Кілттердің Ашық Таратылуы: RSA және Диффи–Хеллман

Пән: Ақпараттық қауіпсіздік

Лекция №5

Орындаған: [Орындағанның Аты-жөні]

Тексерген: [Тексергеннің Аты-жөні]

Университет, Кафедра, [Жыл]

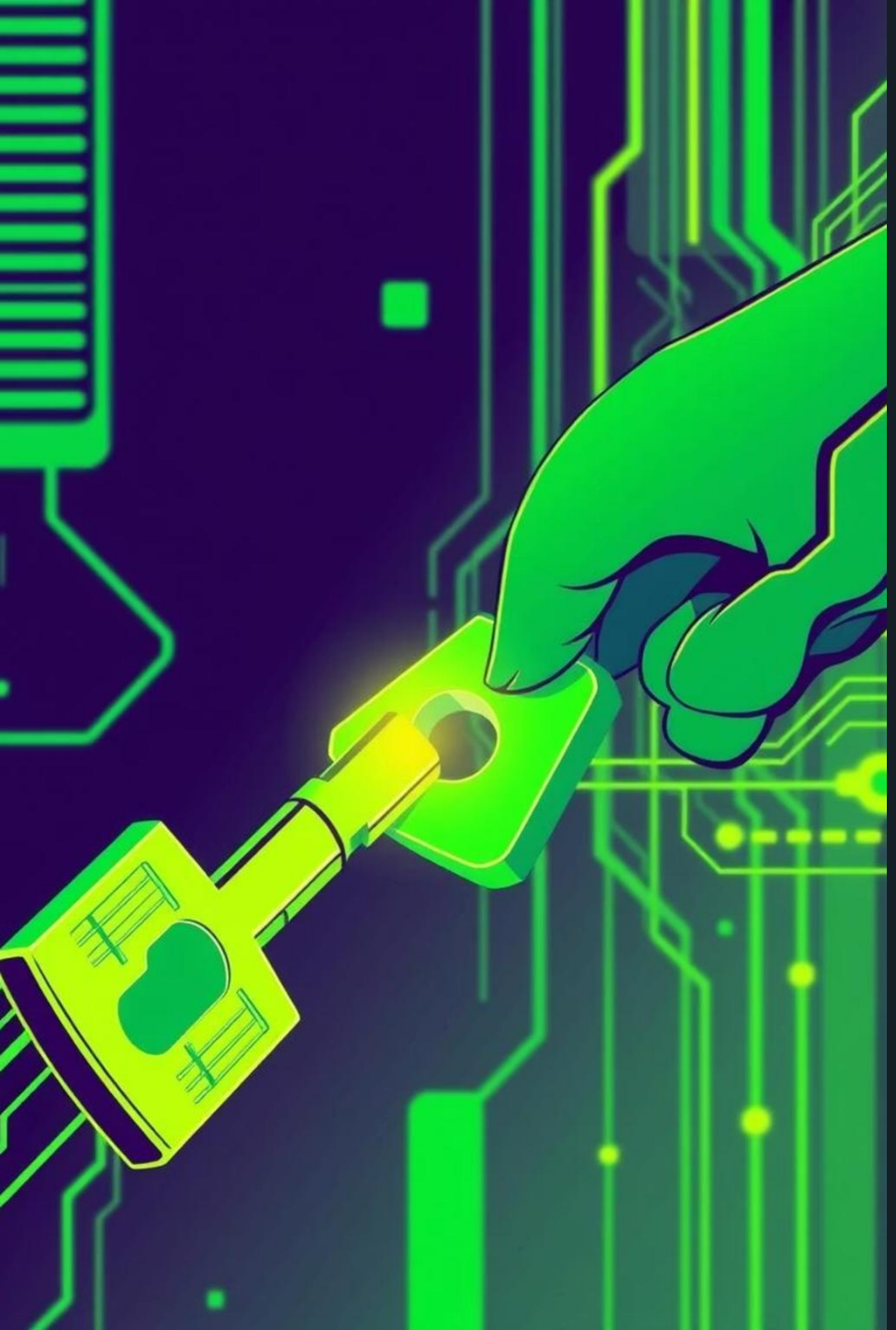
Лекцияның Мақсаты мен Негізгі Сұрақтар

Лекцияның Мақсаты:

- RSA криптожүйесінің жұмыс принципін түсіну.
- Диффи–Хеллман алгоритмінің ашық кілттермен алмасудағы рөлін қарастыру.
- Криптожүйе қауіпсіздігін қамтамасыз ететін техникалық әдістерді түсіндіру.

Негізгі Сұрақтар:

- RSA қалай жұмыс істейді?
- Диффи–Хеллман алгоритмінің идеясы қандай?
- Біржақты функциялар қай жерде қолданылады?
- Ашық кілтті жүйелерде кілтті қауіпсіз тарату қалай ұйымдастырылады?
- RSA мен Диффи–Хеллманның айырмашылығы неде?



Кілтті Тарату Мәселесі және Шешу Тәсілдері

Кілтті Тарату Неге Проблема?

- Қолданушылар ортақ құпия кілтпен алмасуы керек, бірақ бұл әрқашан қауіпсіз емес.
- Егер кілт жиі ауыстырылса, оны үнемі қауіпсіз жеткізу қиынға соғады, бұл жүйені осал етеді.

1. Симметриялық Кілтті Жіберу

Ашық кілтті криптожүйе (мысалы, RSA) арқылы симметриялық кілтті шифрлап жіберу.

2. Диффи–Хеллман Алгоритмін Қолдану

Диффи–Хеллман алгоритмі арқылы ашық арналар арқылы қауіпсіз кілт алмасу.

Ашық кілтті криптография кілт тарату мәселесін жеңілдетеді, бірақ оның да өзіндік талаптары мен шарттары бар екенін есте ұстаған жөн.

Диффи–Хеллман Алгоритмінің Идеясы

Бастапқы Параметрлер:

- Екі қолданушы: A және B.
- Алдын ала жалпы параметрлерге келіседі:

Үлкен модуль N (көбінесе жай сан).

Примитивті элемент $g \in Z_N$.

Бұл N мен g құпия емес, барлық қолданушыларға ортақ болуы мүмкін.

Қолданушылардың Құпия Кілттері:

A өзіне құпия k_A таңдайды.

B өзіне құпия k_B таңдайды.

- Бұл сандар үлкен, кездейсоқ және құпия сақталады.

Идея:

Әрқайсысы өз ашық кілтін есептейді де, ашық арна арқылы алмасады. Нәтижесінде екеуі де бірдей ортақ құпия K-ге ие болады.

Диффи–Хеллман Алгоритмінің Қадамдары

1. A ашық кілтін есептейді:

$y\_A = g^{k\_A} \pmod{N}$

2. B ашық кілтін есептейді:

$y\_B = g^{k\_B} \pmod{N}$

3. Ашық арна арқылы алмасады:

y_A және y_B алмасады.

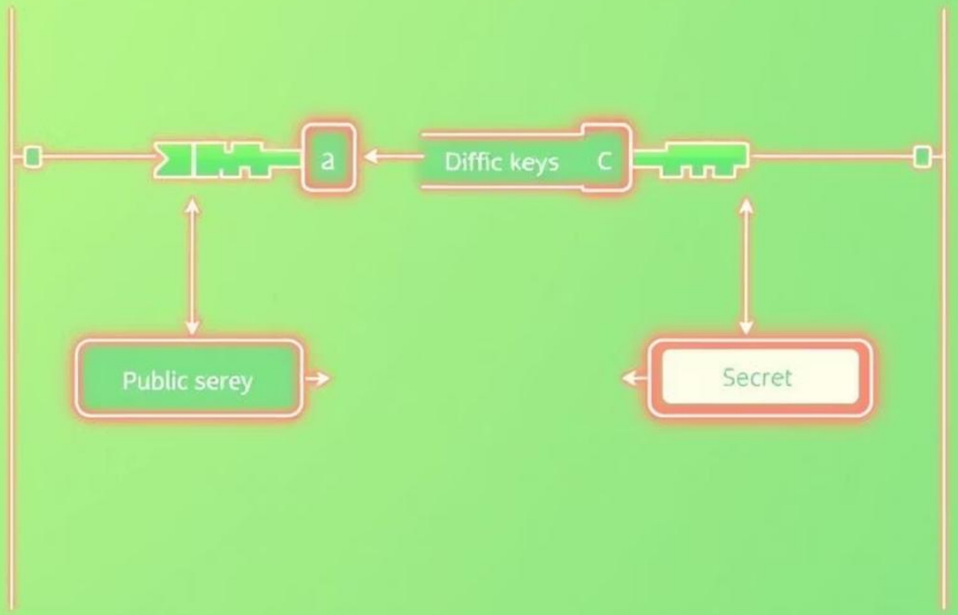
4. A ортақ құпияны есептейді:

$K = (y\_B)^{k\_A} = g^{k\_B\, k\_A} \pmod{N}$

5. B ортақ құпияны есептейді:

$K' = (y\_A)^{k\_B} = g^{k\_A\, k\_B} \pmod{N}$

Теория бойынша $K = K'$, сондықтан ортақ құпия кілт бірдей болады, бұл қауіпсіз байланысты қамтамасыз етеді.



Диффи–Хеллман Мысалы

Мысал ретінде келесі параметрлерді қолданайық:

$N = 47$, $g = 23$.

A үшін құпия кілт: $k\_A = 12$

B үшін құпия кілт: $k\_B = 33$

Ашық кілттерді есептеу:

- $y\_A = g^{k\_A} = 23^{12} \equiv 27 \pmod{47}$
- $y\_B = g^{k\_B} = 23^{33} \equiv 33 \pmod{47}$

Ортақ құпия кілтті есептеу:

A есептейді: $K = y\_B^{k\_A} = 33^{12} \pmod{47}$

B есептейді: $K = y\_A^{k\_B} = 27^{33} \pmod{47}$

Нәтижесінде екі жақта да ортақ құпия кілт $K = 25 \pmod{47}$ болып шығады.

> Қорытынды: Екі жақтың құпиялары (k_A, k_B) әртүрлі болғанымен, ортақ кілт бірдей шығады. Бұл кілт кейін симметриялық шифрлау үшін қолданылуы мүмкін.

Диффи–Хеллман Қауіпсіздігі

Қарсылас не көреді?

Қарсылас тек ашық параметрлерді көреді: N, g, y_A, y_B. Ортақ құпияны табу үшін оған дискретті логарифм есебін шешу керек, мысалы, $g^{k_A} \pmod{N} = y_A$ теңдігінен k_A-ны табу.

Неге қауіпсіз?

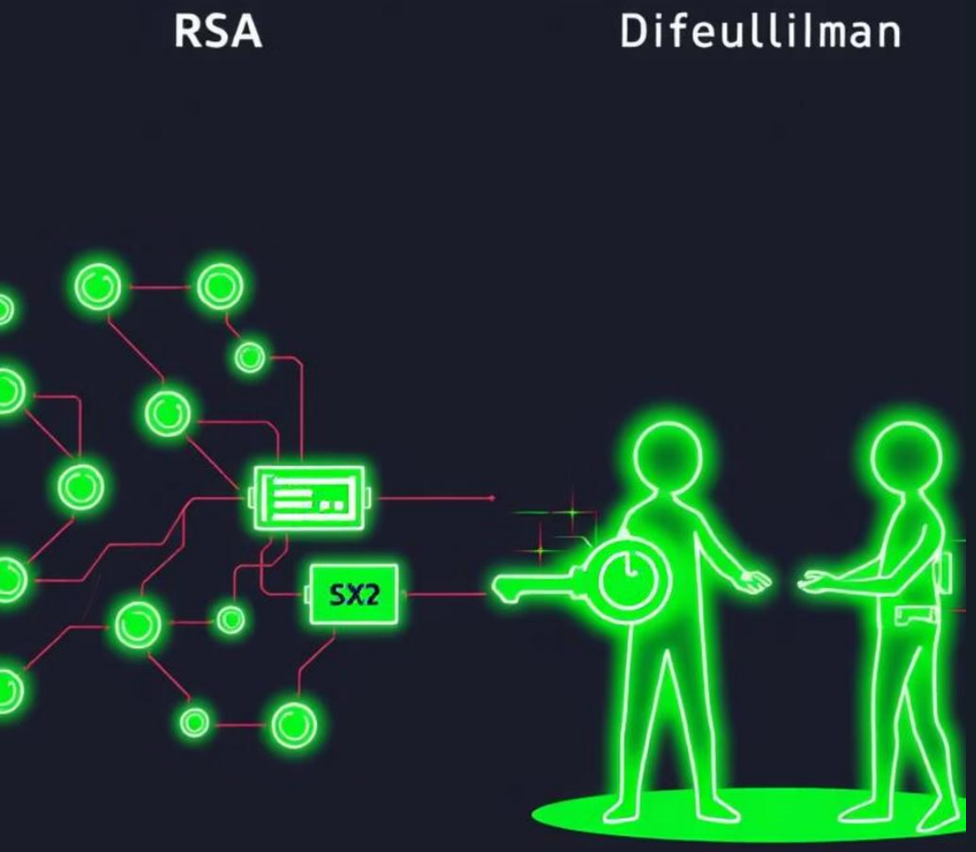
Үлкен N және дұрыс таңдалған g үшін дискретті логарифм есебін шешу өте қиын болып табылады. Қазіргі есептеу мүмкіндіктерімен бұл мәселені шешу іс жүзінде мүмкін емес.

N және g Таңдау Шарттары:

N – өте үлкен жай сан.

$(N-1)/2$ да жай сан болғаны дұрыс.

g – Z_N-дағы примитивті элемент.



RSA және Диффи–Хеллманды Салыстыру

RSA Криптожүйесі

- Факторизацияның (жай бөлгіштерге жіктеудің) қиындығына негізделген.
- Ашық кілтпен шифрлау, құпия кілтпен дешифрлау.
- Кілт генерациясы баяу, өйткені жаңа үлкен жай сандарды табу қажет.

Диффи–Хеллман Алгоритмі

- Дискретті логарифмнің қиындығына негізделген.
- Негізгі мақсаты – ортақ симметриялық кілтті қауіпсіз құру.
- Ортақ құпияны қалыптастыру RSA-ға қарағанда әлдеқайда жылдам орындалады.

SKIP Хаттамасы (Simple Key Management for Internet Protocol):

Диффи–Хеллманға негізделген кілттерді басқару жүйесі. Ол мәліметтерді қорғаудың жоғары деңгейін және кілттердің тез алмасуын қамтамасыз етеді, сондай-ақ топтық таратуда да кілттермен жұмыс істей алады.

Факторизация Қиындығы және Қауіпсіздік Деңгейі

Факторизацияның Дамуы:

Соңғы жылдары үлкен сандарды жіктеу (факторизация) алгоритмдері айтарлықтай жақсарды. GNFS (General Number Field Sieve) – қазіргі ең мықты әдістердің бірі болып табылады және 110 таңбалы және одан үлкен сандарға қолданылады.

Есептеу Ресурстары:

Мипсогод (MIPS-year) – секундына 1 млн операция орындайтын машина бір жылда орындайтын амалдар саны. Түрлі бит ұзындықтағы кілттерге қажетті есептеу көлемі экспоненциалды түрде өседі:

512

Биттік Модуль

Орташа қауіпсіздік

768

Биттік Модуль

Жоғары қауіпсіздік

1024

Биттік Модуль

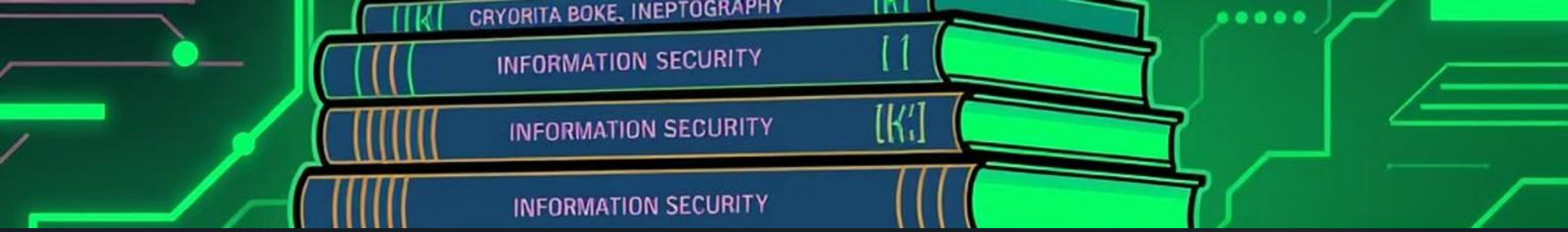
Өте жоғары қауіпсіздік

2048

Биттік Модуль

Ең жоғары қауіпсіздік

> Р. Л. Ривесттің бағалауы бойынша, аппараттық және бағдарламалық прогресті ескере отырып, кілт ұзындығын таңдауда қауіпсіздік пен практикалық мүмкіндіктер арасындағы баланс қажет.



Бақылау Сұрақтары және Пайдаланылған Әдебиеттер

Материалды Меңгеруді Бақылау Сұрақтары:

- RSA криптосистемасының жұмыс істеу принципін өз сөзіңізбен түсіндіріңіз.
- Диффи–Хеллман алгоритмінің негізгі қадамдарын жазыңыз.
- Біржақты функция дегеніміз не? Мысал келтіріңіз.
- RSA мен Диффи–Хеллман алгоритмдерінің арасындағы басты айырмашылықтарды атаңыз.
- Кілттерді қауіпсіз таратудың қандай әдістерін білесіз?

Пайдаланылған Әдебиеттер:

- El Assad, S. (Ed.). (2022). Cryptography and Its Applications in Information Security. MDPI.
- Zheng, Z. (2022). Modern Cryptography Volume 1: A Classical Introduction to Informational and Mathematical Principles. Springer.
- Easttom, C. (2024). Modern Cryptography: Applied Mathematics for Encryption, and Information Security (2nd ed.). Springer.