13-ДӘРІС. КІЛТТЕРДІ БӨЛУ ХАТТАМАЛАРЫ. АШЫҚ КІЛТТІ БАСҚАРУ

- Кілттің өмірлік циклі және симметриялық кілтті тарату
- Диффи–Хеллман келісуі, цифрлық сертификат және PKI

SEC1811 «Ақпаратты криптографиялық қорғау негіздері»

Оқытушы: Ахмедиярова А.Т.

Дәрістің оқу нәтижелері

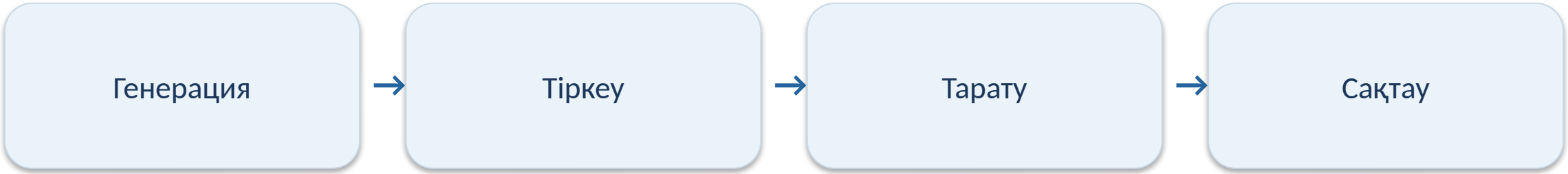
- Кілтті басқарудың кезеңдерін сипаттау
- Кілтті тасымалдау мен келісуді ажырату
- Диффи–Хеллман есебін орындау
- PKI және сертификат тексеруін түсіндіру

Кілттерді басқару дегеніміз не?

Кілттерді басқару — кілтті жасау, тіркеу, тарату, сақтау, пайдалану, жаңарту және жою рәсімдері.

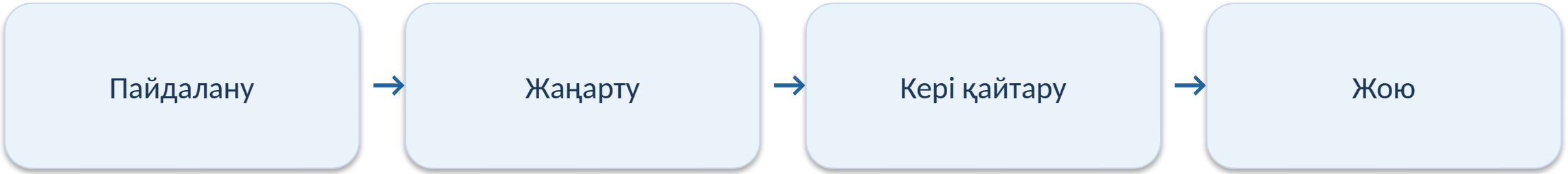
Алгоритм сенімді болса да, кілттің қорғалмауы бүкіл жүйені әлсіретеді.

Кілттің өмірлік циклі



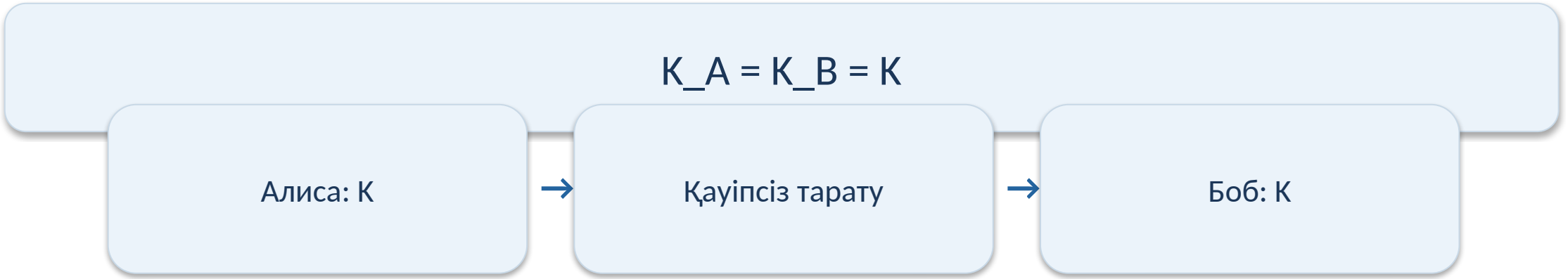
- Әр кезеңде рұқсаттар, мерзімдер және жауапты тараптар анықталады.

Өмірлік циклдің аяқталуы



- Кілтті пайдалану мерзімі шектеледі.
- Компрометация күдігі туғанда кілт дереу тоқтатылады.

Симметриялық кілтті бөлу мәселесі



- Алиса мен Бобта бірдей құпия K болуы керек.
- Қорғалмаған арнада K-ны тікелей жіберу қауіпті.

Пайдаланушылар саны және кілт саны

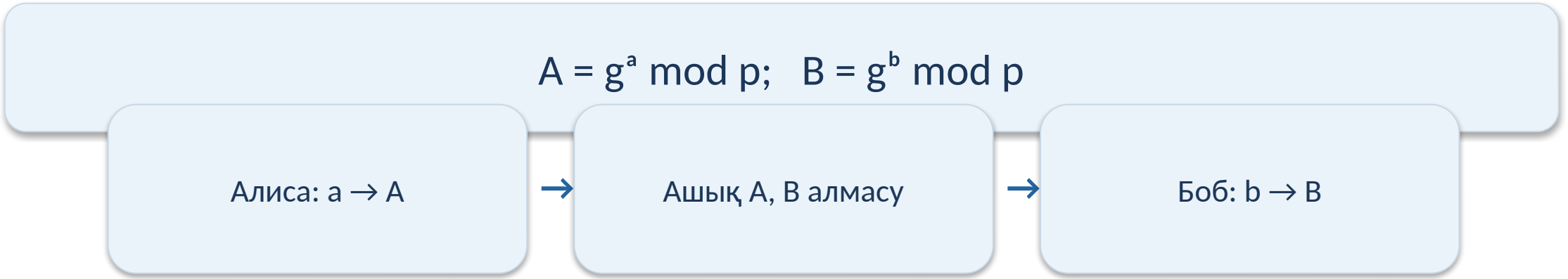
$$N = n(n - 1) / 2$$

- Әр жұп үшін бөлек кілт керек деген болжамда:
- 10 пайдаланушы → 10 × 9 / 2 = 45 кілт.
- 20 пайдаланушы → 20 × 19 / 2 = 190 кілт.

Кілтті тасымалдау және келісу

- Тасымалдау: бір тарап дайын K жасайды да, қорғалған түрде жеткізеді.
- Келісу: екі тарап есептеу арқылы ортақ құпия қалыптастырады; дайын K жіберілмейді.

Диффи–Хеллман: негізгі идея



- p және g — ашық параметрлер; a және b — құпия мәндер.
- Ашық мәндер A және B алмасылады; ортақ құпия жеке есептеледі.

Диффи–Хеллман: есептеу формулалары

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

- Алиса: $K_A = B^a \bmod p$.
- Боб: $K_B = A^b \bmod p$.
- Екі нәтиже де $g^{ab} \bmod p$ мәніне тең.

Оқу мысалы: ашық мәндер

$$p = 23;\ g = 5;\ a = 6;\ b = 15$$

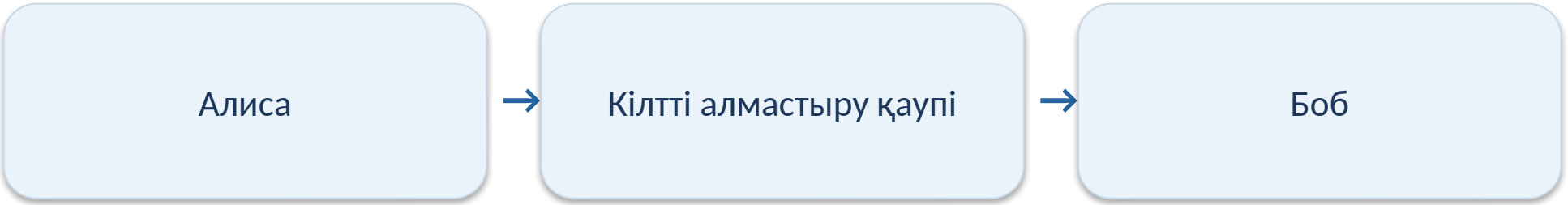
- $p = 23$, $g = 5$, $a = 6$, $b = 15$.
- Алиса: $A = 5^{6} \bmod 23 = 8$.
- Боб: $B = 5^{15} \bmod 23 = 19$.

Оқу мысалы: ортақ құпия

$$K_A = K_B = 2$$

- Алиса: $K_A = 19^{6} \bmod 23 = 2$.
- Боб: $K_B = 8^{15} \bmod 23 = 2$.
- Ортақ нәтиже — 2. Бұл шағын сандар нақты қауіпсіздікке жарамайды.

Неге аутентификация керек?



- Қарапайым Диффи–Хеллман тараптардың кім екенін өзі растамайды.
- Делдал шабуылына жол бермеу үшін түпнұсқалықты тексеру қажет.

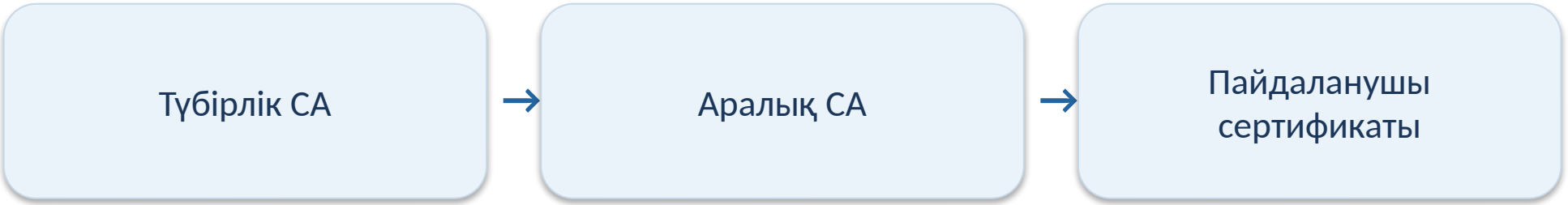
Ашық кілттің түпнұсқалығы

- Ашық кілт құпия емес, бірақ оның иесі сенімді анықталуы тиіс.
- Бобтың орнына басқа адамның кілті берілсе, құпиялылық бұзылуы мүмкін.

Цифрлық сертификат

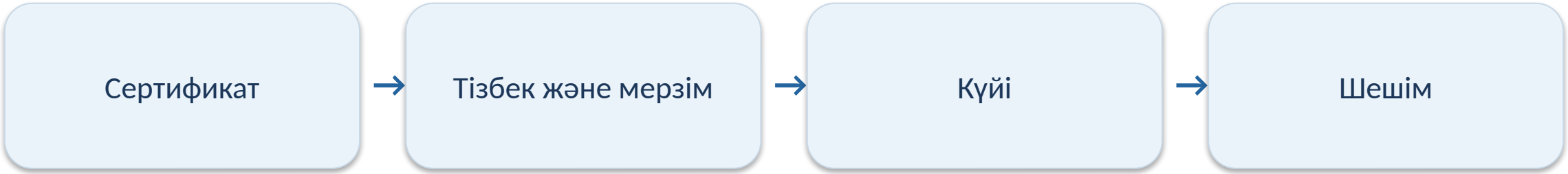
- Сертификат субъектіні ашық кілтпен байланыстырады.
- Негізгі өрістер: субъект, ашық кілт, шығарушы, жарамдылық мерзімі, цифрлық қолтаңба.

PKI инфрақұрылымы



- CA сертификаттарды шығарады және қол қояды.
- Тіркеу рәсімдері мен сертификат күйін тексеру механизмдері қолданылады.

Сертификатты тексеру алгоритмі

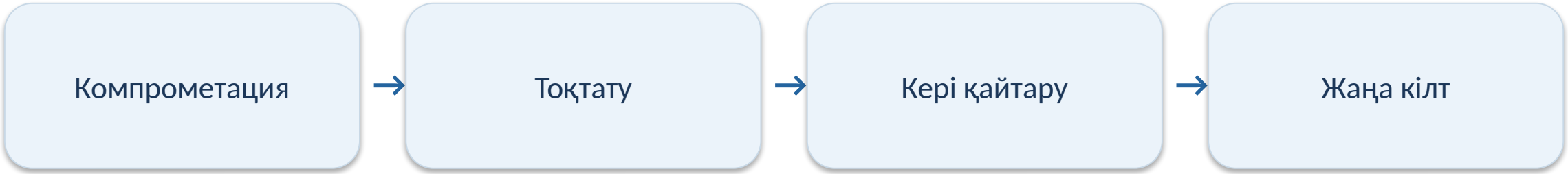


- 1. Сертификаттағы субъект пен мақсатты тексеру.
- 2. Қолтаңба және сенім тізбегін тексеру.
- 3. Жарамдылық мерзімін тексеру.
- 4. Кері қайтару күйін тексеру.

Кілттерді сақтау

- Жабық кілтті ашық мәтіндік файлда сақтау дұрыс емес.
- Қолжетімділікті шектеу, қорғалған қойма немесе аппараттық сақтау қолданылуы мүмкін.

Кілтті кері қайтару



- Кілт жария болып кетсе, оны дереу тоқтату қажет.
- Сертификат күйі CRL немесе OCSP тәрізді механизмдермен тексеріледі.

Механизмдерді салыстыру

Механизм	Мақсаты
Кілт тасымалдау	Дайын К жеткізу
Кілт келісу	Ортақ К есептеу
Сертификат	Кілт иесін растау
PKI	Сертификаттарды басқару

Талдауға арналған жағдай

- Қызметкер жұмыстан шықты, бірақ оның сертификаты белсенді.
- Қандай тәуекел бар? Қай кезеңдер орындалуы керек?
- Жауап: қолжетімділікті тоқтату, кері қайтару, қажет болса кілтті жаңарту.

Қорытынды

- Кілт қауіпсіздігі оның бүкіл өмірлік цикліне байланысты.
- Кілт келісу дайын құпияны ашық арнамен жібермейді.
- PKI ашық кілттің иесін растауға көмектеседі.

Бақылау сұрақтары

- Кілттерді басқару нені қамтиды?
- Кілттің өмірлік циклі қандай?
- Жеке симметриялық кілттер саны қалай есептеледі?
- Тасымалдау мен келісудің айырмасы қандай?
- Диффи–Хеллман идеясы неде?
- Неге аутентификация қажет?
- Сертификат қандай деректерден тұрады?

Әдебиеттер

- Ахметов Б.С. және т.б. Қолданбалы криптология. Алматы, 2016.
- Ахметов Б.С. және т.б. Криптография негіздері. Алматы, 2020.
- Васильева И.Н. Криптографические методы защиты информации. 2024.
- Лось А.Б. және т.б. Криптографические методы защиты информации. 2024.
- Омассон Ж.-Ф. О криптографии всерьез. 2021.