## 13-ДӘРІС
## КІЛТТЕРДІ БӨЛУ ХАТТАМАЛАРЫ. АШЫҚ КІЛТТІ БАСҚАРУ

**Дәрістің мақсаты:** Криптографиялық кілттердің өмірлік циклін түсіндіру, симметриялық кілтті бөлу мен ашық кілтті тарату мәселелерін қарастыру, кілт алмасу хаттамаларының жалпы қағидаларын және ашық кілттің түпнұсқалығын растаудың қажеттілігін түсіндіру.

**Кілттерді басқару ұғымы**

Кілттерді басқару – криптографиялық кілттерді генерациялау, тіркеу, тарату, сақтау, пайдалану, жаңарту, кері қайтарып алу және жою процестерінің жиынтығы. Криптографиялық алгоритм қаншалықты берік болғанымен, егер оның кілті дұрыс қорғалмаса, жүйе сенімді қауіпсіздік бере алмайды.

Кілт криптографиялық түрлендірудің негізгі құпия немесе басқарушы параметрі болып табылады. Сондықтан ақпаратты қорғау тек шифрлау алгоритмін таңдаумен аяқталмайды. Кілттің қай жерде жасалғаны, кімге тиесілі екені, кімнің оған қол жеткізе алатыны, қанша уақыт қолданылатыны және пайдаланудан қалай шығарылатыны да алдын ала анықталуы тиіс.

Кілттерді басқарудың негізгі мақсаты – кілттің бүкіл өмірлік циклі бойында оның құпиялығын, тұтастығын, түпнұсқалығын және рұқсат етілген түрде қолданылуын қамтамасыз ету.

**Кілттің өмірлік циклі**

Криптографиялық кілт бір ғана сәтте қолданылатын мән емес. Ол белгілі бір өмірлік циклден өтеді. Алдымен кілт сенімді тәсілмен генерацияланады. Генерация кезінде кездейсоқтық сапасы маңызды, себебі алдын ала болжанатын кілт криптографиялық қорғауды әлсіретуі мүмкін.

Одан кейін кілт белгілі пайдаланушыға, құрылғыға немесе ақпараттық жүйеге байланыстырылып, тіркеледі және рұқсат етілген мақсатта қолданылады. Қолдану барысында кілт рұқсатсыз оқудан, көшірмеден және өзгертуден қорғалуы тиіс.

Белгілі мерзім өткен соң кілт жаңартылуы немесе басқа кілтпен ауыстырылуы мүмкін. Егер кілттің құпиялығы бұзылды деген күдік туындаса, пайдаланушының өкілеттігі аяқталса немесе кілт енді қажет болмаса, ол пайдаланудан шығарылып, қажет болған жағдайда кері қайтарылады және қауіпсіз түрде жойылады.

Генерация → Тіркеу → Тарату → Сақтау → Пайдалану → Жаңарту → Кері қайтару → Жою

**Симметриялық кілтті бөлу мәселесі**

Симметриялық криптожүйеде екі тарап бір ортақ құпия кілтпен жұмыс істейді. Сондықтан сол кілт жіберушіде де, қабылдаушыда да болуы керек. Негізгі мәселе – ортақ кілтті екі тарапқа қауіпсіз жеткізу.

$$K_A = K_B = K$$

Егер құпия кілт қорғалмаған байланыс арнасымен жіберілсе, оны бөгде тұлға ұстап қалуы немесе көшіріп алуы мүмкін. Мұндай жағдайда шабуылдаушы шифрланған деректерді оқуға мүмкіндік алуы ықтимал.

Сондықтан симметриялық кілтті алдын ала қауіпсіз арнамен жеткізу, сенімді кілт тарату орталығын пайдалану немесе асимметриялық криптография көмегімен ортақ кілтті қауіпсіз қалыптастыру сияқты тәсілдер қолданылуы мүмкін.

Пайдаланушылар саны көбейген сайын жеке кілттерді басқару қиындайды. Егер әрбір екі пайдаланушы өзара жеке симметриялық кілт қолданса, n пайдаланушыға қажетті кілттер саны:

$$N = n(n - 1) / 2$$

Мысалы, 10 пайдаланушы үшін 45 жеке кілт жұбы қажет болуы мүмкін. Сондықтан ірі жүйелерде кілттерді орталықтандырылған немесе автоматтандырылған басқару маңызды.

**Кілт алмасу және кілт келісу**

Кілттерді басқаруда «кілтті тасымалдау» және «кілтті келісу» ұғымдарын ажырату қажет. Кілтті тасымалдау кезінде дайын құпия кілт бір тарапта қалыптастырылып, екінші тарапқа қорғалған тәсілмен жеткізіледі.

А тарапы: K генерациялайды → қорғалған түрде → В тарапы K алады

Кілт келісу кезінде ортақ құпия кілттің өзі байланыс арнасы арқылы дайын күйінде жіберілмейді. Екі тарап өздерінің құпия мәндері мен хаттаманың ашық параметрлерін пайдаланып, есептеу нәтижесінде бірдей ортақ құпияға келеді.

А тарапының есебі → ортақ K ← В тарапының есебі

Демек, бірінші жағдайда кілт тасымалданады, ал екінші жағдайда ортақ кілт екі тараптың есептеулері нәтижесінде қалыптасады.

**Диффи–Хеллман идеясы**

Диффи–Хеллман тәсілі – екі тараптың ашық байланыс арнасы арқылы ортақ құпия мән қалыптастыру идеясын көрсететін классикалық кілт келісу механизмі. Тараптар кейбір ашық параметрлерді ортақ пайдаланады, бірақ әрқайсысы өзінің құпия мәнін жасырын сақтайды.

Оқу моделінде ортақ ашық параметрлер p және g деп белгіленсін. Алиса құпия a мәнін, ал Боб құпия b мәнін таңдайды. Олар ашық мәндерді есептейді:

$$A = g^a \bmod p$$
$$B = g^b \bmod p$$

A және B мәндері ашық арна арқылы берілуі мүмкін. Одан кейін Алиса:

$$K_A = B^a \bmod p$$

мәнін, ал Боб:

$$K_B = A^b \bmod p$$

мәнін есептейді. Математикалық қасиеттердің нәтижесінде екі тарап бірдей ортақ құпия мәнге келеді:

$$K_A = K_B = g^{ab} \bmod p$$

Бұл оқу формулалары кілт келісудің негізгі идеясын көрсетеді: ортақ құпияның өзі ашық арнамен тікелей жіберілмейді.

Алайда Диффи–Хеллманның қарапайым түрі тараптардың кім екенін өздігінен растамайды. Егер түпнұсқалықты тексеру механизмі болмаса, арадағы делдал әр тараппен бөлек байланыс орнатуға әрекет етуі мүмкін. Сондықтан практикалық хаттамаларда кілт келісу механизмі аутентификация құралдарымен бірге қолданылады.

**Ашық кілтті тарату мәселесі**

Ашық кілт құпия ақпарат емес және оны жариялауға болады. Бірақ ашық кілттің нақты кімге тиесілі екені сенімді түрде расталуы тиіс. Ашық кілтті криптографиядағы негізгі мәселелердің бірі де осы.

Мысалы, Алиса Бобқа хабарлама жібергісі келіп, Бобтың ашық кілтін алады. Егер шабуылдаушы өз ашық кілтін Бобтың кілті ретінде көрсетсе, Алиса хабарламаны қате кілтпен

шифрлауы мүмкін. Сондықтан «бұл ашық кілт шынымен Бобқа тиесілі ме?» деген сұраққа сенімді жауап беру қажет.

Осы міндетті шешу үшін ашық кілтті белгілі субъектінің деректерімен байланыстыратын цифрлық сертификаттар және ашық кілт инфрақұрылымы қолданылады.

**Цифрлық сертификат**

Цифрлық сертификат – ашық кілтті белгілі бір субъектінің деректерімен байланыстыратын электрондық құрылым. Сертификат пайдаланушының, ұйымның немесе ақпараттық ресурстың ашық кілтінің тиесілігін растауға көмектеседі.

Сертификатта әдетте субъект туралы ақпарат, оның ашық кілті, сертификаттың жарамдылық мерзімі, сертификатты шығарған тарап туралы мәлімет және сертификаттың тұтастығы мен түпнұсқалығын тексеруге арналған цифрлық қолтаңбаға қатысты деректер болады.

Сертификатты пайдалану кезінде оның тек бар болуы жеткіліксіз. Оның жарамдылық мерзімі аяқталмағанын, сенімді тізбекке жататынын және кері қайтарылмағанын тексеру қажет.

**Ашық кілт инфрақұрылымы**

PKI (Public Key Infrastructure) – ашық кілттер мен цифрлық сертификаттарды басқаруға арналған ұйымдастырушылық және техникалық инфрақұрылым. Ол тек бағдарламалық құралдан тұрмайды; оның құрамына ережелер, рәсімдер, жауапты тараптар және техникалық механизмдер кіреді.

PKI құрамында сертификаттау орталығы (CA), тіркеу рәсімдері, цифрлық сертификаттар, сертификат саясаты және сертификаттардың күйін тексеру механизмдері болуы мүмкін. Сертификаттау орталығы сертификатқа қол қою арқылы белгілі бір ашық кілт пен субъект арасындағы байланысты растауға қатысады.

Кейбір жағдайларда сенім бір ғана сертификатпен шектелмейді. Түпкі сенімді орталықтан аралық сертификаттар арқылы соңғы пайдаланушы сертификатына дейін сертификаттар тізбегі қалыптасуы мүмкін.

Сенімді түбірлік CA → Аралық CA → Пайдаланушы сертификаты

**Кілттерді сақтау**

Жабық және симметриялық кілттер рұқсатсыз оқудан, көшірмеден, өзгертуден және жойылудан қорғалуы тиіс. Кілтті кәдімгі мәтіндік файлда ашық түрде сақтау дұрыс емес, себебі файлға қол жеткізген тұлға кілтті де иеленуі мүмкін.

Кілтті сақтау тәсілі жүйенің қауіп моделіне және қорғалатын ақпараттың маңыздылығына сәйкес таңдалады. Бағдарламалық жүйелерде рұқсаттарды шектеу, қорғалған кілт қоймалары және операциялық жүйенің қауіпсіз сақтау механизмдері қолданылуы мүмкін. Жоғары талап қойылатын жүйелерде арнайы қорғалған аппараттық құралдар пайдаланылуы ықтимал.

Маңызды қағида – қолданбаға кілт қажет болған жағдайда ғана оған рұқсат беру және кілтке қол жеткізу құқықтарын мүмкіндігінше шектеу.

**Кілтті жаңарту және кері қайтару**

Криптографиялық кілтті шексіз уақыт қолдану дұрыс емес. Кілттің қолданылу мерзімін шектеу ұзақ уақыт бойы бір кілтке тәуелділікті азайтады. Белгіленген мерзім аяқталғанда ескі кілт жаңа кілтпен ауыстырылуы мүмкін.

Кілттің құпиялығы бұзылды деген күдік пайда болса, оны жоспарланған мерзімнің аяқталуын күтпей пайдаланудан шығару қажет. Мұндай жағдай кілттің компрометациясы деп қарастырылады.

Ашық кілт сертификаты үшін сертификаттың кері қайтарылғаны туралы ақпарат пайдаланушыларға қолжетімді болуы тиіс. Сертификаттың күйін тексеру үшін сертификаттарды кері қайтару тізімдері немесе онлайн күй тексеру механизмдері қолданылуы мүмкін.

Компрометация → Кілтті тоқтату → Кері қайтару → Жаңа кілт → Жаңа сертификат

**Кілттерді басқарудағы негізгі қауіптер**

Кілттерді басқарудағы қауіптер тек кілтті ұрлаумен шектелмейді. Әлсіз кездейсоқ генерация, кілтті қорғалмаған арнамен жіберу, рұқсатсыз көшіру, мерзімі өткен кілтті қолдану, бұрынғы қызметкердің кілтін белсенді күйде қалдыру немесе кері қайтарылған сертификатты тексермеу де қауіпсіздікке әсер етеді.

Сондықтан кілттерді басқару техникалық және ұйымдастырушылық шаралардың бірлігі ретінде қарастырылады. Жүйеде кімнің кілт жасайтыны, кімнің оны қолданатыны, қандай жағдайда жаңартылатыны және оқиға болған кезде кімнің кілтті кері қайтаратыны нақты белгіленуі тиіс.

**Кілттерді басқару тәсілдерін салыстыру**

| Механизм | Негізгі мақсаты | Ерекшелігі |
|---|---|---|
| Кілтті тасымалдау | Дайын кілтті екінші тарапқа жеткізу | Кілт қорғалған түрде тасымалданады |
| Кілт келісу | Ортақ құпияны бірлесіп қалыптастыру | Дайын ортақ кілт ашық арнамен берілмейді |
| Цифрлық сертификат | Ашық кілттің субъектке тиесілігін байланыстыру | Ашық кілттің түпнұсқалығын тексеруге көмектеседі |
| PKI | Сертификаттар мен ашық кілттерді басқару | Ұйымдастырушылық және техникалық инфрақұрылым |
| Кері қайтару | Жарамсыз немесе компрометацияланған кілтті тоқтату | Кілтті әрі қарай қолдануға жол бермейді |

**Қорытынды**

Кілттерді басқару криптографиялық қорғаудың ажырамас бөлігі болып табылады. Қауіпсіздік тек алгоритмнің математикалық беріктілігіне емес, кілттің бүкіл өмірлік цикліне байланысты. Кілт сенімді генерацияланып, дұрыс таратылып, қорғалған ортада сақталып, тек рұқсат етілген мақсатта қолданылып, уақтылы жаңартылып және қажет болған жағдайда дереу кері қайтарылуы тиіс.

Симметриялық жүйелерде негізгі мәселе – ортақ құпия кілтті қауіпсіз бөлу, ал асимметриялық жүйелерде ашық кілттің нақты иесіне тиесілігін растау маңызды. Кілт келісу хаттамалары, цифрлық сертификаттар және PKI осы міндеттерді шешуге арналған өзара байланысты механизмдер болып табылады.

**Қорытынды**

Криптографиялық қауіпсіздік алгоритммен ғана емес, кілттердің бүкіл өмірлік циклін дұрыс басқарумен анықталады. Симметриялық кілттерді қауіпсіз бөлу, ашық кілттердің түпнұсқалығын растау, сертификаттарды басқару, кілттерді қорғап сақтау және уақытында жаңарту біртұтас жүйе ретінде қарастырылуы тиіс.

**Бақылау сұрақтары**

1. Кілттерді басқару дегеніміз не?
2. Кілттің өмірлік циклі қандай кезеңдерден тұрады?
3. Симметриялық кілтті бөлу мәселесі неде?

4. Кілтті бөлу мен кілт келісудің айырмашылығы қандай?
5. Диффи–Хеллман тәсілінің жалпы идеясы қандай?
6. Ашық кілттің құпия болмауы неліктен оның түпнұсқалығын тексеру қажеттілігін жоймайды?
7. Цифрлық сертификаттың мақсаты қандай?
8. PKI дегеніміз не?
9. Құпия кілттерді сақтау кезінде не ескеріледі?
10. Кілтті жаңарту және кері қайтару не үшін қажет?

**Әдебиеттер тізімі:**

1. Ахметов Б.С., Корченко А.Г., Сиденко В.П., Дрейс Ю.А., Алимсеитова Ж.К. Қолданбалы криптология: шифрлау әдістері. Оқулық. Алматы: ҚазҰТЗУ, 2016. – 500 б.
2. Ахметов Б.С., Кузнецов А.А., Краснобаев В.А., Алимсеитова Ж.К., Кузнецова Т.Ю. Криптография негіздері: сандар теориясының, топтардың, өрістердің, сақиналардың элементтері. Алматы: АЭжБУ, 2020.
3. Васильева И.Н. Криптографические методы защиты информации. Москва: Юрайт, 2024.
4. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации для изучающих компьютерную безопасность. Москва: Юрайт, 2024.
5. Омассон Ж.-Ф. О криптографии всерьез. Практическое введение в современное шифрование. Москва: ДМК Пресс, 2021.