастапқы материалды жібереді. Бұл тетік А мәні мен КТО үшін өзара сәйкестендіруді және В мәні үшін КТО-ның бір тараптық сәйкестендірілуін қамтамасыз етеді. Бірегейлігі мен мерзімділігі уақыт белгісі немесе дәйекті санның көмегімен қамтамасыз етіледі. Бұл тетік А, В, және КТО Т уақыт таңбасының немесе N кездейсоқ сандарының дұрыстығын тексеру және генерациялау мүмкіндігінің болуын талап етеді.



10-сурет – №10 тетік

Қадамдар:

(1) А мәні КТО-на уақыт таңбасы немесе T_A/N_A дәйекті сан және В айырмашылықты идентификаторы бар хабарды жібере отырып, КТО-дан бастапқы материалды сұратады. Деректер жиектері K_{AT} кілтінің көмегімен шифрланған.

(la) (1) хабарды алып КТО оны ашып көрсетеді және уақыт таңбасының немесе дәйекті санның дұрыстығын тексереді.

(2) Кілттерді тарату орталығы А мәніне уақыт таңбасы немесе T_T/N_T дәйекті саны, В мәнінің айырмашылықты идентификаторы және F бастапқы материалы бар хабарды жібереді. Деректер жиектері K_{AT} кілтінің көмегімен шифрланған.

(2a) (2) хабарды алып, А оны ашып көрсетеді, уақыт таңбасының немесе дәйекті санның дұрыстығын тексереді және К кілтін алады.

(3) Кілттерді тарату орталығы В мәніне уақыт таңбасы немесе T'_T/N'_T дәйекті саны, А мәнінің айырмашылықты идентификаторы және F бастапқы

материалы бар хабарды жібереді. Деректер жиектері $К_{ВТ}$ кілтінің көмегімен шифрланған.

(3а) (3) хабарды алып, В оны ашып көрсетеді, уақыт таңбасының немесе дәйекті санның дұрыстығын тексереді және К кілтін алады. А айырмашылықты идентификаторы В мәніне кілттің А мәнімен сұралғанын көрсетеді.

Ескертпе

1 2 және 3- қадамдардың реті өзгеруі мүмкін.

2 Бұл тетік А және В мәндерінің арасындағы сәйкестендіруді қамтамасыз етпейді. Кілтті құрғаннан кейін мәндерді сәйкестендіру *ҚР СТ ИСО/МЭК 9798-2* немесе *[8]* тетіктердің біреуін қолдана отырып жүзеге асырылуы мүмкін.

7 Кілттерді көрсету орталығы

Кілттерді трансляциялау орталығының (КТрО) міндеті КТрО-мен ортақ кілті бар мәндер арасындағы кілттерді трансляциялау болып табылады. Мәндердің біреуі (бастамашы) Кілттерді трансляциялау орталығы және бастамашымен ортақ қолданылатын кілтпен шифрланған К кілтін КТрО-на жібереді. Кілттерді трансляциялау орталығы К кілтін ашып көрсетеді және оны екінші мәнмен (соңғы алушымен) ортақ қолданылатын кілтпен қайта шифрлайды. Осы процестің нәтижесінде трансляцияланған кілт алынады. Бұдан әрі Кілттерді трансляциялау орталығы мына әрекеттердің біреуін жүзеге асырады:

(a) трансляцияланған кілтті бастамашыға қайта жіберу, ол содан кейін оны соңғы алушыға жіберу;

(b) соңғы алушыға трансляцияланған кілтті жіберу.

КТрО қолданылатын ортада бастамашының кілтті алу немесе генерациялау мүмкіндігі болуы қажет.

Осы бөлімде анықталған тетіктерді іске асыруда келесілер тұспалданады:

– Т (Кілттерді тарату орталығы) сенім білдірілген үшінші тарап бар, онымен А және В мәндері сәйкесінше $К_{АТ}$ және $К_{ВТ}$ ортақ кілті бар;

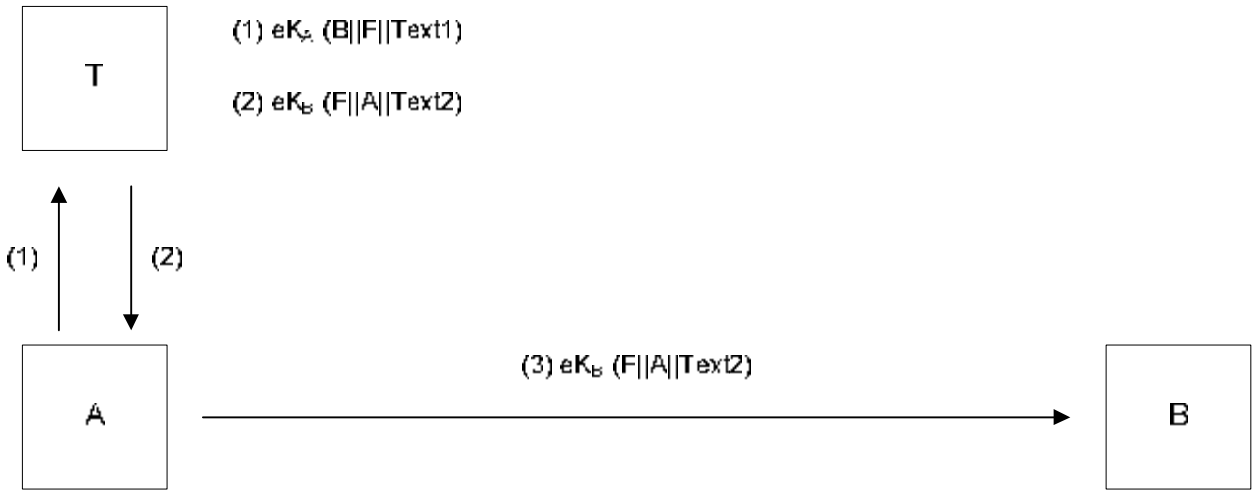
– Кілттерді трансляциялау орталығы кем дегенде бір мән үшін (әдеттегідей бастамашы үшін) интерактивті режимде (on-line) қол жеткізімді;

– құпия К кілтін алуға немесе генерациялауға бастамашының мүмкіндігі бар;

– К кілтінің құпиялылығын қамтамасыз ету, оның өзгеруін анықтау, қайтара қолдану мен ауыстырып алу бөлігінде қауіпсіздіктің барлық талаптары ескерілді.

7.1 №11 кілтті құру тетіктері

№11 кілтті құру тетігінде К кілті А мәнімен беріледі. Бұл тетік оның көмегімен құрылған К кілтін сәйкестендіруді қамтамасыз етпейді.



11-сурет – № 11 тетік

Қадамдар:

А мәні уақыт таңбасы немесе T_A/N_A дәйекті сан және В айырмашылықты идентификаторы бар хабарды жібере отырып, КТрО-дан бастапқы материалды сұратады. Деректер жиектері K_{AT} кілтінің көмегімен шифрланған.

(1а) (1) хабарды алып, КТрО F-ті ашып көрсетеді, А айырмашылықты идентификаторын қосады және екеуін K_{BT} кілтімен шифрлайды.

(2) Кілттерді трансляциялау орталығы А мәніне шифрланған бастапқы материалды қайта жібереді.

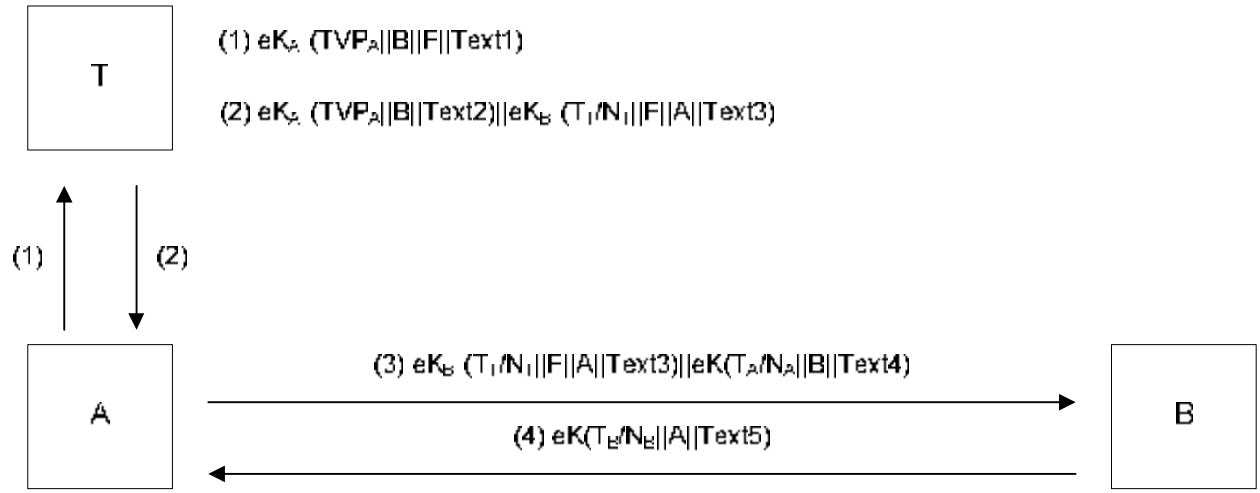
(3) А мәні (2) хабардың қорғалған бөлігін В мәніне жібереді.

(3а) (3) хабарды алып, В мәні шифрланған бөлікті ашып көрсетеді және осылайша К кілтін алады. А айырмашылықты идентификаторы В мәніне кілттің А мәнімен сұралғанын көрсетеді.

7.2 №12 кілтті құру тетіктері

№12 кілтті құру тетігі *ҚР СТ ИСО/МЭК 9798-2,* 6.2.-бөлімінде анықталған бес өткелекті сәйкестендіру тетігінен құрылған (бірақ толығымен қабыспайды). Бұл тетікте К кілті А мәнімен беріледі. №12 кілтті құру тетігі өзара аутентификацияны қамтамасыз етеді, яғни екі өзара әрекет ететін мәндер осы тетіктің көмегімен аутентификациялануы мүмкін. Бірегейлігі мен мерзімділігі кездейсоқ сандардың көмегімен қамтамасыз

етіледі. Бұл тетік А, В мәндерінің және КТО-ның кездейсоқ сандарды генерациялауға мүмкіндігінің болуын талап етеді.



12-сурет – №12 тетік

Қадамдар:

(1) В мәні А мәніне R_B кездейсоқ санды жібере отырып тетікке бастамашылық етеді.

(2) А КТрО-на R_A кездейсоқ санын, R_B кездейсоқ санын, В мәнінің айырмашылықты идентификаторын және F қосымша материалды (К кілті мен қосымша деректерді) жібере отырып, кілтті трансляциялауды сұратады. Деректер жиектері K_{AT} кілтінің көмегімен шифрланған.

(2а) (2) хабарды алып, КТрО шифрланған F бастапқы материалын ашып көрсетеді және деректердің қосымша жиектерімен бірге оны қайта шифрлайды.

(3) Кілттерді трансляциялау орталығы А мәніне 2 негізгі бөліктен тұратын хабарды жібереді:

а) $eK_{AT}(R_A \parallel B \parallel$ *Мәтін2*$)$

б) $eK_{BT}(R_B \parallel F \parallel A \parallel$ *Мәтін3*$)$

(3а) (3) хабарды алып, А мәні (а) бөлігін ашып көрсетеді және айырмашылықты идентификаторды және (2) қадамда КТО-ға жіберілген R_A кездейсоқ саны (3) хабарда қолданылғанын тексереді.

(4) А мәні хабардың (b) бөлігін В мәніне жібереді. (4) хабар В мәніне F кілтінен құрылған кілттің бүтіндігін тексеруге мүмкіндік беретін eK ($R'_A \parallel R_B \parallel$ *Text4*) деректер жиектері бар хабар жібереді.

(4а) (4) хабарды алып, В мәні бірінші бөлікті ашып көрсетеді және К кілтін алады. Егер А мәніне жіберілген кездейсоқ R_B саны (1) қадамда (4)

хабардың бірінші бөлігінде қолданылған болса, бұл В мәніне (1) хабарға жауап ретінде хабарды А мәні жібергенін көрсетеді.

(4b) В мәні, егер қошталатын болса, (4) хабардың екінші бөлігін ашып көрсетеді және (1) қадамда А мәнімен жіберілген R_B саны (4) хабардың екінші бөлігінде қолданылғандығын тексереді.

Міндетті емес қосымша талаптар:

Келесі қадамдар, егер тек бір тараптық аутентификация ғана талап етілсе немесе ол мүлде талап етілмесе, іске қосылуы мүмкін.

(5) В мәні А мәніне $eK(R_B \parallel R'_A \parallel$ *Мәтін5*) хабарын жібереді, сонысымен ол да К кілтін алғандығын растайды. (5) қадам (4) қадамда қосымша деректерді қолдануды талап етеді.

(5a) (5) хабарды алып, А мәні (4) қадамда В мәніне жіберген R'_A кездейсоқ саны (5) хабарда қолданылғандығын тексереді.

Ескертпе

1 Кілтті растаудың міндетті емес процесінде қолданылған е шифрлау алгоритмі кілттерді тарату үшін қолданылған шифрлаудың алгоритмінен (е деп белгіленген) ерекшеленуі мүмкін.

2 Өзара сәйкестендіруге қол жеткізу үшін (4) және (4b) қадамдарындағы қосымша шамаларды және міндетті емес (5) және (5a) қадамдарын қолдану қажет.

А қосымшасы
(анықтамалық)
Кілтті құру тетіктерінің қасиеті

А.1 кестесі осы стандартта анықталған кілттерді құру тетіктерінің негізгі қасиеттері бойынша қорытынды жасайды. Міндетті емес деректер кестеде жақшаның ішінде көрсетілген, мысалы, № 8 тетіктің өзара сәйкестендіруге қол жеткізу үшін міндетті емес төртінші қадамы бар.

А.1 кесте

Кілтті құру тетігінің нөмірі	1	2	3	4	5	6	7	8	9	10	11	12
Үшінші тараптың қатысуы	-	-	-	-	-	-	КТО	КТО	КТО	КТО	КТО	КТО
Қадамдар саны	1	1	1	2	2	3	3	3(4)	4(5)	3	3	4(5)
Кілтті бақылау	А[1)] мәні	А мәні	А мәні	А мәні	А/В	А/В	КТО	КТО	КТО	КТО	А мәні	А мәні
[2)] кілтін сәйкестендіру	жоқ	жоқ	иә	иә	иә	иә	иә	иә	иә	иә	иә	иә
[3)] қайталап қолдануды анықтау	жоқ	жоқ	T/N	R	T/N	R	жоқ	T/N	R	T/N	жоқ	R
[4)] кілтін растау	жоқ	жоқ	жоқ	жоқ	жоқ	жоқ	жоқ	міндетті түрде емес	міндетті түрде емес	жоқ	жоқ	Міндетті түрде емес
[5)] мәндерін сәйкестендіру	жоқ	жоқ	А	А	А+В	А+В	жоқ	міндетті түрде емес	міндетті түрде емес	жоқ	жоқ	міндетті түрде емес

Ескертпе:

1 №1 тетігін қолданған жағдайда К кілті тікелей А мәнімен берілмейді, А мәнімен берілген уақытында өзгеретін шамадан құралады.

2 Аталған мәтінде кілтті сәйкестендіру дегеніміз кілттің бүтіндігін растаған сияқты кілт көзін сәйкестендіру да кіретін кілтті айқын сәйкестендіруді білдіреді. Барлық

тетіктер ең аз дегенде айқын емес аутентификацияны ұсынады, себебі белгілі бір құпия кілтті иеленетін тараптар ғана дұрыс кілтті қалпына келтіре алады.

3 T/N уақыт таңбасы немесе дәйекті санның көмегімен қайталап пайдалануды анықтауды білдіреді; R кездейсоқ сандардың көмегімен жаңғыртуды анықтауды білдіреді.

4 Кілтті растау Б қосымшасында сипатталған әдістер арқылы қамтамасыз етілуі мүмкін.

5 Аталған мәтінде мәндерді сәйкестендіру тек қана А және В мәндері арасындағы сәйкестендіруге жатады. №№ 8, 9 және 12 тетіктері жағдайында бір тараптық және өзара сәйкестендіру қосымша қамтамасыз етілуі мүмкін.

Айырмашылықты идентификатор ауыстырып алу шабуылынан, яғни А немесе В мәндерінің жария хабарын өзін А немесе В мәндері рөлінде білдіргісі келетін үшінші тараптың қайталап қолдануынан қорғану үшін тетіктердің кейбірінің хабарының шифрланған бөлігіне кіреді. Анық айтатын болсақ, кейбір жағдайларда айырмашылықты идентификаторды қосу «тойтарыс беру» (reflection attacks) түріндегі шабуылдан қорғану үшін қолданылады. Аталған түрдегі шабуылдар ауыстырып алудың ерекше түрі болып табылады және іске асырудың келесі тұрпатты сценарийін иемденеді: бір мәннің, мысалы А мәні, жіберген хабары, А мәнді ол жария мәнмен өзара әрекет ететіндігіне сендіру үшін үшінші тараппен осы мәнге қайта жіберіледі. Айырмашылықты идентификаторлар «тойтарыс беру» түріндегі шабуыл іске асуы мүмкін емес ортада, сипаттамасында айырмашылықты идентификатор болмауына рұқсат берілгені анық көрсетілген хабарлар үшін қолданылмауы мүмкін. А-дан В-ға және В-дан А-ға жіберілетін хабар үшін жеке қолданылатын А және В мәндерінің екі ортақ құпия кілті бар (бір бағыттағы кілттер) орта «тойтарыс беру» түріндегі шабуыл іске асырылуы мүмкін емес нақты жағдай болып табылады.

Б қосымша
(анықтамалық)
Көмекші әдістер

Б.1 Деректердің бүтіндігі

Осы стандартта анықталған кілттерді құру тетіктерінде деректердің бүтіндігін қамтамасыз ету үшін мәтін жиектері қолданылуы мүмкін. Егер осы мақсат үшін хэш-функция қолданылатын болса, хэш-код шифрлау алдында деректерге қосылуы мүмкін немесе шифрланбаған мәтін жиектері енгізілуі мүмкін. Егер хабарды сәйкестендіру коды қолданылатын болса, онда ол жасалған К кілтінен құрылған кілт арқылы есептеп шығарылуы мүмкін.

Хабардың бүтіндігін қамтамасыз ету үшін

$$eK_{AB}(\ldots \| K \| Text1)$$

Text1 төмендегіге ауыстырылуы мүмкін

Text1* || h (... || K || Text1*), мұнда h(X), X деректерінің хэш-кодын білдіреді,

немесе шифрланбаған

$$macK*(eK_{AB}(\ldots \| K \| Text1))$$ мәтін жиектеріне қосылуы мүмкін

мұнда К* - К –дан жасалған кілтті білдіреді.

Біріккен шифрланған екі деректер жиектері Кілттерді тарату орталығымен немесе Кілттерді трансляциялау орталығымен (№№ 7, 8, 9, 12-тетіктеріндегі сияқты) кері жіберілсе, 4-бөлімнің а) және б) талаптары әрқашан баламалы бола бермейді. а) талабы тек әр шифрланған бөліктің бүтіндігін жекелеп кепілдендіре алады, сол уақытта б) талабы осыған қосымша барлық хабардың бір бүтін ретінде бүтіндігіне кепілдік бере алады. Тек екінші жағдайда ғана шабуылдың байланыстың қандай каналына бағытталғандығын анықтауы мүмкін.

Мысалы,

$$eK_{AT}(\ldots) \| eK_{BT}(\ldots)$$ хабары

Т-дан А-ға, Т-дан А-ға дейінгі жолда хабардың кез-келген бөлігінің өзгеруін анықтау үшін жіберілген тетікте,

$macK_{AT}*(eK_{AT}(\ldots) \| eK_{BT}(\ldots)) \| macK_{BT}*(eK_{BT}(\ldots))$ шифрланбаған мәтін жиектері қосылуы мүмкін,

мұнда $K_{AT}*$ және $K_{BT}*$ - K_{AT} и K_{BT} кілттерінен жасалған кілттерді білдіреді.

Б.2 Кілттерді есептеп шығару

Кілттерді есептеп шығару – бұл деректердің екі немесе одан да көп элементтерінен кілттерді құру әдісі, олардың ішінде f кілтін (кеңінен танымал болуы мүмкін) генерациялау функциясы қолданылатын ең аз дегенде біреуі құпия болып табылады. Осындай мысалдарға келесілер жатады:

(а) F_1 және F_2 деректерінің 2 екі құпия элементтерінің модулы жөнінде бит бойынша қосу, яғни

$$K = f (F_1, F_2) = F_1 \oplus F_2$$

(б) екі деректер элементінің қосылуына h хэш-функциясын қолдану, ИСО/МЭК 10118-да анықталғандай, F_1 және F_2, олардың ішінде ең аз дегенде біреуі құпия болып табылады, яғни

$$K = f(F_1, F_2) = h(F_1 \parallel F_2).$$

Кейбір жағдайларда кілтті генерациялау функциясы бір бағытты болғаны дұрыс, яғни функция жұмысының нәтижесін біле отырып, кіретін құпия шамаларға жататын кез-келген ақпаратты алу мүмкін емес болатын еді. Жоғарыда мысалда келтірілген (а) функциясы осы мағынада алғанда бір бағытты болып саналмайтындығын атап кеткен жөн, себебі К нәтижесін біле отырып, F_1 және F_2. кіретін екі құпия шамаларға қатысты пайдалы ақпаратты бірден алуға болады. №1 кілтті құру тетігінде кілтті генерациялау функциясы осы тетік арқылы құрылған К кілтінің компрометациясы K_{AB} ортақ құпия кілтінің (ұзақ уақыт пайдаланылуы мүмкін) компрометациясына әкеліп соқтырмайтындай бір бағытты болуы тиіс.

Б.3 Кілттің өзгерісі

Кілттің өзгерісі бұл бір кілттен қосымша кілттерді құру әдісі. Мысалы, К* кілтін берілген К кілтінен құру үшін бірінші төрт биттен бастап К кілтінің кезектесетін төрт биттік блокты толықтыруға болады.

Б.4 Кілтті растау

Кілтті растау – бұл мәннің біреуінің басқа мәннің нақты кілтті иемденетінінің кепілдігін алуы. Мысалы, Х мәні

Y мәнінің eK(TVP || Text) хабарын жібере отырып, Y мәнінің құпия К кілтін иемденетінін растай алады, мұнда TVP –Y мәніне мәлім уақытында өзгеретін шаманы білдіреді.

Б.5 Кілтті құру тетігінің және сәйкестендірудің үйлесуі

Сәйкестендіруді қамтамасыз ету үшін кілтті құру тетігі *ҚР СТ ИСО/МЭК 9798-2* немесе ИСО/МЭК 9798-4:1995 стандарттарында анықталған сәйкестендіру тетігімен қисындасуы мүмкін. Төменде келтірілген мысалда №1 кілтті құру тетігінің *ИСО/МЭК 9594-8*, 5.1.2.-бөлімінде анықталған екі өткелекті бір тараптық сәйкестендіру тетігімен қисындасуын көрсетеді.

Қадамдар:

(1) В мәні R_B кездейсоқ санын генерациялайды және оған А мәнін жібереді.

(1а) А және В екі мәні R_B кездейсоқ санына K_{AB} ортақ кілтке байланысты v қорытынды криптографиялық функцияны қолдана отырып, К кілтін жасайды:

$$K = vK_{AB}(R_B).$$

(2) А мәні В мәніне v' $K_{AB}(R_B \parallel B)$ қайтарады - R_B санына және В айырмашылықты идентификаторынан алынған қорытынды криптографиялық мағыналар.

(2а) (2) хабарды алып, В мәні оның айырмашылықты идентификаторын және (1) қадамда А мәніне жіберілген R_B кездейсоқ санының (2) хабарда қолданылғандығын тексереді.

Қосымша
БИБЛИОГРАФИЯ

[1] *ИСО 8732: 1988 Банк ісі. Кілттерді басқару (шолу).*

[2] *ИСО/МЭК 9797:1994 Ақпараттық технологиялар. Қорғаныс әдістері. Қорытынды криптографиялық қызметті қолданатын, шифрлаудың блоктық алгоритмін қолданатын деректердің бүтіндігін қамтамасыз ету тетіктері.*

[3] *ҚР СТ ИСО/МЭК 10116: 1991 Ақпараттық технологиялар. Шифрлаудың биттік блоктық алгоритмдерінің жұмыс істеу режімдері.*

[4] *ИСО/МЭК 10118-1: 1994 Ақпараттық технологиялар. Қорғаныс әдістері. Хэш-функциялар. 1-бөлім. Жалпы ережелер.*

[5] *ИСО/МЭК 10118-2: 1994 Ақпараттық технологиялар. Қорғаныс әдістері. Хэш-функциялар. 2-бөлім. Шифрлаудың n-биттік блоктық алгоритмдерін қолданатын хэш-функциялар.*

[6] *ИСО 11568-3: 1994 Банк ісі. Кілттерді басқару (бөліктері). 3-бөлім. Симметриялық шифрлау үшін арналған кілттің өмірлік циклі.*

[7] ИСО/МЭК 9798-4:1995 Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сәйкестендіру тетіктері. 4-бөлім. Бақылау криптографиялық қызметтерді пайдаланатын тетіктер

[8] ИСО 7498-2:1989 Ақпаратты өңдеу жүйелері. Ашық жүйелердің өзара әрекеті. Негізгі эталондық үлгі. 2-бөлік. Қауіпсіздік архитектурасы

ӘОЖ 681.324:006.354 **МСЖ 35.040**

Түйінді сөздер: деректерді өңдеу, ақпараттық алмасу, ақпаратты қорғау, қорғаныс әдістері, сәйкестендіру, алгоритмдер, кілттерді басқару.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

УПРАВЛЕНИЕ КЛЮЧАМИ

Часть 2
Механизмы, использующие симметричные методы

СТ РК ИСО/МЭК 11770-2-2008
(ИСО/МЭК 11770-2:1996 «Информационная технология. Методы и средства обеспечения безопасности. Управление ключами. Часть2. Механизмы, использующие симметричные методы», IDT)

Издание официальное

Комитет по техническому регулированию и метрологии
Министерства индустрии и торговли Республики Казахстан
(Госстандарт)

Астана

Предисловие

1 ПОДГОТОВЛЕН ЗАО «Инфосистемы Джет».

ВНЕСЕН Агентством Республики Казахстан по информатизации и связи.

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан № 107-од от 25.02.2008.

3 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 11770-2:1996 «Информационная технология. Методы и средства обеспечения безопасности. Управление ключами. Часть2. Механизмы, использующие симметричные методы» («Information technology. Security techniques. Key management. Part 2. Mechanisms using symmetric techniques»), IDT, с дополнительными требованиями, отражающими потребности экономики Республики Казахстан, которые выделены курсивом.

4 СРОК ПЕРВОЙ ПРОВЕРКИ 2013 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УПРАВЛЕНИЕ КЛЮЧАМИ ЧАСТЬ 2 Механизмы, использующие симметричные методы

Дата введения 2008.07.01

1 Область применения

Целью управления ключами является предоставление процедур для работы с ключевым материалом, который используется в симметричных или асимметричных криптографических алгоритмах в соответствии с действующей политикой безопасности. Настоящий стандарт *СТ РК ИСО/МЭК 11770-2-2008* определяет механизмы формирования ключа с использованием симметричных криптографических методов.

Выбор и применение конкретных средств криптографической защиты информации регламентируется законодательством Республики Казахстан и не является предметом рассмотрения настоящего стандарта СТ РК ИСО/МЭК11770-2.

Механизмы формирования ключа с использованием симметричных криптографических методов могут быть образованы из механизмов аутентификации, описанных в *СТ РК ИСО/МЭК 9798-2* и [8], путем определения порядка использования текстовых полей, предусмотренных в этих механизмах. Другие механизмы формирования ключа используются в специфических средах (см. ИСО 8732). Кроме формирования ключа, эти механизмы могут использоваться для односторонней или взаимной аутентификации взаимодействующих сущностей, а также для обеспечения целостности ключа и возможности подтверждения ключа.

В настоящем стандарте *СТ РК ИСО/МЭК 11770-2-2008* рассматриваются три среды формирования ключей: при соединении «точка – точка», с использованием Центра распространения ключей (ЦРК) и с использованием Центра трансляции ключей (ЦТК). Настоящий стандарт *СТ РК ИСО/МЭК 11770-2-2008* задает требования к содержанию сообщений, используемых при передаче ключевого материала и при обеспечении условий, необходимых для формирования ключевого материала. В данном документе не рассматривается другая информация, которая может содержаться в подобных сообщениях, а также не рассматриваются другие типы сообщений, такие как сообщения об ошибках. Полный формат рассматриваемых сообщений не входит в рассмотрение настоящего стандарта *СТ РК ИСО/МЭК 11770-2-2008.*

Настоящий стандарт *СТ РК ИСО/МЭК 11770-2-2008* непосредственно не рассматривает вопросы междоменного управления ключами, а также не определяет реализацию механизмов управления ключами. Допускается существование различных продуктов, которые соответствуют требованиям настоящего стандарта *СТ РК ИСО/МЭК 11770-2-2008*, но не совместимы между собой.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК ИСО/МЭК 9798-1-1991 Информационные технологии. Методы и средства обеспечения безопасности. Механизмы аутентификации. Часть 1. Общие положения.

СТ РК ИСО/МЭК 9798-2-1994 Информационные технологии. Методы и средства обеспечения безопасности. Механизмы аутентификации. Часть 2. Механизмы с применением алгоритмов симметричного шифрования.

СТ РК ИСО/МЭК 11770-1-1996 Информационные технологии. Методы и средства обеспечения безопасности. Управление ключами. Часть 1. Основные положения.

3 Термины, определения и обозначения

В настоящем стандарте применены следующие термины с соответствующими определениями.

3.1 Термины и определения

В настоящем стандарте, *СТ РК ИСО/МЭК 11770-2-2008*, используются термины и определения, описанные в *СТ РК ИСО/МЭК 11770-1-2008*.

3.1.1 Аутентификация сущности (entity authentication): Подтверждение того, что сущность является тем, за кого себя выдает.

3.1.2 Двухточечное формирование ключа (point-to-point key establishment): Непосредственное формирование ключей сущностями без привлечения третьей стороны.

3.1.2 Избыточность (redundancy): Любая информация, которая известна и может быть проверена.

3.1.3 Контроль над ключом (key control): Возможность выбрать ключ или параметры, используемые при вычислении ключа.

3.1.4 Отличительный идентификатор (distinguishing identifier): Информация, по которой можно однозначно определить сущность.

3.1.5 Параметр, меняющийся во времени (time variant parameter): Элемент данных, такой как случайное число, последовательное число или метка времени, который используется для проверки того, что сообщение не используется повторно.

3.1.6 Подтверждение ключа (key confirmation): Получение одной из сущностей гарантий того, что другая сущность обладает корректным ключом.

3.1.7 Последовательное число (sequence number): Меняющийся во времени параметр, значение которого берется из заданной последовательности, и который не повторяется в течение определенного времени.

3.1.8 Случайное число (random number): Меняющийся во времени параметр, значение которого непредсказуемо.

3.1.9 Функция генерации ключа (key generating function): Функция, которая принимает на входе несколько параметров, из которых, как минимум, один является секретным, и выдает на выходе ключ, соответствующий алгоритму и своему назначению. Эта функция должна обладать таким свойством, чтобы было вычислительно неосуществимо получить результирующий ключ без знания секретных параметров на входе.

3.2 Обозначения

В настоящем стандарте *СТ РК ИСО/МЭК 11770-2-2008* используются следующие обозначения:

X	отличительный идентификатор сущности X
ЦРК	Центр распространения ключей
ЦТК	Центр трансляции ключей
T	отличительный идентификатор Центра распространения ключей или Центра трансляции ключей
F	ключевой материал
$К_{XY}$	секретный ключ, связанный с сущностями X и Y
R	случайное число
R_X	случайное число, созданное сущностью X
T/N	метка времени или последовательное число
T_X/N_X	метка времени или последовательное число, созданное сущностью X
TVP	меняющийся во времени параметр
TVP_X	параметр, меняющийся во времени параметр, созданный сущностью X
eK(Z)	результат шифрования данных Z с помощью симметричного алгоритма и ключа К
dK(Z)	результат расшифрования данных Z с помощью симметричного алгоритма и ключа К
vK(Z)	результат контрольной криптографической функции, вычисленной для данных Z с использованием ключа К. vK(Z) также называется Код аутентификации сообщений (MAC) и может обозначаться macK(Z)

f	функция генерации ключа
X || Y	результат последовательного соединения элементов данных X и Y в указанном порядке.

Поля *Text1*, *Text2*, определенные в механизмах, могут содержать дополнительные данные для использования в приложениях и не рассматриваются в настоящем стандарте (данные поля могу быть пустыми), их отношения и содержание зависят от конкретных приложений. Одним из способов применения данных полей является аутентификация сообщений (см. приложение Б).

Аналогичным образом дополнительные незашифрованные текстовые поля могут добавляться в начало или конец любого сообщения. Они не влияют на безопасность и явным образом не включены в механизмы, описываемые в настоящем стандарте.

Необязательные элементы данных показаны *курсивом*.

4 Требования к механизмам, использующим симметричные методы

Механизмы формирования ключа, описанные в настоящем стандарте, используют симметричные криптографические методы, а именно - симметричные алгоритмы шифрования и/или функции генерации ключа. Криптографические алгоритмы и время жизни ключа должны выбираться таким образом, чтобы было невозможно вычислить ключ в течение времени его жизни. Если не выполняются приведенные далее дополнительные условия, процесс формирования ключа может быть скомпрометирован, или он не может быть реализован.

Механизмы, которые используют симметричные алгоритмы шифрования, должны удовлетворять одному из следующих требований:

а) алгоритм шифрования, его режим работы и избыточность открытого текста должны позволять получателю, имеющему соответствующие средства, выявлять подделки или изменения данных;

б) целостность зашифрованных данных должна гарантироваться механизмами обеспечения целостности данных. Если для этой цели используется хэш-функция, то хэш-код должен быть либо добавлен к данным перед шифрованием, либо помещен в незашифрованное текстовое поле.

Примечание.

1 Режимы работы блочных алгоритмов шифрования указаны в *СТ РК ИСО/МЭК 10116-2008*.

2 Механизмы обеспечения целостности данных стандартизованы в *[2]*.

3 Если используется ЦРК или ЦТК, требования а) и б) не всегда эквивалентны в части возможности однозначного выявления канала связи, подвергнувшегося атаке (см. примеры в Приложении Б).

В каждом обмене в механизмах, описанных в разделах 5, 6 и 7, получатель сообщения должен знать заявленную сущность его создателя. Если это не выполняется в контексте, в котором используется данный механизм, то это можно реализовать, например, путем включения идентификаторов в дополнительные незашифрованные текстовые поля некоторых сообщений.

Ключевой материал может быть сформирован по защищенным и незащищенным коммуникационным каналам. Если используются только симметричные криптографические методы, то, как минимум, обмен первым ключом между сущностями должен происходить по защищенным каналам для установления защищенного обмена.

Для использования механизмов формирования ключа, описанных в настоящем стандарте, необходимо использование меняющихся во времени параметров, таких как метки времени, последовательные или случайные числа. В данном контексте использование термина случайные числа включает непредсказуемые псевдослучайные числа. Свойства подобных параметров, особенно неповторяемость значений, важны для обеспечения защиты рассматриваемых механизмов формирования ключа. Дополнительная информация о меняющихся во времени параметрах приведена в приложении В стандарта *СТ РК ИСО/МЭК 9798-2-2008*.

5 Формирование ключа при соединении «точка-точка»

Формирование ключа при соединении «точка-точка» является базовым механизмом любой схемы формирования ключа. В этом случае требуется наличие изначального общего ключа у взаимодействующих сущностей, что непосредственно позволяет им формировать последующие ключи.

При реализации механизмов, описанных в этом разделе, подразумевается:

– сущности А и В имеют общий ключ $К_{АВ}$;

– как минимум, одна из сущностей может генерировать, получать или участвовать в генерации секретного ключа К, как это описано в конкретных механизмах;

– учтены все требования безопасности в части обеспечения конфиденциальности ключа К и выявления его изменения и воспроизведения.

5.1 Механизм формирования ключа №1

В механизме формирования ключа №1 ключ К образуется из меняющегося во времени параметра TVP, например, случайного числа R, метки времени Т или последовательного числа N с использованием функции генерации ключа. Механизм формирования ключа №1 не обеспечивает

аутентификацию ключа К, сформированного с его помощью. Этот механизм требует, чтобы сущность А могла генерировать TVP.

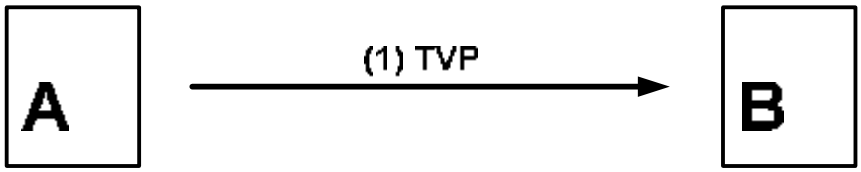


Рисунок 1. Механизм№1

Шаги:

(1) Сущность А генерирует случайное число R, метку времени Т или последовательное число N и передает его сущности В.

(1а) Обе сущности А и В получают ключ К с помощью функции генерации ключа f, на вход которой подается общий секретный ключ $К_{АВ}$ и меняющийся во времени параметр TVP:

$$К = f(К_{АВ}, TVP) \qquad (1)$$

Примеры функций генерации ключа приведены в приложении Б.

Примечание. Для обеспечения аутентификации, механизм формирования ключа №1 может быть скомбинирован с механизмом аутентификации, как описано в *СТ РК ИСО/МЭК 9798-2-2008* или *[8]* (см. приложение Б).

5.2 Механизм формирования ключа №2

В механизме формирования ключа №2 ключ К предоставляется сущностью А. Этот механизм не обеспечивает ни аутентификацию ключа К, сформированного с его помощью, ни аутентификацию сущности.

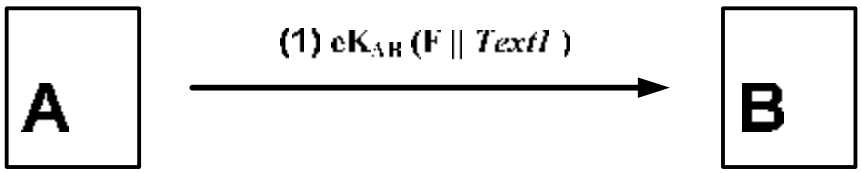


Рисунок 2. Механизм №2

Шаги:

(1) Сущность А посылает сущности В ключевой материал F (ключ К и дополнительные данные), зашифрованный с применением ключа $К_{АВ.}$

(1а) Получив сообщение, В расшифровывает зашифрованную часть и получает ключ К.

5.3 Механизм формирования ключа №3

Механизм формирования ключа №3 образован из однопроходного механизма аутентификации сущностей, описанных в *СТ РК ИСО/МЭК 9798-2-2008*, раздел 5.1.1. В этом механизме ключ К предоставляется сущностью А. Механизм формирования ключа №3 обеспечивает одностороннюю

аутентификацию, т.е. только сущность А может быть явно аутентифицирована этим механизмом. Уникальность и своевременность обеспечиваются с помощью меток времени или последовательных чисел. Этот механизм требует, чтобы обе сущности А и В имели возможность генерировать или проверять действительность меток времени Т или последовательных чисел N.

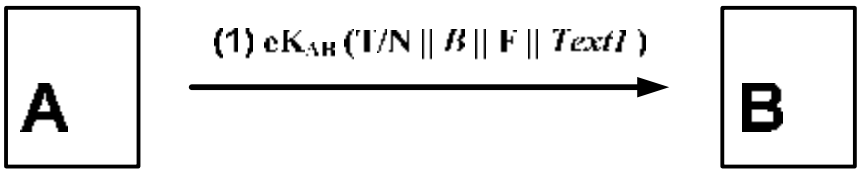


Рисунок 3. Механизм №3

Шаги:

(1) Сущность А посылает сущности В метку времени или последовательное число T/N, отличительный идентификатор В и ключевой материал F (ключ К и дополнительные данные). Включение отличительного идентификатора В необязательно. Поля данных шифруются с помощью ключа K_{AB}.

(1a) Получив сообщение, В расшифровывает отличительный идентификатор, если он присутствует, проверяет метку времени или последовательное число и получает ключ К.

Примечание. Посылка отличительного идентификатора В включается в шаг (1) для предотвращения возможности подмены, т.е. воспроизведения данного сообщения злоумышленником, выдающим себя за В (см. приложение А). В среде, где такая атака невозможна, идентификатор можно не включать.

5.4 Механизм формирования ключа №4

Механизм формирования ключа №4 образован из двухпроходного одностороннего механизма аутентификации сущностей, описанного в *СТ РК ИСО/МЭК 9798-2-2008*, раздел 5.1.2. В этом механизме ключ К предоставляется сущностью А. Механизм формирования ключа №4 обеспечивает одностороннюю аутентификацию, т.е. только сущность А может быть явно аутентифицирована с помощью этого механизма. Уникальность и своевременность обеспечиваются с помощью случайного числа RB. Этот механизм требует, чтобы сущность В имела возможность генерировать случайные числа.

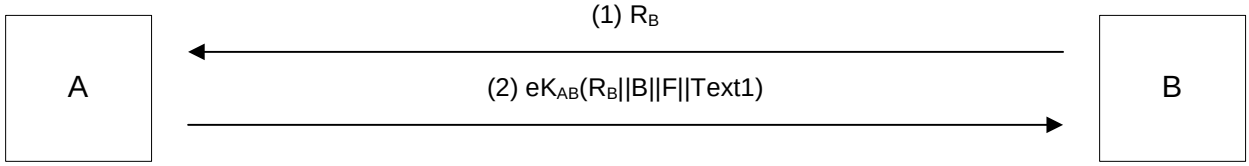


Рисунок 4. Механизм №4

Шаги:

(1) Сущность В посылает сущности А случайное число R_B.

(2) Сущность А посылает сущности В полученное случайное число R_B, отличительный идентификатор В и ключевой материал F (ключ К и дополнительные данные). Включение отличительного идентификатора В необязательно. Поля данных шифруются с помощью ключа K_{AB}.

(2а) Получив сообщение (2), сущность В расшифровывает зашифрованную часть, проверяет правильность своей части, проверяет правильность своего отличительного идентификатора, если он присутствует, проверяет, что случайное число R_B, посланное сущности А на шаге (1), использовалось в сообщении (2) и получает ключ К.

Примечание. Посылка отличительного идентификатора В включается в шаг (2), чтобы предотвратить возможность подмены, т.е. воспроизведения данного сообщения злоумышленником, выдающим себя за В (см. приложение А). В среде, где такая атака невозможна, идентификатор можно не включать.

5.5 Механизм формирования ключа №5

Механизм формирования ключа №5 образован из двухпроходного механизма взаимной аутентификации сущностей, описанного в *СТ РК ИСО/МЭК 9798-2-2008*, раздел 5.2.1. Данный механизм позволяет обеим сущностям А и В участвовать в процессе формирования ключа К. Механизм формирования ключа №5 обеспечивает взаимную аутентификацию, т.е. производится аутентификация обеих взаимодействующих сущностей. Уникальность и своевременность обеспечиваются с помощью меток времени, либо последовательных чисел. Для данного механизма необходимо наличие у обеих сущностей А и В возможности генерирования и проверки достоверности меток времени Т или последовательных чисел N.

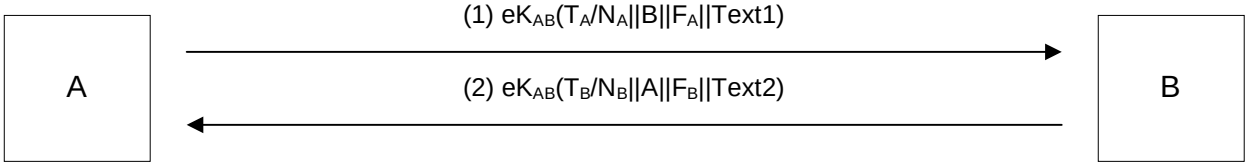


Рисунок 5. Механизм №5

Шаги:

(1) Сущность А посылает сущности В метку времени или последовательное число T_A/N_A, отличительный идентификатор В и ключевой материал F_A. Включение отличительного идентификатора В необязательно. Поля данных шифруются с помощью ключа K_{AB}.

(1а) Получив сообщение (1), В расшифровывает зашифрованную часть, проверяет правильность своего отличительного идентификатора, если он присутствует, и проверяет метку времени или последовательное число.

(2) B посылает A метку времени или последовательное число T_B/N_B, отличительный идентификатор A и ключевой материал F_B. Включение отличительного идентификатора A необязательно. Поля данных шифруются с помощью ключа K_{AB}.

(2a) Получив сообщение (2), A расшифровывает зашифрованную часть, проверяет правильность своего отличительного идентификатора, если он присутствует, и проверяет метку времени или последовательное число.

(2б) Обе сущности A и B получают ключ K с помощью функции генерации ключа f, которая имеет на входе секретный ключевой материал F_A и F_B:

$$K = f(F_A, F_B) \qquad (2)$$

Примеры функций генерации ключа приведены в приложении Б.

Примечание.

1 В механизме формирования ключа №5 любое из двух полей с ключевым материалом FA и FB может быть пустым, но не оба одновременно.

2 Отличительный идентификатор B включается в шаг (1), чтобы предотвратить возможность подмены, т.е. воспроизведения данного сообщения злоумышленником, выдающим себя за B. По этой же причине в шаге (2) используется отличительный идентификатор A. В среде, где такая атака невозможна, один или оба идентификатора могут быть опущены.

5.6 Механизм формирования ключа №6

Механизм формирования ключа №6 образован из трехпроходного механизма аутентификации, описанного в разделе 5.2.2 стандарта *СТ РК ИСО/МЭК 9798-2-2008*. Этот механизм позволяет обеим сущностям A и B участвовать в формировании ключа K. Механизм формирования ключа №6 обеспечивает взаимную аутентификацию, т.е. обе взаимодействующих сущности могут быть аутентифицированы этим механизмом. Уникальность и своевременность обеспечиваются с помощью случайных чисел. Этот механизм требует, чтобы обе сущности A и B имели возможность генерировать случайные числа.

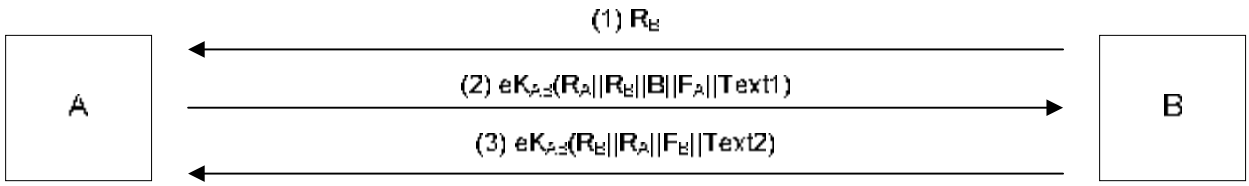


Рисунок 6. Механизм №6

Шаги:

(1) Сущность B посылает сущности A случайное число R_B.

(2) Сущность A посылает сущности B случайное число R_A, полученное случайное число R_B, отличительный идентификатор B и ключевой материал

F_A. Включение отличительного идентификатора В необязательно. Поля данных шифруются с помощью ключа $К_{АВ}$.

(2а) Получив сообщение (2), сущность В расшифровывает зашифрованную часть, проверяет правильность своего отличительного идентификатора, если он присутствует, и проверяет, что случайное число R_B, посланное сущности А на шаге (1), было использовано в сообщении (2).

(3) Сущность В посылает сущности А случайные числа R_B и R_A и ключевой материал F_B. Поля данных шифруются ключом $К_{АВ}$.

(3а) Получив сообщение (3), сущность А расшифровывает зашифрованную часть и проверяет, что случайное число R_A, посланное сущности В на шаге (2), было использовано в сообщении (3).

(3б) Обе сущности А и В образуют ключ К, используя функцию генерации ключа f, которая имеет на входе секретный ключевой материал FA и F_B:

$$К = f(F_A, F_B) \qquad (3)$$

Примеры функций генерации ключа приведены в приложении Б.

Примечание.

1 В механизме формирования ключа №6 любое из двух полей с ключевым материалом FA и FB может быть пустым, но не оба одновременно.

2 Отличительный идентификатор В включается в шаг (2), чтобы предотвратить возможность атак типа «отражение» (reflection attacks). В среде, где такая атака невозможна, этот идентификатор может быть опущен.

3 Один из вариантов механизма формирования ключа №6 может быть построен из двух параллельных механизмов формирования ключа №4, один из которых инициируется сущностью А, а другой - сущностью В.

6 Центр распространения ключей

Задачей Центра распространения ключей (ЦРК) является генерация/формирование и распространение ключей для сущностей, которые имеют общий ключ с ЦРК.

В этом разделе определяются четыре механизма формирования ключа. В первых трех механизмах одна из двух сущностей запрашивает ключ К у ЦРК для дальнейшей передачи другой сущности. Центр распространения ключей генерирует или другим образом получает ключ К и посылает сообщение запросившей сущности, защищенное ключом, совместно используемым Центром распространения ключей и второй сущностью, и которое может быть затем послано запросившей сущностью конечному получателю. В последнем механизме ЦРК генерирует или другим образом получает ключ К и посылает его непосредственно каждому из взаимодействующих сущностей. Эти сообщения защищаются ключами, совместно используемыми ЦРК и соответствующей сущностью. Если необходимо, аутентификация запрашивающей сущности перед Центром

распространения ключей может быть обеспечена путем включения кода аутентификации сообщения (MAC) в незашифрованное текстовое поле сообщения с запросом.

Во всех этих механизмах, только ЦРК должен иметь возможность генерировать или другим образом получать ключи. После того как ЦРК распространил ключ, две сущности могут работать в режиме «точка-точка».

При реализации механизмов, описанных в этом разделе, подразумевается:

– существуют доверенная третья сторона Т (Центр распространения ключей), с которой сущности А и В имеют общие ключи – $К_{АТ}$ и $К_{ВТ}$ соответственно. Центр распространения ключей имеет возможность генерировать или другим образом получать ключ К;

– Центр распространения ключей доступен в интерактивном режиме (on-line) для сущности, запрашивающей ключ;

– учтены все требования безопасности в части обеспечения конфиденциальности ключа К, выявления его изменений, повторного использования и атак подмены.

6.1 Механизм формирования ключа №7

В механизме формирования ключа №7 ключ К предоставляется Центром распространения ключей. Данный механизм не обеспечивает аутентификации ключа К, сформированного с его помощью.

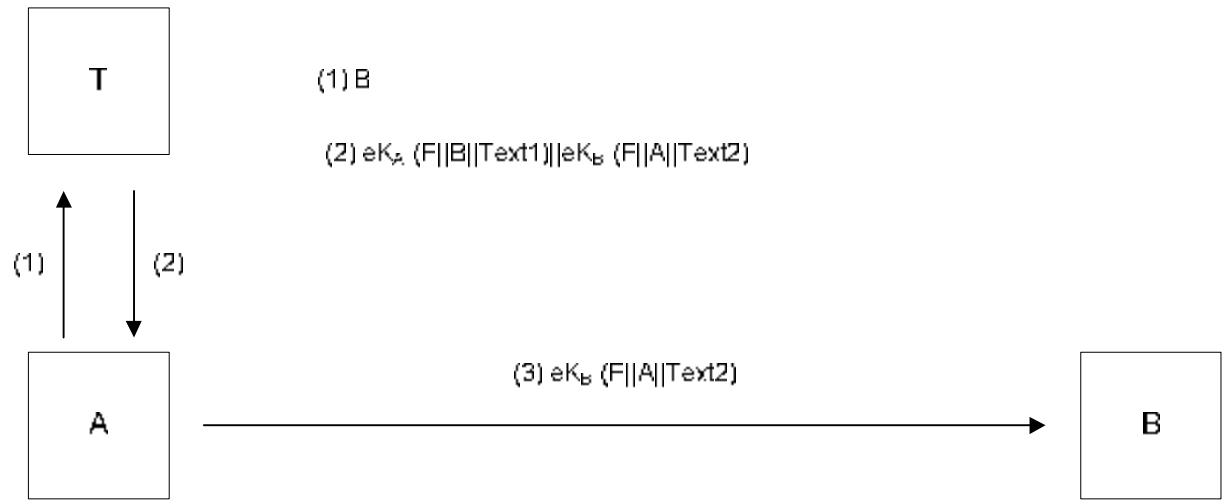


Рисунок 7. Механизм №7

Шаги:

(1) Сущность А запрашивает ключевой материал у ЦРК, послав ЦРК сообщение, которое содержит отличительный идентификатор сущности В.

(2) Центр распространения ключей посылает защищенное сообщение сущности А, которое содержит ключевой материал F (ключ К и дополнительные данные). Это сообщение состоит из 2 основных частей:

(а) eKAT(F || B || *Textl*)

(б) eK_{BT}(F || A || *Text2*)

(2а) Получив сообщение (2), А расшифровывает часть (а), проверяет правильность отличительного идентификатора и получает ключ К.

(3) А пересылает часть (б) сообщения (2) сущности В.

(3а) Получив сообщение (3), В расшифровывает зашифрованную часть, проверяет правильность отличительного идентификатора и также получает ключ К.

6.2 Механизм формирования ключа №8

Механизм формирования ключа №8 образован из четырехпроходного механизма аутентификации, описанного в *СТ РК ИСО/МЭК 9798-2-2008*, раздел 6.1. В данном механизме ключ К предоставляется Центром распространения ключей. Механизм формирования ключа №8 может обеспечивать взаимную аутентификацию, т.е. обе взаимодействующие сущности могут быть аутентифицированы с помощью этого механизма. Уникальность и своевременность обеспечиваются с помощью меток времени и последовательных чисел. Этот механизм требует, чтобы сущности А, В и ЦРК имели возможность генерировать или проверять правильность меток времени Т или последовательных чисел N.

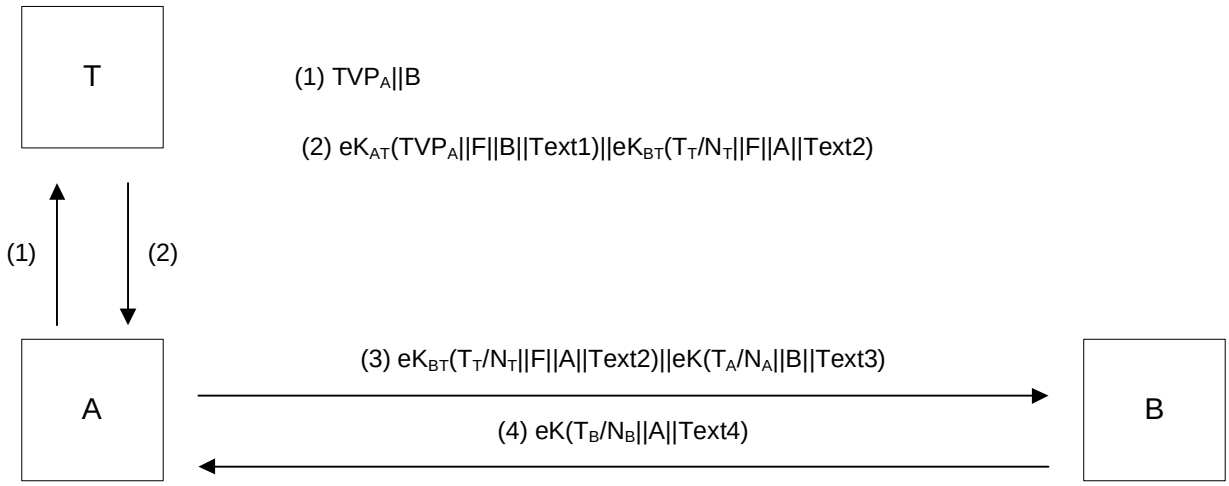


Рисунок 8. Механизм №8

Шаги:

(1) Сущность А запрашивает ключевой материал у ЦРК, послав ЦРК сообщение, которое содержит меняющийся во времени параметр TVP_A (случайное число, метка времени или последовательное число) и отличительный идентификатор сущности В.

(2) Центр распространения ключей посылает защищенное сообщение сущности А, которое содержит ключевой материал F (ключ К и дополнительные данные). Это сообщение состоит из 2 основных частей:

(а) eKAT(TVPA || F || B || *Textl*)

(б) $eK_{BT}(T_T/N_T$ || F || A || *Text2*)

(2а) Получив сообщение (2), А расшифровывает часть (а), проверяет, что меняющийся во времени параметр TVP_A, посланный ЦРК на шаге (1), использован в сообщении (2), проверяет правильность отличительного идентификатора и получает ключ К.

(3) Сущность А пересылает часть (б) сообщения (2) сущности В. Сообщение (3) дополнительно может содержать поле данных eK(TA/NA || F || B || *Text3*), которое позволит сущности В проверить целостность ключа К, сформированного из F.

(3а) Получив сообщение (3), В расшифровывает первую часть, проверяет правильность метки времени или последовательного числа и получает ключ К. Отличительный идентификатор показывает В, что ключ был запрошен сущностью А.

(3б) Сущность В расшифровывает вторую часть сообщения (3), если она присутствует, и проверяет правильность меняющегося во времени параметра и отличительного идентификатора.

Дополнительные необязательные шаги:

Следующие шаги могут быть опущены, если требуется только односторонняя аутентификация, или она не требуется совсем.

(4) Сущность В возвращает eK(TB/NB || A || Text4) сущности А, т.о. подтверждая, что она получил ключ К.

(4а) Получив сообщение (4), А расшифровывает его и проверяет правильность меняющегося во времени параметра и отличительного идентификатора.

Примечание.

1 Алгоритм шифрования e, применяемый в необязательном процессе подтверждения ключа, может отличаться от алгоритма шифрования (также обозначенного e), используемого для распространения ключей.

2 Для достижения взаимной аутентификации и соответствия четырехпроходному механизму аутентификации, определенному в *СТ РК ИСО/МЭК 9798-2-2008*, необходимо использовать дополнительные параметры в шагах (3) и (3б) и необязательные шаги (4) и (4а).

6.3 Механизм формирования ключа №9

Механизм формирования ключа №9 образован из пятипроходного механизма аутентификации, описанного в СТ РК ИСО/МЭК 9798-2-2008, раздел 6.2. В данном механизме ключ К предоставляется Центром распространения ключей. Механизм формирования ключа №9 может обеспечивать взаимную аутентификацию, т.е. обе взаимодействующие сущности могут быть аутентифицированы с помощью этого механизма. Уникальность и своевременность обеспечиваются с помощью случайных

чисел. Этот механизм требует, чтобы сущности А, В и ЦРК имели возможность генерировать случайные числа.

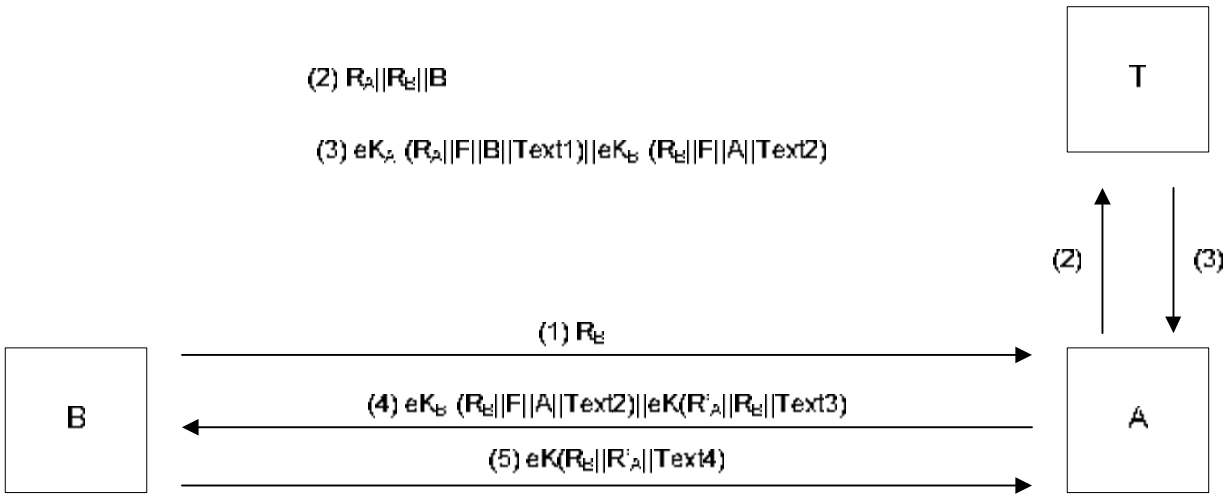


Рисунок 9. Механизм №9

Шаги:

(1) Сущность В инициирует механизм посылкой случайного числа R_B сущности А.

(2) Сущность А запрашивает ключевой материал у ЦРК, послав ЦРК сообщение, которое содержит случайное число R_A, случайное число R_B и отличительный идентификатор В.

(3) Центр распространения ключей посылает защищенное сообщение сущности А, которое содержит ключевой материал F (ключ К и дополнительные данные). Это сообщение состоит из 2 основных частей:

(а) eКАТ(RA || F || B || *Text1*)

(б) $eK_{BT}(R_B$ || F || A || *Text2*)

(3а) Получив сообщение (3), сущность А расшифровывает часть (а), проверяет, что случайное число R_A, посланное ЦРК на шаге (2), использовалось в сообщении (3), проверяет правильность отличительного идентификатора и получает ключ К.

(4) Сущность А пересылает часть (б) сообщения (3) сущности В. Сообщение (4) может содержать дополнительное поле данных eK(R'A || RB || Text3), которое включает в себя случайные числа RB и R'A и позволяет сущности В проверить целостность ключа К, сформированного из F.

(4а) Получив сообщение (4), сущность В расшифровывает первую часть, проверяет, что случайное число R_B, посланное сущности А на шаге (1), использовано в сообщении (4), и получает ключ К. Отличительный идентификатор показывает В, что ключ был запрошен сущностью А.

(4б) Сущность В расшифровывает вторую часть сообщения (4), если она присутствует, и проверяет, что случайное число R_B, посланное сущности А на шаге (1) использовано во второй части сообщения (4).

Дополнительные необязательные шаги:

Следующие шаги могут быть опущены, если требуется только односторонняя аутентификация, или она не требуется совсем.

(5) Сущность B возвращает eK(RB || R'A || Text4) сущности A, тем самым подтверждая, что она тоже получила ключ K. Шаг (5) требует использования дополнительных данных на шаге (4).

(5a) Получив сообщение (5), сущность A расшифровывает его и проверяет, что случайное число R'_A посланное сущности B на шаге (4), использовано в сообщении (5).

Примечание.

1 Алгоритм шифрования *e*, применяемый в необязательном процессе подтверждения ключа, может отличаться от алгоритма шифрования (также обозначенного *e*), используемого для распространения ключей.

2 Для достижения взаимной аутентификации и соответствия пятипроходному механизму аутентификации, определенному в *СТ РК ИСО/МЭК 9798-2-2008*, необходимо использовать дополнительные параметры в шагах (4) и (4б) и необязательные шаги (5) и (5а).

6.4 Механизм формирования ключа №10

В механизме формирования ключа №10 ЦРК передает ключевой материал непосредственно обеим сущностям. Этот механизм обеспечивает взаимную аутентификацию для сущности A и ЦРК и одностороннюю аутентификацию ЦРК для сущности B. Уникальность и своевременность обеспечиваются с помощью меток времени или последовательных чисел. Этот механизм требует, чтобы сущности A, B и ЦРК имели возможность генерировать или проверять правильность меток времени T или последовательных чисел N.

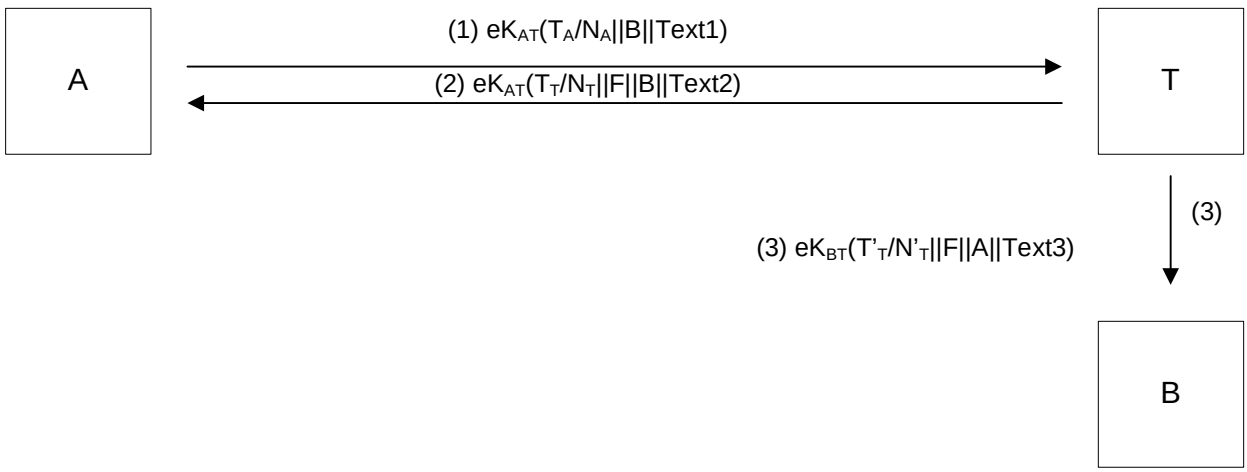


Рисунок 10. Механизм №10

Шаги:

(1) Сущность А запрашивает ключевой материал у ЦРК, посылая ЦРК сообщение, которое содержит метку времени или последовательное число T_A/N_A и отличительный идентификатор сущности В. Поля данных зашифрованы с помощью ключа $К_{АТ}$.

(la) Получив сообщение (1), ЦРК расшифровывает его и проверяет правильность метки времени или последовательного числа.

(2) Центр распространения ключей посылает сущности А сообщение, которое содержит метку времени или последовательное число T_T/N_T, отличительный идентификатор сущности В и ключевой материал F. Поля данных шифруются с помощью ключа $К_{АТ}$.

(2а) Получив сообщение (2), А расшифровывает его, проверяет правильность метки времени или последовательного числа и получает ключ К.

(3) Центр распространения ключей посылает сущности В сообщение, которое содержит метку времени или последовательное число T'_T/N'_T, отличительный идентификатор сущности А и ключевой материал F. Поля данных шифруются с помощью ключа $К_{ВТ}$.

(3а) Получив сообщение (3), В расшифровывает его, проверяет правильность метки времени или последовательного числа и получает ключ К. Отличительный идентификатор А показывает сущности В, что ключ был запрошен сущностью А.

Примечание.

1 Порядок шагов 2 и 3 может быть изменен.

2 Этот механизм не обеспечивает аутентификацию между сущностями А и В. После формирования ключа, аутентификация сущностей может быть осуществлена с использованием одного из механизмов из *СТ РК ИСО/МЭК 9798-2-2008* или *[8]*.

7 Центр трансляции ключей

Задачей Центра трансляции ключей (ЦТК) является трансляция ключей между сущностями, которые имеют общий ключ с ЦТК. Одна из сущностей (инициатор) посылает ЦТК ключ К, зашифрованный ключом, совместно используемым Центром трансляции ключей и инициатором. Центр трансляции ключей расшифровывает ключ К и повторно зашифровывает его ключом, совместно используемым со второй сущностью (конечным получателем). В результате этого процесса получается транслированный ключ. Далее Центр трансляции ключей осуществляет одно из следующих действий:

(а) отправка транслированного ключа обратно инициатору, который затем перешлет его конечному получателю;

(б) пересылка транслированного ключа конечному получателю.

В среде, где используется ЦТК, инициатор должен иметь возможность генерировать или другим образом получать ключи.

При реализации механизмов, определенных в этом разделе, подразумевается, что:

– существует доверенная третья сторона Т (Центр трансляции ключей), с которой сущности А и В имеют общие ключи $К_{АТ}$ и $К_{ВТ}$ соответственно;

– Центр трансляции ключей доступен в интерактивном режиме (on-line), как минимум, для одной сущности (как правило, для инициатора);

– инициатор имеет возможность генерировать или другим образом получать секретный ключ К;

– учтены все требования безопасности в части обеспечения конфиденциальности ключа К, выявления его изменений, повторного использования и атак подмены.

7.1 Механизм формирования ключа №11

В механизме формирования ключа №11 ключ К предоставляется сущностью А. Этот механизм не обеспечивает аутентификации ключа К, сформированного с его помощью.

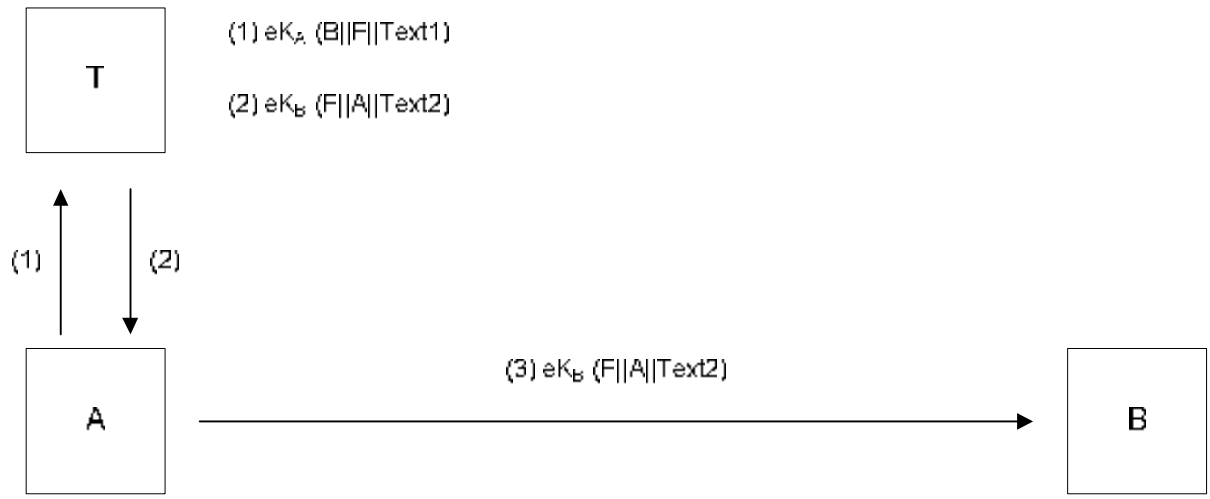


Рисунок 11. Механизм №11

Шаги:

(1) Сущность А запрашивает трансляцию ключа посылкой в ЦТК сообщения, которое зашифровано ключом $К_{АТ}$ и содержит отличительный идентификатор получателя В и ключевой материал F (ключ К и дополнительные данные).

(1а) Получив сообщение (1), ЦТК расшифровывает F, добавляет отличительный идентификатор А и повторно шифрует оба ключом $К_{ВТ}$.

(2) Центр трансляции ключей посылает повторно зашифрованный ключевой материал сущности А.

(3) Сущность А пересылает защищенную часть сообщения (2) сущности В.

(3а) Получив сообщение (3), сущность В расшифровывает зашифрованную часть и таким образом получает ключ К. Отличительный идентификатор А показывает сущности В, что ключ был запрошен сущностью А.

7.2 Механизм формирования ключа №12

Механизм формирования ключа №12 образован (но не полностью совместим) из пятипроходного механизма аутентификации, определенного в *СТ РК ИСО/МЭК 9798-2-2008*, раздел 6.2. В этом механизме ключ К предоставляется сущностью А. Механизм формирования ключа №12 может обеспечивать взаимную аутентификацию, т.е. обе взаимодействующих сущности могут быть аутентифицированы с помощью этого механизма. Уникальность и своевременность обеспечиваются с помощью случайных чисел. Этот механизм требует, чтобы сущности А, В и ЦТК имели возможность генерировать случайные числа.

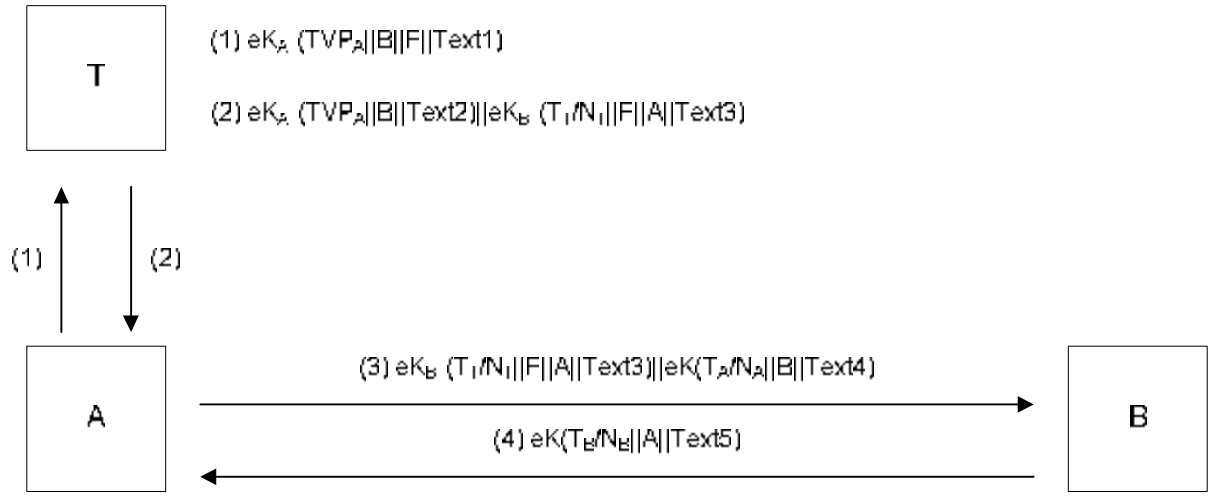


Рисунок 12. Механизм №12

Шаги:

(1) Сущность В инициирует механизм, посылая сущности А случайное число R_B.

(2) Сущность А запрашивает трансляцию ключа, посылая в ЦТК сообщение, которое содержит случайное число RA, случайное число RB, отличительный идентификатор сущности В и ключевой материал F (ключ К и дополнительные данные). Поля данных шифруются ключом КАТ.

(2а) Получив сообщение (2), ЦТК расшифровывает зашифрованный ключевой материал F и повторно шифрует его вместе с дополнительными полями данных.

(3) Центр трансляции ключей посылает сущности А сообщение, которое состоит из 2 основных частей:

а) $eK_{AT}(R_A \parallel B \parallel \textit{Text2})$

б) $eK_{BT}(R_B \| F \| A \| \textit{Text3})$

(3а) Получив сообщение (3), сущность А расшифровывает часть (а) и проверяет отличительный идентификатор и то, что случайное число RA, посланное в ЦТК на шаге (2), использовано в сообщении (3).

(4) Сущность А пересылает часть (б) сообщения (3) сущности В. Сообщение (4) может содержать поле данных eK(R'A || RB || Text4), которое позволяет сущности В проверить целостность ключа К, сформированного из F.

(4а) Получив сообщение (4), сущность В расшифровывает первую часть и получает ключ К. Если случайное число RB, посланное сущности А на шаге (1), было использовано в первой части сообщения (4), это показывает сущности В, что сообщение было послано сущностью А, как ответ на сообщение (1).

(4б) Сущность В расшифровывает вторую часть сообщения (4), если она присутствует, и проверяет, что случайное число R_B, посланное сущностью А на шаге (1), было использовано во второй части сообщения (4).

Дополнительные необязательные шаги:

Следующие шаги могут быть опущены, если требуется только односторонняя аутентификация, или она не требуется совсем.

(5) Сущность В посылает сообщение $eK(R_B \| R'_A \| \textit{Text5})$ сущности А, тем самым подтверждая, что она также получила ключ К. Шаг (5) требует использования дополнительных данных на шаге (4).

(5а) Получив сообщение (5), сущность А проверяет, что случайное число R'_A, посланное сущности В на шаге (4), было использовано в сообщении (5).

Примечание.

1 Алгоритм шифрования *e*, применяемый в необязательном процессе подтверждения ключа, может отличаться от алгоритма шифрования (также обозначенного *e*), используемого для распространения ключей.

2 Для достижения взаимной аутентификации необходимо использовать дополнительные параметры в шагах (4) и (4б) и необязательные шаги (5) и (5а).

Приложение А
(справочное)
Свойства механизмов формирования ключа

Таблица А.1 подводит итог по основным свойствам механизмов формирования ключа, определенных в настоящем стандарте.

Таблица А.1

Номер механизма формирования ключа	Участие третьей стороны	Число шагов	Контроль над ключом	Аутентификация ключа[1)]	Выявление повторного использования[2)]	Подтверждение ключа[3)]	Аутентификация сущностей[4)]
1	нет	1	A[5)]	нет	нет	нет	нет
2	нет	1	A	нет	нет	нет	нет
3	нет	1	A	да	T/N	нет	A
4	нет	2	A	да	R	нет	A
5	нет	2	A/B	да	T/N	нет	A+B
6	нет	3	A/B	да	R	нет	A+B
7	ЦРК	3	ЦРК	да	Нет	нет	нет
8	ЦРК	3(4)	ЦРК	да	T/N	не обязательно	не обязательно
9	ЦРК	4(5)	ЦРК	да	R	не обязательно	не обязательно
10	ЦРК	3	ЦРК	да	T/N	нет	нет
11	ЦРК	3	A	да	нет	нет	нет
12	ЦРК	4(5)	A	да	R	не обязательно	не обязательно

[1)] Под аутентификацией ключа в данном контексте подразумевается явная аутентификация ключа, включающая как подтверждение целостности ключа, так и аутентификацию источника ключа. Все механизмы предлагают, как минимум, неявную аутентификацию, т.к. только стороны, обладающие определенным секретным ключом, могут восстановить правильный ключ.

[2)] T/N обозначает выявление повторного использования с помощью меток времени или последовательных чисел; R обозначает выявление воспроизведения с помощью случайных чисел.

[3)] Подтверждение ключа может быть обеспечено с помощью методов, описанных в приложении Б.

[4)] Аутентификация сущностей в данном контексте относится только к аутентификации между сущностями А и В. В случае механизмов №№ 8, 9 и 12 может быть дополнительно обеспечена односторонняя или взаимная аутентификация.

[5)] В случае использования механизма №1, ключ К не предоставляется сущностью А непосредственно, а образуется из меняющегося во времени параметра, предоставляемого сущностью А.

Примечание. Необязательные данные показаны в таблице в скобках, например, механизм №8 имеет необязательный четвертый шаг для достижения взаимной аутентификации.

Отличительные идентификаторы включаются в зашифрованные части сообщений некоторых из механизмов для защиты от атак подмены, т.е. повторного использования легальных сообщений сущности А или В третьей стороной, желающей выступать в роли сущности А или В. Более конкретно, в некоторых случаях включение отличительного

идентификатора используется для защиты от атак типа «отражение» (reflection attacks). Атаки данного типа являются специфическим видом атак подмены и имеют следующий типовой сценарий реализации: сообщение, посланное одной сущностью, например, А отсылается обратно этой сущности третьей стороной, чтобы убедить сущность А, что она взаимодействует с легальной сущностью. Отличительные идентификаторы могут не использоваться в среде, где реализация атак типа «отражение» невозможно, для сообщений, в описаниях которых явно указана допустимость отсутствия отличительных идентификаторов. Конкретным случаем, когда атака типа «отражение» не может быть реализована, является среда, в которой сущности А и В имеют два общих секретных ключа (однонаправленные ключи), используемых отдельно для сообщений, посылаемых от А к В и от В к А.

Приложение Б
(справочное)
Вспомогательные методы

Б.1 Целостность данных

В механизмах формирования ключа, определенных в настоящем стандарте, для обеспечения целостности данных могут использоваться текстовые поля. Если для этой цели используется хэш-функция, хэш-код должен добавляться к данным перед шифрованием или помещаться в незашифрованное текстовое поле. Если используется код аутентификации сообщений, то он может быть вычислен с помощью ключа, образованного из сформированного ключа К. Во всех случаях получатель ключа К имеет возможность проверить целостность полученного сообщения и ключа.

Для обеспечения целостности сообщения

eKAB(... || K || Text1)

Text1 может быть заменен на

Text1* || h (... || K || Text1*), где h(X) обозначает хэш-код данных X,

либо может быть добавлено незашифрованное текстовое поле

macK*(eKAB(... || K || Text1)), где K* обозначает ключ, образованный из К.

Когда два объединенных зашифрованных поля данных посылаются назад Центром распространения ключей или Центром трансляции ключей (как в механизмах №№ 7, 8, 9, 12) требования а) и б) раздела 4 не всегда эквивалентны. Требование а) может только гарантировать индивидуально целостность каждой зашифрованной части, в то время как требование б) может в дополнение к этому гарантировать целостность всего сообщения, как единого целого. Только во втором случае возможно однозначно определить на какой канал связи направлена атака.

Например, в механизме, где сообщение

eKAT(...) || eKBT(...)

посылается от Т к А, для того чтобы выявить изменение любой части сообщения на пути из Т в А, может быть добавлено незашифрованное текстовое поле

macKAT*(eKAT(...) || eKBT(...)) || macKBT*(eKBT(...)),

где K_{AT}* и K_{BT}* обозначают ключи, образованные из ключей K_{AT} и K_{BT}.

Б.2 Вычисление ключа

Вычисление ключа - это способ формирования ключа из двух или более элементов данных, из которых, как минимум, один является секретным, с использованием функции генерации ключа f (которая может быть широко известна). Примерами таких функций являются:

(а) Побитовое сложение по модулю 2 двух секретных элементов данных F_1 и F_2, т.е.

$$K = f (F_1, F_2) = F_1 \oplus F_2$$

(б) Применение хэш-функции h, как определено в *[5] и [6]*, к объединению двух элементов данных F_1 и F_2, из которых, как минимум, один является секретным, т.е.

$$K = f(F_1, F_2) = h(F_1 \| F_2).$$

В некоторых ситуациях желательно, чтобы функция генерации ключа была однонаправленной, т.е. зная результат работы функции, было бы вычислительно невозможно получить любую информацию, относящуюся к секретным входным параметрам. Следует отметить, что приведенная в примере выше функция (а) не является однонаправленной в этом смысле, т.к. зная результат К, можно сразу получить полезную информацию касающуюся двух секретных входных параметров F_1 и F_2. В механизме

формирования ключа №1 функция генерации ключа должна быть однонаправленной, чтобы, компрометация ключа К, сформированного с помощью этого механизма, не привела к компрометации общего секретного ключа $К_{AB}$ (который может использоваться длительное время).

Б.3 Сдвиг ключа

Сдвиг ключа это способ формирования дополнительных ключей из одного ключа. Например, чтобы сформировать ключ К* из данного ключа К, можно дополнить чередующиеся четырехбитные блоки ключа К, начиная с первых четырех битов.

Б.4 Подтверждение ключа

Подтверждение ключа - это получение одной из сущностей гарантий того, что другая сущность обладает корректным ключом. Например, сущность X может подтвердить сущности Y, что она владеет секретным ключом К, послав сообщение

eK(TVP || Text) сущности Y,

где TVP обозначает меняющийся во времени параметр, известный сущности Y.

Б.5 Комбинация механизма формирования ключа и аутентификации

Для обеспечения аутентификации, механизм формирования ключа может быть скомбинирован с механизмом аутентификации, определенным в *СТ РК ИСО/МЭК 9798-2*-2008 или *[8]*. Пример, приведенный ниже, показывает результат комбинации механизма формирования ключа №1 с двухпроходным односторонним механизмом аутентификации, определенным в *[8]*, раздел 5.1.2.

Шаги:

(1) Сущность В генерирует случайное число R_B и передает его сущности А.

(1а) Обе сущности А и В образуют ключ К, применяя к случайному число R_B контрольную криптографическую функцию v, связанную с общим ключом $К_{AB}$:

$$К = vK_{AB}(R_B).$$

(2) Сущность А возвращает сущности В v' K_{AB}(R_B || В) - контрольное криптографическое значение полученное из числа R_B и отличительного идентификатора В.

(2а) Получив сообщение (2), сущность В проверяет, что ее отличительный идентификатор и случайное число R_B, посланное сущности А на шаге (1), использованы в сообщении (2).

Приложение
(справочное)
БИБЛИОГРАФИЯ

[1] ИСО 8732: 1988 Банковское дело. Управление ключами (обзор).

[2] ИСО/МЭК 9797:1994 Информационные технологии. Методы защиты. Механизмы обеспечения целостности данных, использующие контрольную криптографическую функцию, применяющую блочный алгоритм шифрования.

[4] СТ РК ИСО/МЭК 10116: 1991 Информационные технологии. Режимы работы n-битных блочных алгоритмов шифрования.

[5] ИСО/МЭК 10118-1: 1994 Информационные технологии. Методы защиты. Хэш-функции. Часть 1. Общие положения

[6] ИСО/МЭК 10118-2: 1994 Информационные технологии. Методы защиты. Хэш-функции. Часть 2. Хэш-функции, использующие n-битные блочные алгоритмы шифрования.

[7] ИСО 11568-3: 1994 Банковское дело. Управление ключами (детали). Часть 3. Жизненный цикл ключа для симметричных шифров.

[8] ИСО/МЭК 9798-4:1995 Информационные технологии. Методы и средства обеспечения безопасности. Механизмы аутентификации. Часть 4. Механизмы, использующие контрольные криптографические функции.

[9] ИСО 7498-2:1989 Системы обработки информации. Взаимодействие открытых систем. Базовая эталонная модель. Часть 2. Архитектура безопасности.

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: обработка данных, информационный обмен, взаимодействие сетей, взаимодействие открытых систем, коммуникационные процедуры, защита информации, технологии безопасности, обзор.

Для заметок

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074