12-ДӘРІС. АШЫҚ КІЛТТІ КРИПТОЖҮЙЕЛЕР

Асимметриялық криптографиялық алгоритмдер

RSA

Цифрлық қолтаңба

SEC1811 «Ақпаратты криптографиялық қорғау негіздері»

Оқытушы: Ахмедиярова А.Т.

Дәрістің оқу нәтижелері

- Ашық және жабық кілттің айырмашылығын түсіндіру
- Асимметриялық шифрлаудың жұмысын сызбада көрсету
- Цифрлық қолтаңбаны шифрлаудан ажырату
- RSA кілттерін есептеп, хабарды шифрлау және ашу
- Симметриялық және асимметриялық тәсілдерді салыстыру

Бір кілт пен екі кілттің айырмашылығы

Симметриялық	Ортақ К	К → дешифрлау
К → шифрлау		

Асимметриялық тәсілде шифрлау мен дешифрлау үшін әртүрлі кілттер қолданылады.

Асимметриялық криптография деген не?

Математикалық байланысқан екі кілт қолданылады: РК және SK

РК (public key) — ашық, басқа адамдарға беруге болады

SK (private key) — жабық, тек иесінде сақталады

Ашық кілттен жабық кілтті табу іс жүзінде өте қиын болуы тиіс

Кілттердің қызметі

АШЫҚ КІЛТ (PK)

Шифрлау

Қолтаңбаны тексеру

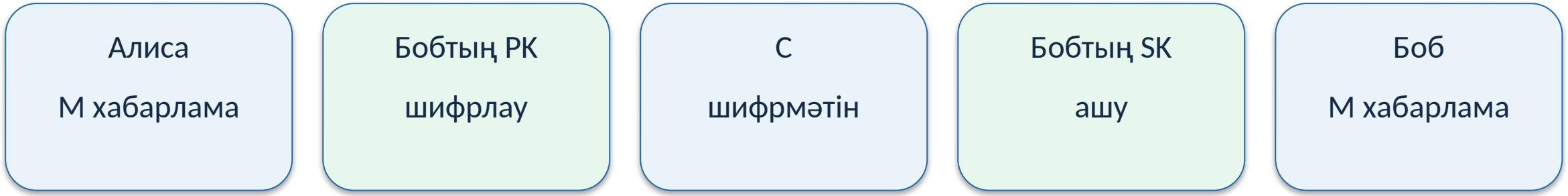
ЖАБЫҚ КІЛТ (SK)

Дешифрлау

Қолтаңба жасау

Есте сақтаңыз: жабық кілт ешкімге берілмейді.

Құпия хабарды жіберу сызбасы



Алиса Бобтың ашық кілтін пайдаланады. Хабарды тек Боб өзінің жабық кілтімен аша алады.

Асимметриялық шифрлау формулалары

C = E_PK(M) — хабарды алушының ашық кілтімен шифрлау

M = D_SK(C) — жабық кілтпен бастапқы хабарды алу

M — бастапқы хабар; C — шифрмәтін

Маңызды: ашық кілттің шынымен Бобқа тиесілі екенін тексеру керек

Күнделікті өмірдегі ұқсастық

Ашық құлып

Кез келген адам жаба алады

Жеке кілт

Тек иесі аша алады

Бұл тек түсіндіруге арналған ұқсастық: нақты криптография математикалық амалдарға негізделеді.

Ашық кілттің түпнұсқалығы неге маңызды?

Алаяқ өз кілтін «Бобтың кілті» деп ұсынуы мүмкін

Алиса қате кілтпен шифрласа, құпия хабар басқа адамға жетуі ықтимал

Сондықтан кілттің иесін сертификатпен немесе сенімді тәсілмен растау қажет

Цифрлық қолтаңба дегеніміз не?

Электрондық құжаттың кімнен келгенін тексеруге көмектеседі

Құжаттың өзгертілген-өзгертілмегенін анықтауға мүмкіндік береді

Қол қою үшін — жабық кілт; ***тексеру үшін*** — ашық кілт

Қолтаңба мен шифрлау бірдей ұғым емес

Цифрлық қолтаңбаның жасалу сызбасы



Хэш — құжаттан есептелетін қысқа сандық мән. Құжат өзгерсе, хэш те әдетте өзгереді.

Цифрлық қолтаңбаны тексеру

Құжат + S

Қол қоюшының РК

Қолтаңбаны тексеру

Жарамды / жарамсыз

Тексеру нәтижесі құжаттың тұтастығын және тиісті кілтпен қол қойылғанын бағалауға мүмкіндік береді.

Шифрлау мен қолтаңбаны шатастырмаңыз

ШИФРЛАУ

Мақсаты: құпиялылық

Алушының PK → алушының SK

ҚОЛТАҢБА

Мақсаты: түпнұсқалық, тұтастық

Қол қоюшының SK → PK арқылы тексеру

RSA деген не?

RSA — ашық кілтті криптографияның классикалық алгоритмі

Негізі: жай сандар, модульдік арифметика, Эйлер функциясы

Алдымен екі әртүрлі жай сан p және q таңдалады

Кейін n, φ(n), e және d есептеледі

Келесі есеп — тек оқу мысалы, нақты қорғанысқа жарамайды

RSA-дағы негізгі белгілер

p, q — әртүрлі жай сандар

$n = p \times q$ — модуль

$\varphi(n) = (p-1)(q-1)$ — Эйлер функциясы

e — ашық көрсеткіш; d — жабық көрсеткіш

PK = (e,n); SK = (d,n)

RSA кілтін құру алгоритмі

1. p және q	2. n = pq	3. φ(n)	4. e таңдау	5. d табу

Шарттар: $1 < e < \varphi(n)$, ЕҮОБ$(e,\varphi(n)) = 1$ және $ed \equiv 1 \pmod{\varphi(n)}$.

1-қадам. Жай сандарды таңдау

p = 5 q = 11

5 пен 11 — жай сандар. Олар әртүрлі.

2-қадам. n және φ(n) есептеу

$$n = p \times q = 5 \times 11 = 55$$

$$\varphi(n) = (p-1)(q-1)$$

$$\varphi(55) = 4 \times 10 = 40$$

3-қадам. e мәнін таңдау

e = 3

1 < 3 < 40

ЕҮОБ(3, 40) = 1

Демек, e = 3 таңдауға болады.

4-қадам. Жабық d көрсеткішін табу

$$3d \equiv 1 \pmod{40}$$

d = 27, өйткені 3 × 27 = 81

81 = 2 × 40 + 1

«mod 40» — 40-қа бөлгендегі қалдықты қарастыру.

RSA кілттері дайын

АШЫҚ КІЛТ

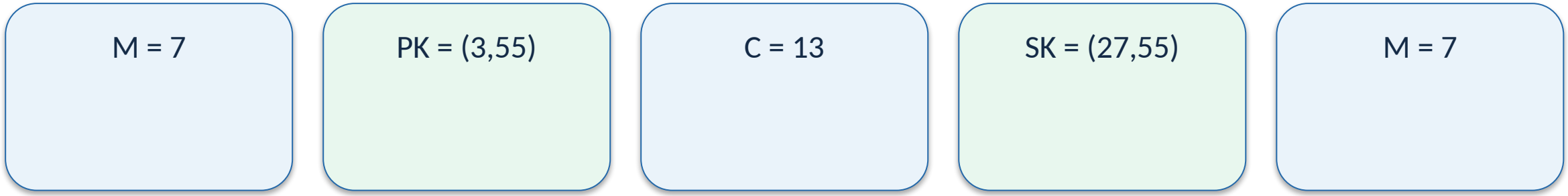
PK = (3, 55)

ЖАБЫҚ КІЛТ

SK = (27, 55)

e = 3 жарияланады, d = 27 құпия сақталады.

RSA: толық жұмыс сызбасы



Алдымен шифрлаймыз, кейін жабық кілтпен бастапқы мәнді қайта аламыз.

5-қадам. RSA арқылы шифрлау

$$C \equiv M^e \pmod{n}$$

$$C \equiv 7^3 \pmod{55}$$

$$7^3 = 343$$

$$343 = 6 \times 55 + 13$$

$$C = 13$$

13 — шифрланған нәтиже.

6-қадам. RSA арқылы дешифрлау

$$M \equiv C^d \pmod{n}$$

$$M \equiv 13^{27} \pmod{55}$$

$$27 = 16 + 8 + 2 + 1$$

Үлкен дәрежені бірден есептемейміз: модульдік дәрежелеуді қолданамыз.

Модульдік дәрежелеу: аралық нәтижелер

$13^{2} \bmod 55 = 4$

$13^{4} \bmod 55 = 16$

$13^{8} \bmod 55 = 36$

$13^{16} \bmod 55 = 31$

Әр келесі дәрежені алдыңғы нәтижені квадраттау арқылы есептейміз.

Дешифрлау нәтижесін тексеру

$$13^{27} \equiv 31 \times 36 \times 4 \times 13 \pmod{55}$$

$$\equiv 7 \pmod{55}$$

Бастапқы M = 7 қалпына келді!

RSA-ның тағы бір шағын мысалы

$p = 5, q = 11 \rightarrow n = 55$

$e = 3, d = 27$

$M = 2$

$C = 2^3 \bmod 55 = 8$

$8^{27} \bmod 55 = 2$

Симметриялық және асимметриялық тәсілдер

СИММЕТРИЯЛЫҚ

Бір ортақ кілт

Жылдам

Көлемді деректерге тиімді

АСИММЕТРИЯЛЫҚ

Ашық және жабық кілт

Есептеуі күрделірек

Кілт келісу, қолтаңба

Гибридті криптография: екі тәсіл бірге

Асимметриялық кілт келісу

Ортақ сеанстық кілт

Симметриялық деректерді шифрлау

Мақсат: кілттермен қауіпсіз жұмыс істеу және үлкен көлемдегі деректерді жылдам қорғау.

Нақты жүйелерде неге назар аударамыз?

p=5 және q=11 — тек оқу есебі, қауіпсіз емес

Қарапайым $C = M^e \bmod n$ өздігінен жеткілікті қорғаныс емес

Нақты RSA шифрлау үшін стандартталған қауіпсіз толтыру схемалары қажет

Жабық кілтті қорғау және ашық кілттің түпнұсқалығын тексеру міндетті

Практикалық тапсырмалар

1. p=3, q=11 болса, n мен φ(n) табыңыз
2. e=3 саны φ(n)=20 үшін жарамды ма? Неліктен?
3. p=5, q=11, e=3 үшін d мәнін анықтаңыз
4. M=2 үшін RSA шифрлауын орындаңыз
5. Шифрлау мен цифрлық қолтаңбаның екі айырмашылығын атаңыз

Бақылау сұрақтары

1. Асимметриялық криптография деген не?
2. РК және SK қандай міндет атқарады?
3. Цифрлық қолтаңба қалай тексеріледі?
4. RSA-да n, φ(n), e, d қалай табылады?
5. Неге RSA-ның оқу мысалы нақты қорғанысқа жарамайды?
6. Гибридті криптожүйе не үшін қажет?

Қорытынды

Асимметриялық криптография екі түрлі кілтке сүйенеді

Ашық кілт жарияланады, жабық кілт құпия сақталады

RSA — модульдік арифметикаға негізделген классикалық мысал

Цифрлық қолтаңба мен шифрлаудың мақсаттары әртүрлі

Практикада екі криптографиялық тәсіл бірге қолданылады

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