Криптожүйелерді жүйелеу және орындаудың қауіпсіздігі

Лекция №6

Пәні: Ақпараттық қауіпсіздік

Орындаған: [Орындаушының аты-жөні]

Тексерген: [Тексерушінің аты-жөні]

Университет, кафедра, жыл

Лекцияның мақсаты және негізгі сұрақтар

Мақсаты:

- RSA жүйесін жеделдету әдістерін (Қытай қалдық теориясы, CRT) түсіндіру.
- Эль-Гамаль, Месси–Омура, Полига–Хеллман сияқты асимметриялық криптожүйелердің жұмыс принципін қарастыру.
- Аралас шифрлау әдісінің артықшылықтарын көрсету.
- Кілт ұзындығы мен қауіпсіздіктің өзара байланысын түсіндіру.

Негізгі сұрақтар:

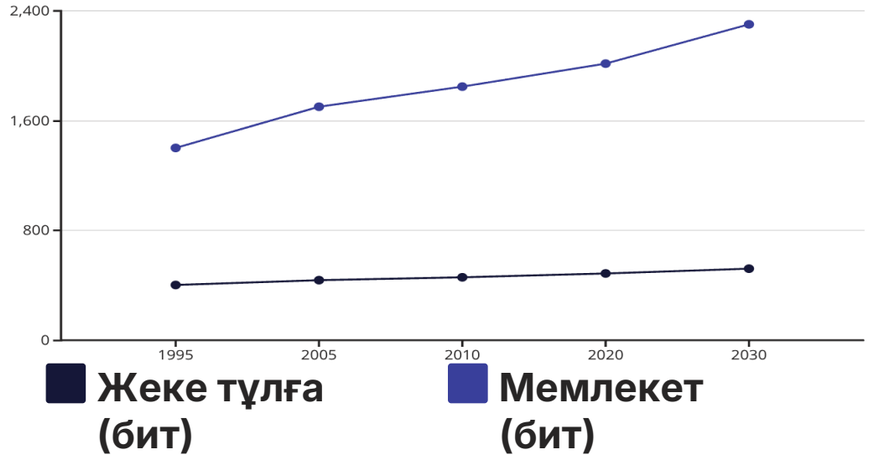
1. RSA шифрын CRT арқылы қалай жеделдетуге болады?
2. Эль-Гамаль криптожүйесінің қауіпсіздігі неден туындайды?
3. Месси–Омура және Полига–Хеллман алгоритмдерінің ерекшеліктері қандай?
4. Аралас (гибрид) шифрлау деген не және неге қолданылады?
5. Кілт ұзындығы уақытқа байланысты қалай өзгеріп отырады?

Кілт ұзындығы мен қауіпсіздік: тарихи даму

Криптожүйенің қауіпсіздігі кілт ұзындығына тікелей байланысты. Есептеу техникасы күшейген сайын «қауіпсіз» деп саналатын кілт ұзындықтары да өседі.

Тарихи мысал – RSA-129:

- 129 ондық таңбалы (≈ 425 бит) сан 1977 ж. «сынақ» ретінде жарияланған.
- 17 жыл бойы (1600 компьютер бірігіп) факторизация жасалды, тек 1994 ж. толық шешілді.
- Қазір осындай есеп қазіргі техникамен әлдеқайда тез шешіледі, бұл кілт ұзындығының маңыздылығын көрсетеді.



Бұл график әр жылға арналған болжамды қауіпсіз кілт ұзындықтарын көрсетеді.

RSA жүйесін CRT арқылы жеделдету

Мәселе: Дешифрлау формуласы: $M=C^d \mod N$. Бұл — дәрежеге көтеру, өте ауыр есеп (үлкен d, үлкен N).

CRT идеясы:

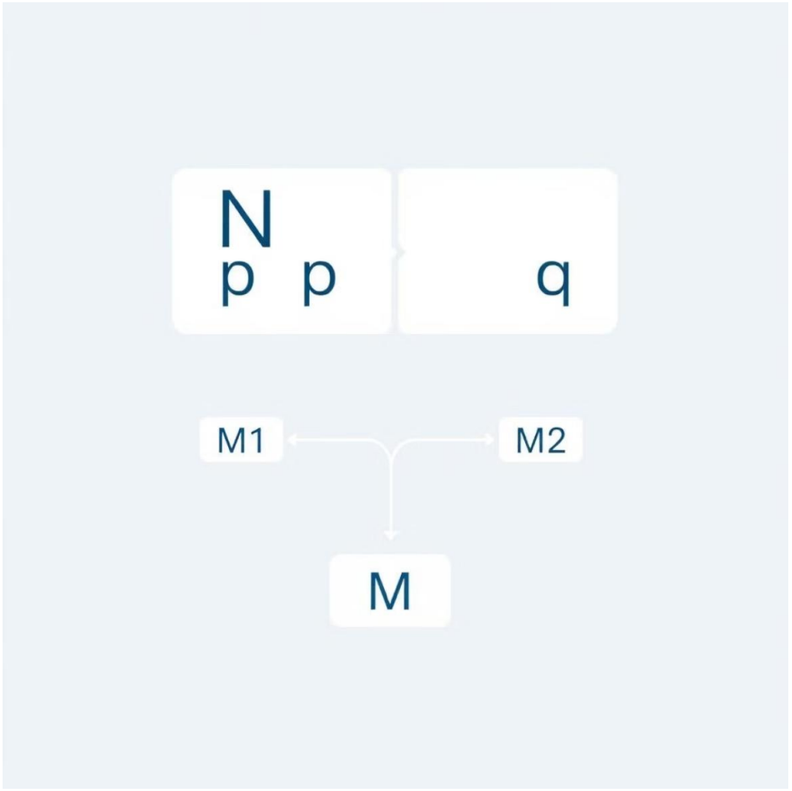
Егер $N=p \cdot q$ болса, есептеуді кіші модульдерге бөлуге болады:

- $d_1 = d \mod (p-1)$
- $d_2 = d \mod (q-1)$
- $M_1 = C^{d_1} \mod p$
- $M_2 = C^{d_2} \mod q$

Сосын Қытай қалдық теоремасы (CRT) арқылы M-ді қайта құрамыз.

Қорытынды:

CRT қолданғанда дешифрлау шамамен 4 есе жылдамдайды, бұл үлкен деректер көлемімен жұмыс істегенде маңызды.



Бұл схема CRT қолдану арқылы RSA дешифрлау процесінің қалай жеделдетілетінін көрсетеді.

CRT-тің практикалық тиімділігі

1

SRC (Single-Radix Conversion) формуласы:

$$M = M_1 \ (q^{-1} \mod p) \ q + M_2 \ (p^{-1} \mod q) \ p \mod N$$

Бұл стандартты түрлендіру әдісі, екі кері элементті есептеуді қажет етеді.

2

MRC (Mixed-Radix Conversion) формуласы:

$$M = M_1 + [(M_2 - M_1) \ (p^{-1} \mod q) \mod q] \ p$$

Артықшылығы – бір ғана кері элемент есептеледі, соңында модульдік қысқарту жеңілдейді. Бұл есептеуді оңтайландырады.

Жылдамдық туралы:

Төмендегі кестеде RSA-CRT жеделдетуінің нақты уақыттары көрсетілген, CRT қолданғанда дешифрлау уақыты кәдімгі RSA-ға қарағанда айтарлықтай аз.

Биік	RSA Шифрлау (мс)	RSA Дешифрлау (мс)	RSA-CRT Дешифрлау (мс)
96	1.2	3.5	0.9
88	0.9	2.8	0.7
64	0.5	1.5	0.4

Практикада қолданылуы:

Аппараттық криптомодульдерде, смарт-карталарда және аппараттық қауіпсіздік модульдерінде (HSM) CRT-нұсқасы жиі қолданылады, өйткені ол өнімділікті арттырады.

Эль-Гамаль

Негізі:

1985 ж. ұсынылған. Қауіпсіздігі дискретті логарифм есебінің қиындығына негізделген. Хабарды шифрлауға да, цифрлық қолтаңба жасауға да қолданылады.

Жұмыс принципі:

Параметрлер анықталып, құпия және ашық кілттер генерацияланады. Шифрлау үшін кездейсоқ k таңдалып, (a, b) шифрмәтіні жасалады. Дешифрлау үшін M бастапқы хабар қалпына келтіріледі.

Ерекшеліктері:

Әр шифрлау үшін жаңа k таңдалады, бұл бірдей хабардың әр жолы басқа шифрмәтін беруін қамтамасыз етеді. Хабардың өлшемі екі еселенеді (M орнына (a, b)).

Шифрлау және Дешифрлау Формулалары:

Параметрлер: p – үлкен жай сан; g – $\mathbb{Z}_p^\ast$ тобының генераторы.

Құпия кілт: x ($1 < x < p-1$).

Ашық кілт: $y = g^x \bmod p$.

Шифрлау: $a = g^k \bmod p$, $b = y^k \cdot M \bmod p$.

Дешифрлау: $M = b \cdot a^{-x} \bmod p$.

Месси–Омура протоколы

Месси–Омура протоколы «Төрт көз» шифры ретінде белгілі, бұл хабарды толық ашу үшін екі жақтың да қатысуын талап етеді.

0

0

1. А жіберуші:

***C_1 = M^{e_A} \mod p* есептеп, В-ға жібереді. Бұл қадамда хабар А-ның құпия кілтімен шифрланады.**

2. В қабылдаушы:

***C_2 = C_1^{e_B} \mod p* есептеп, А-ға қайтарады. Енді хабар екі құпия кілтпен шифрланған.**

0

0

3. А:

***C_3 = C_2^{d_A} \mod p* есептеп, В-ға қайта жібереді. А өзінің шифрлауын алып тастайды.**

4. В:

***M = C_3^{d_B} \mod p* есептеп, бастапқы хабарды алады. В өзінің шифрлауын алып тастап, хабарды оқиды.**

Артықшылықтары:

Екі жақтың да құпия кілттері бөлек, бұл қауіпсіздікті арттырады.

- **Бір адамның кілті белгілі болса да, екіншісіз толық ашу мүмкін емес.**

Сенімділік деңгейі жоғары, өйткені ешбір тарап хабарды жалғыз өзі дешифрлай алмайды.

Полига–Хеллман алгоритмі

Жалпы сипаттамасы:

Полига–Хеллман алгоритмі RSA-ға ұқсас, бірақ ол ашық кілтті жүйе емес.

Формулалар:

Шифрлау: $C = M^e \mod n$

Дешифрлау: $M = C^d \mod n$

Мұндағы $e \cdot d \equiv 1 \mod \varphi(n)$

Ерекшеліктері:

n – жай сандардың көбейтіндісі емес (RSA-дан айырмашылығы).

$\varphi(n)$ мәні құпия саналады, бұл алгоритмнің қауіпсіздігін арттырады.

Қауіпсіздігі – n модулі бойынша дискретті логарифм есебінің қиындығына негізделген.

- АҚШ және Канадада патенттелген, бұл оның тарихи және коммерциялық маңыздылығын көрсетеді.

Қысқа қорытынды:

Теориялық жағынан RSA-ға ұқсас болғанымен, Полига–Хеллман алгоритмін кілттерді жариялап қолдануға келмейді, бұл оны тек белгілі бір жағдайларда қолдануды шектейді.

Аралас (гибрид) шифрлау әдісі

Аралас шифрлау әдісі симметриялық және асимметриялық алгоритмдердің артықшылықтарын біріктіреді, бұл деректерді тиімді және қауіпсіз шифрлауға мүмкіндік

1

1. Хабарламаны симметриялық шифрлау

Хабарламаның өзі симметриялық алгоритммен (мысалы, AES) шифрланады.

Бұл үшін кездейсоқ K сессиялық кілті қолданылады.

2

2. Сессиялық кілтті асимметриялық шифрлау

Сессиялық кілт асимметриялық алгоритммен (мысалы, RSA) шифрланады.

Қабылдаушының ашық кілтімен K шифрланып, хабарға қосылып жіберіледі.

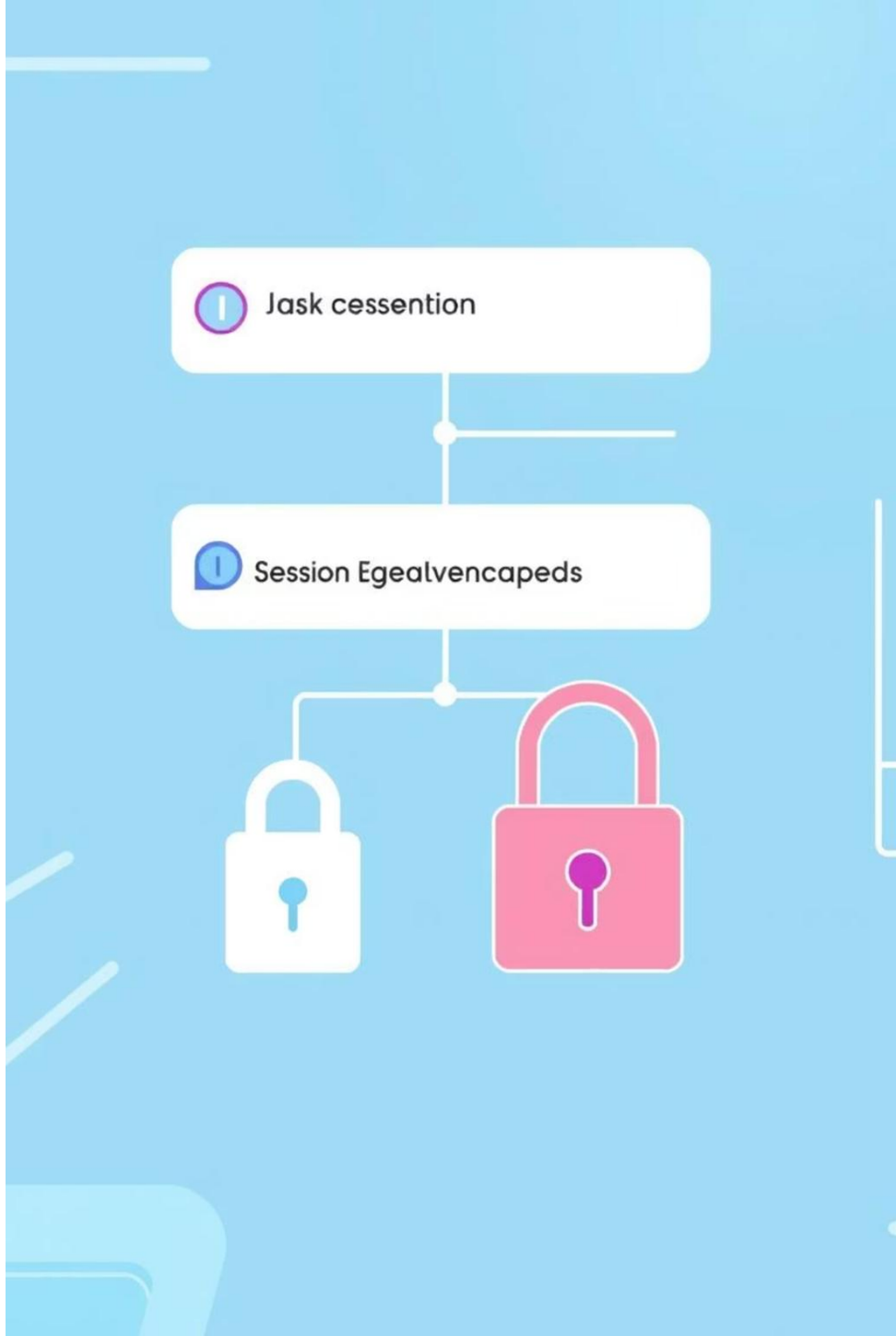
Артықшылықтары:

Жылдамдық: деректердің негізгі көлемі симметриялық әдіспен жылдам шифрланады.

Қауіпсіздік: сессиялық кілт асимметриялық шифрлау арқылы қауіпсіз тасымалданады.

Масштабталу: әр сеансқа жаңа кездейсоқ кілт қолданылады.

Икемділік: әртүрлі симметриялық және асимметриялық алгоритмдерді біріктіруге болады.



Бақылау сұрақтары және пайдаланылған әдебиеттер

Бақылау сұрақтары:

1. Қытай қалдық теоремасы RSA дешифрлауды неліктен жеделдетеді?

Эль-Гамаль жүйесіндегі a және b компоненттерінің рөлі қандай?

3. Месси–Омура протоколы қалай жұмыс істейді және оның негізгі ерекшелігі неде?
4. Полига–Хеллман алгоритмін неге ашық кілтті жүйе деп санауға болмайды?
5. Аралас шифрлау әдісінің негізгі артықшылықтарын
6. Кітаңызындығының уақыт бойынша өзгеру себептерін түсіндіріңіз.

Пайдаланылған әдебиеттер:

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.
Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson.
Paar, C., & Pelzl, J. (2010). *Understanding Cryptography*. Springer.
Адамбеков, А. (2020). Ашық кілтті криптожүйелер және симметриялық криптографиялық алгоритмдер. *Криптография және ақпараттық қауіпсіздік журналы*.