12-ДӘРІС
АШЫҚ КІЛТТІ КРИПТОЖҮЙЕЛЕР. АСИММЕТРИЯЛЫҚ КРИПТОГРАФИЯЛЫҚ АЛГОРИТМДЕР

Дәрістің мақсаты

Ашық кілтті криптографияның негізгі идеясын түсіндіру, ашық және жабық кілттердің қызметін ажырату, асимметриялық шифрлау мен цифрлық қолтаңбаның жалпы қағидаларын және RSA математикалық моделінің оқу деңгейіндегі негіздерін көрсету.

Асимметриялық криптография ұғымы

Асимметриялық криптография – криптографиялық түрлендірулерді орындау үшін математикалық байланысқан екі түрлі кілт қолданылатын криптография бағыты. Бұл кілттер ашық кілт (public key) және жабық немесе жеке кілт (private key) деп аталады. Ашық кілтті басқа пайдаланушыларға таратуға болады, ал жабық кілт тек оның иесінде құпия сақталуы тиіс.

(PK, SK)

Мұндағы PK – ашық кілт, SK – жабық кілт. Негізгі идея – кілттердің математикалық байланыста болуы, бірақ ашық кілтті білу арқылы жабық кілтті есептеп табу практикалық тұрғыдан өте қиын болатындай математикалық есептерді пайдалану. Бұл тәсіл симметриялық криптографиядағы кілтті алдын ала құпия түрде жеткізу мәселесін жеңілдетеді.

Ашық және жабық кілт

Кілт	**Мақсаты**	**Құпиялығы**
Ашық кілт PK	Шифрлау немесе цифрлық қолтаңбаны тексеру	Жария болуы мүмкін
Жабық кілт SK	Дешифрлау немесе цифрлық қолтаңба жасау	Құпия сақталады

Ашық кілттің жария болуы криптожүйенің қауіпсіздігін бұзбауы тиіс. Негізгі қорғалатын объект – жабық кілт. Егер жабық кілт бөгде тұлғаның қолына түссе, сол кілтке негізделген қауіпсіздік бұзылуы мүмкін. Сондықтан жабық кілтті қауіпсіз генерациялау, сақтау және пайдалану маңызды талап болып табылады.

Асимметриялық шифрлау

Құпия хабарламаны жіберуші алушының ашық кілтін пайдаланып шифрлайды. Ал алынған шифрмәтінді алушы өзінің жабық кілтімен дешифрлайды.

$$C = E_PK(M)$$
$$M = D_SK(C)$$

Мұнда M – ашық мәтін, C – шифрмәтін, PK – алушының ашық кілті, SK – алушының жабық кілті. Мысалы, Алиса Бобқа құпия хабарлама жібергісі келсе, Бобтың ашық кілтін пайдаланып хабарламаны шифрлайды, ал Боб өзінің жабық кілті арқылы оны қалпына келтіреді. Бұл жағдайда шифрлау кілтін алдын ала құпия арна арқылы бөлісу қажет емес, бірақ ашық кілттің шынымен тиісті иеге тиесілі екенін растау мәселесі сақталады.

Цифрлық қолтаңба идеясы

Цифрлық қолтаңба – электрондық деректердің түпнұсқалығын және тұтастығын тексеруге мүмкіндік беретін криптографиялық механизм. Қолтаңба иесі өзінің жабық кілтін пайдаланып қолтаңба қалыптастырады, ал тексеруші ашық кілт арқылы оның дұрыстығын тексереді.

$$M \rightarrow H(M) \rightarrow Sign_SK(H(M)) \rightarrow S$$

Мұндағы H(M) – хабарламаның криптографиялық хэші, SK – қол қоюшының жабық кілті, S – цифрлық қолтаңба. Практикада көбіне хабарламаның толық мәтініне тікелей қолтаңба жасалмайды: алдымен $h=H(M)$ хэш-мәні есептеледі. Хабарлама өзгерсе, оның хэші де өзгеруі ықтимал, сондықтан тексеру кезінде деректердің өзгертілгенін анықтауға болады. Цифрлық қолтаңба құпиялылықты қамтамасыз ететін шифрлаумен бірдей ұғым емес.

RSA-ның математикалық негізі

RSA – ашық кілтті криптографияның классикалық алгоритмдерінің бірі. Оның математикалық негізінде жай сандар, модульдік арифметика, Эйлер функциясы және модуль бойынша кері элемент ұғымдары жатыр. Оқу моделінде алдымен екі әртүрлі жай сан p және q таңдалады.

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

Келесі кезеңде e саны таңдалады. Ол $1<e<\varphi(n)$ және $\gcd(e,\varphi(n))=1$ шарттарын қанағаттандыруы керек. Содан кейін d саны e-нің φ(n) модулі бойынша кері элементі ретінде есептеледі:

$$ed \equiv 1 \pmod{\varphi(n)}$$
$$d \equiv e^{-1} \pmod{\varphi(n)}$$

Оқу моделінде ашық кілт PK=(e,n), ал жабық кілт SK=(d,n) параметрлерімен байланыстырылады.

RSA кілттерін есептеудің қарапайым мысалы

Екі жай сан таңдаймыз: p=5 және q=11. Сонда $n=5\cdot11=55$. Эйлер функциясы $\varphi(n)=(5-1)(11-1)=4\cdot10=40$. Енді 40-пен өзара жай e=3 санын аламыз, себебі $\gcd(3,40)=1$.

d санын $3d \equiv 1 \pmod{40}$ шарты бойынша табамыз. d=27, өйткені $3\cdot27=81$ және $81 \equiv 1 \pmod{40}$.

$$PK = (3,55)$$
$$SK = (27,55)$$

RSA шифрлау

Ашық мәтін ретінде оқу мысалы үшін M=7 мәнін алайық. Шифрлау формуласы:

$$C \equiv M^e \pmod{n}$$
$$C \equiv 7^3 \pmod{55} = 343 \pmod{55} = 13$$

Демек, M=7 ашық мәні C=13 шифрмәтініне түрленеді.

RSA дешифрлау

Алынған C=13 шифрмәтінін жабық d=27 кілті арқылы дешифрлаймыз:

$$M \equiv C^d \pmod{n}$$
$$M \equiv 13^{27} \pmod{55}$$

Үлкен дәрежені бірден есептеудің орнына модульдік дәрежелеу қолданылады: $13^2 \equiv 4 \pmod{55}$, $13^4 \equiv 16 \pmod{55}$, $13^8 \equiv 36 \pmod{55}$, $13^{16} \equiv 31 \pmod{55}$. $27=16+8+2+1$ болғандықтан:

$$13^{27} \equiv 31\cdot36\cdot4\cdot13 \equiv 7 \pmod{55}$$

Нәтижесінде бастапқы M=7 мәні қайта қалпына келеді.

RSA жұмысының жалпы сұлбасы

$$p, q \rightarrow n=pq \rightarrow \varphi(n) \rightarrow e \rightarrow d$$

$$M \rightarrow (e,n) \text{ арқылы шифрлау} \rightarrow C \rightarrow (d,n) \text{ арқылы дешифрлау} \rightarrow M$$

RSA-ның маңызды ерекшелігі – шифрлау үшін қажетті (e,n) ашық кілтін жариялауға болады, ал d жабық параметрі құпия сақталады.

Симметриялық және асимметриялық криптографияның айырмашылығы

Белгі	**Симметриялық криптография**	**Асимметриялық криптография**
Кілттер	Ортақ құпия кілт	Ашық және жабық кілт
Кілтті тарату	Құпия түрде ұйымдастыру қажет	Ашық кілт жариялануы мүмкін
Жылдамдық	Әдетте жоғары	Әдетте есептеу күрделілігі жоғарырақ
Үлкен көлемдегі деректер	Тиімді	Әдетте негізгі мақсат емес
Цифрлық қолтаңба	Негізгі қызметі емес	Қолданылады
Негізгі мәселе	Құпия кілтті қауіпсіз бөлу	Жабық кілтті қорғау және ашық кілттің түпнұсқалығын растау

Практикалық ақпараттық жүйелерде симметриялық және асимметриялық криптография көбіне бірін-бірі толықтыратын механизмдер ретінде қолданылады. Асимметриялық механизмдер кілттерді басқару, келісу немесе цифрлық қолтаңба міндеттерінде қолданылса, үлкен көлемдегі деректерді қорғау үшін жылдам симметриялық алгоритмдер пайдаланылуы мүмкін.

Жоғарыдағы p=5 және q=11 мәндері тек математикалық принципті түсіндіруге арналған оқу мысалы. Нақты криптографиялық жүйелерде мұндай шағын параметрлер қауіпсіз емес және қарапайым $C=M^e \bmod n$ схемасы өздігінен жеткілікті қорғаныс болып саналмайды; стандартталған қауіпсіз схемалар мен параметрлер қолданылады.

Шағын есептік мысал

p=5, q=11 алайық. n=55, $\varphi(n)=4\cdot10=40$. e=3 таңдауға болады, себебі gcd(3,40)=1. $3d\equiv1 \pmod{40}$, сондықтан d=27. M=2 үшін $C=2^3 \bmod 55=8$. Дешифрлау $8^{27} \bmod 55$ арқылы бастапқы 2 мәнін береді. Бұл тек математикалық қағиданы көрсетуге арналған шағын оқу мысалы.

Симметриялық және асимметриялық тәсілдерді салыстыру

Белгі	**Симметриялық**	**Асимметриялық**
Кілттер	Ортақ құпия кілт	Ашық/жабық жұбы
Жылдамдық	Әдетте жоғары	Әдетте баяурақ
Кілт бөлу	Құпия арна мәселесі бар	Ашық кілт жарияланады, бірақ түпнұсқалығы тексерілуі тиіс
Қолдану	Негізгі деректерді шифрлау	Кілт алмасу, қолтаңба, шағын криптографиялық операциялар

Гибридті қолдану

Практикалық жүйелерде симметриялық және асимметриялық тәсілдер жиі бірге қолданылады: асимметриялық механизм кілтті келісуге немесе түпнұсқалықты растауға, ал симметриялық алгоритм негізгі деректер ағынын тиімді шифрлауға қызмет етеді.

Қорытынды

Ашық кілтті криптография ашық және жабық кілт жұбына негізделеді. Ол құпия кілтті алдын ала ортақ арнамен жеткізу мәселесін өзгертіп, шифрлау, кілт алмасу және цифрлық қолтаңба міндеттерін шешуге мүмкіндік береді. RSA оның сандар теориясына негізделген классикалық мысалы болып табылады.

Бақылау сұрақтары

1. Асимметриялық криптография дегеніміз не?
2. Ашық және жабық кілттердің айырмашылығы қандай?
3. Асимметриялық шифрлау қалай орындалады?
4. Цифрлық қолтаңбада жабық және ашық кілттер қалай қолданылады?
5. RSA-да n қалай есептеледі?
6. RSA үшін φ(n) қалай табылады?
7. e және d параметрлері қандай қатынасты қанағаттандырады?
8. RSA-ның оқу формуласындағы шифрлау мен дешифрлау қалай жазылады?
9. Симметриялық және асимметриялық шифрлардың негізгі айырмашылығы неде?
10. Гибридті криптографиялық жүйе не үшін қолданылады?

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.