Асимметриялық криптография және жылдам әдістер

Пән: Ақпараттық қауіпсіздік

Лекция №4: Асимметриялық криптография және ашық кілтті жүйелер

Лекция мақсаты мен негізгі сұрақтар

Мақсаты

Асимметриялық (ашық кілтті) криптожүйелердің идеясын түсіндіру және RSA криптожүйесінің негізгі қадамдарын қарастыру.

Негізгі сұрақтар

- Асимметриялық криптожүйелер деген не?
- Біржақты функция және оның маңызы неде?
- RSA криптожүйесіндегі кілттер және шифрлау/ашу процестері.

Бұл лекция ақпаратты қауіпсіз жіберудің маңызды әдістерінің бірі болып табылатын асимметриялық криптографияның негіздерін түсінуге бағытталған.

Симметриялық пен асимметриялық криптографияны салыстыру

Симметриялық криптожүйелер

- Шифрлау мен дешифрлау үшін бірдей құпия кілт пайдаланылады.
- Жылдам, үлкен көлемдегі деректерге ыңғайлы.
- Кілтті тарату мәселесі қиындық туғызады (қауіпсіз жеткізу қажет).

Асимметриялық криптожүйелер

- Екі түрлі кілт: ашық (барлығына белгілі) және құпия (тек иесіне белгілі).
- Ашық кілтпен шифрлау, құпия кілтпен ашу орындалады.
- Кілтті тарату қауіпсіздігі жоғары, себебі құпия кілт жіберілмейді.

Ашық кілтті криптожүйенің жалпы схемасы

Негізгі идея: Қабылдаушы (B) кілттер жұбын (KB – ашық, kB – құпия) генерациялайды. Жіберуші (A) B-ның ашық кілтін алып, хабарды шифрлайды, ал B құпия кілтпен хабарды ашады.

Ерекшеліктері:

- Ашық кілт (KB) және шифрмәтін (C) қорғалмаған арна арқылы жіберілуі мүмкін.
- Қауіпсіздік құпия кілтті (kB) табудың қиындығына негізделген.
- Шифрлау және ашу алгоритмдері ашық болуы мүмкін.

Ашық кілтті жүйеге қойылатын талаптар

Кілттер жұбын табу оңай

Қабылдаушы (B) өз жұбын (KB, kB) тез есептей алуы қажет.

Шифрлау және дешифрлау оңай

Ашық кілт пен хабарды біле отырып, шифрмәтін жылдам есептеледі, сондай-ақ құпия кілтпен дешифрлау да жылдам болуы керек.

Қарсылас үшін кілтті табу қиын

Ашық кілт белгілі болса да, құпия кілтті есептеу өте қиын болуы қажет.

Қарсылас үшін хабарды табу қиын

Ашық кілт пен шифрмәтін белгілі болғанда да, бастапқы хабарды табу есептеу жағынан мүмкін болмауы керек.

Бұл талаптар асимметриялық криптожүйенің практикалық қауіпсіздігінің негізі болып саналады.

Біржақты функция ұғымы

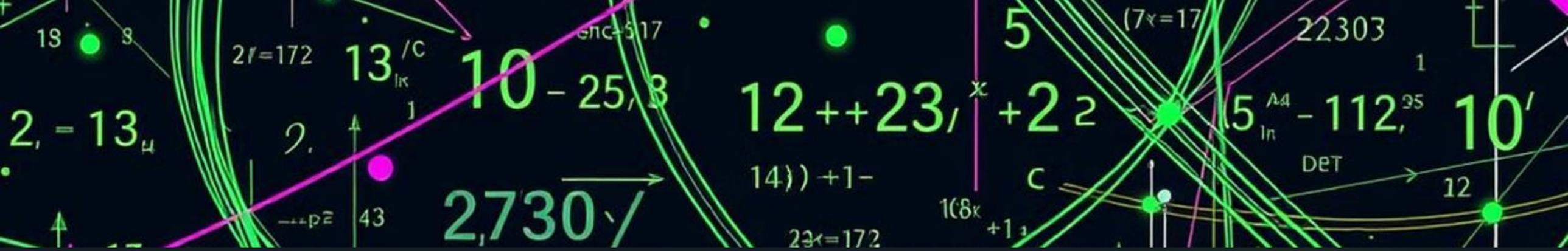
Анықтама

Біржақты функция $f : X \to Y$ – тура бағытта есептеу оңай (x берілсе, $y = f(x)$ тез табылады), ал кері бағытта қиын (көп y үшін, оған сәйкес x-ті табу өте қиын).

Мысал: Көбейту және факторизация

Екі үлкен жай сан P және Q берілсе, $N = P \cdot Q$ табу оңай. Бірақ үлкен N берілгенде, оны P және Q көбейткіштеріне жіктеу өте қиын.

Қауіпсіз криптожүйелерді құру үшін осындай "есептеуге оңай, кері табуға қиын" функциялар қолданылады.



Модульдік экспоненттеу және дискретті логарифм

Модульдік экспоненттеу

N модулі және A негізі берілсін. $f(x) = A^x \pmod N$ функциясын тура бағытта есептеуге тиімді алгоритмдер бар (жылдам дәрежелеу).

$$f(x) = A^x \pmod N$$

Бұл біржақты функцияның "оңай бағыты".

Дискретті логарифм есебі

Берілген A, N, y үшін $A^x \equiv y \pmod N$ теңдігін қанағаттандыратын x табу керек. Қазіргі уақытта бұл есеп үшін жылдам алгоритм табылған жоқ.

$$A^x \equiv y \pmod N$$

Бұл біржақты функцияның "қиын бағыты".

Осындай есептер біржақты функция рөлін атқара алады. Дискретті логарифмдеуге негізделген көптеген ашық кілтті жүйелер бар.

«Құпия жолы бар» біржақты функциялар және RSA идеясы

Құпия жол идеясы

Біржақты функцияға арнайы құпия ақпарат (құпия жол) белгілі болса, кері функцияны есептеу оңай болады.

RSA жүйесіндегі модульдік экспоненттеу

Ашық параметрлер: n, e. Құпия параметр: d немесе n-нің жай көбейткіштері p, q.

Басты идея

n = p·q – екі үлкен жай санның көбейтіндісі. p және q белгілі болса, d-ны табу жеңіл; ал p мен q-ды білмей d табу өте қиын.

Бұл қағида RSA криптожүйесінің негізі болып табылады, онда кілттерді генерациялау және хабарды шифрлау/дешифрлау осы біржақты функцияның қасиеттерін пайдаланады.

RSA криптожүйесінің жұмыс қадамдары

1. Кілттерді генерациялау

Екі үлкен жай сан (p, q) таңдалады, n = p·q және ϕ(n) = (p−1)(q−1) есептеледі. Содан кейін e және d сандары d·e ≡ 1 (mod ϕ(n)) шартын қанағаттандыратындай етіп табылады.

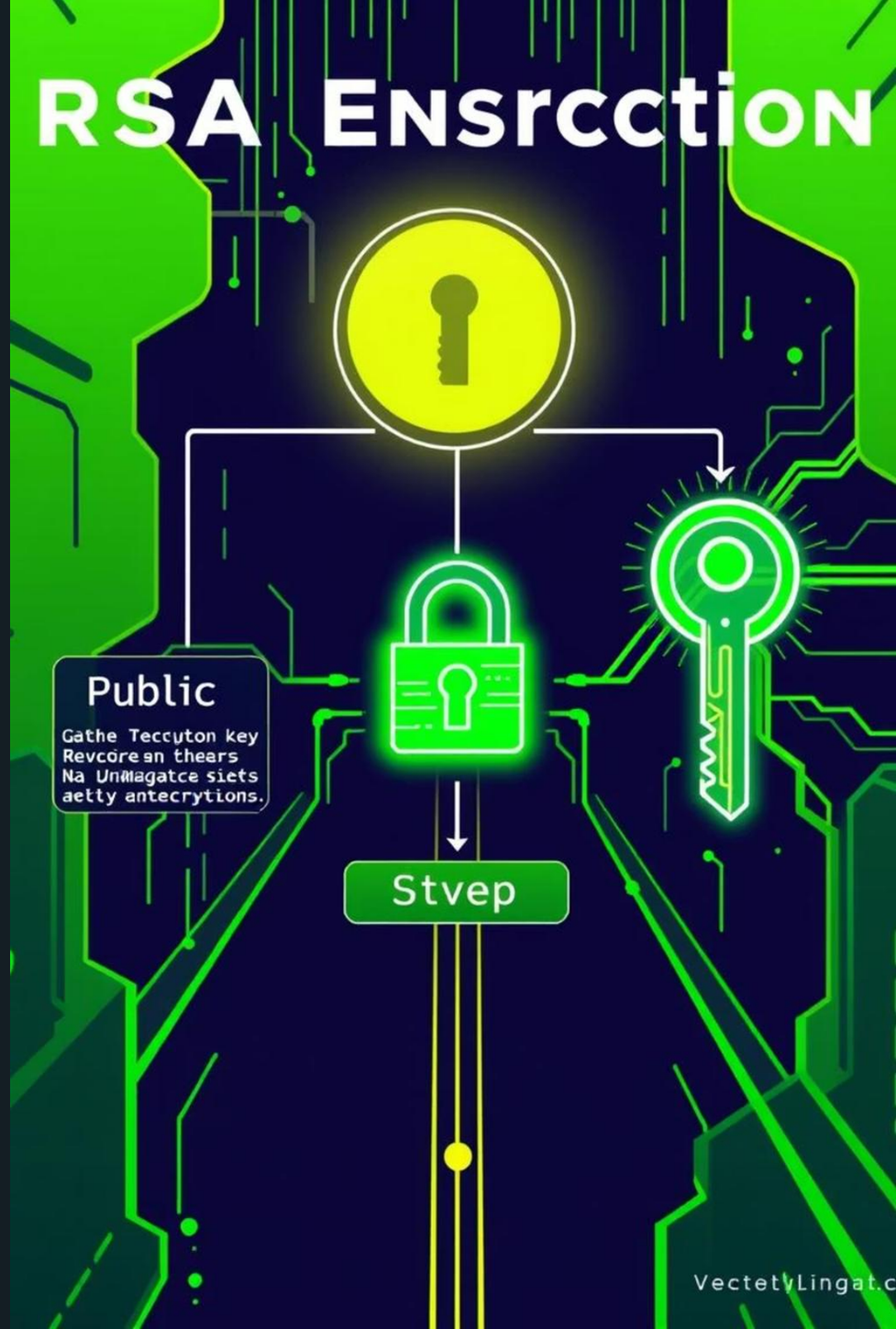
2. Ашық және құпия кілттер

Ашық кілт: (e, n) – барлығына белгілі. Құпия кілт: (d, n) – тек иеде сақталады.

3. Шифрлау және дешифрлау

Шифрлау: $C = M^e \pmod n$, мұндағы M – хабардың сандық көрінісі. Дешифрлау: $M = C^d \pmod n$.

RSA жүйесі n-ді p және q-ға жіктеудің қиындығына негізделеді, бұл d-ны табуды өте қиындатады. Бұл тек шифрлауға ғана емес, цифрлық қолтаңба жасауға да қолданылады.



Бақылау сұрақтары және пайдаланылған әдебиеттер

Бақылау сұрақтары

- Асимметриялық және симметриялық криптожүйелердің негізгі айырмашылығы қандай?
- Ашық және құпия кілттің қолданылуы мен мақсаты неде?
- Біржақты функцияның мәні мен мысалдарын келтіріңіз.
- «Құпия жолы бар» біржақты функцияны түсіндіріңіз.
- RSA кілттерін генерациялау және шифрлау/дешифрлау формулаларын жазыңыз.

Пайдаланылған әдебиеттер

- Қырғызбаева, Г. Ә. (2021). Криптография негіздері. Алматы: Қазақ университеті.
- Нұрсейіт, Р. М. (2022). Цифрлық қауіпсіздік: теория мен практика. Алматы: «Қазақ ұлттық кітапханасы».
- Махмутов, К. Т., & Шекенова, А. О. (2023). Симметриялық және асимметриялық криптожүйелер. ҚазМУ хабаршысы, 3(45), 56–62.