№12 Лекция тақырыбы: Ашық кілтті криптожүйелердің концепциясы. DES (Data Encryption Standard). AES(Advanced Encryption Standard)

Лекцияның оқыту нәтижелері: Криптографиялық жүйелердің жалпы принциптерін және олардың ақпараттық қауіпсіздіктегі рөлін түсіндіру. DES алгоритмінің құрылымын, жұмыс кезеңдерін және шектеулерін сипаттау. AES алгоритмінің негізгі операцияларын және оның DES-тен артықшылығын түсіндіру.

Лекция мазмұны:

1. Ашық кілтті криптожүйелер концепциясы
2. DES және AES шифрлау әдістері

Қазіргі заманда ақпаратты қорғау өте маңызды мәселе болып отыр. Интернет пен басқа да коммуникациялық технологиялардың дамуы адамдар арасындағы ақпарат алмасуды жеңілдетті, бірақ оның қауіпсіздігі де сол деңгейде қиындай түсті. Әсіресе банк жүйелері, мемлекеттік мекемелер және жеке адамдардың мәліметтері осы қауіптің астында қалып отыр. Сондықтан ақпаратты қорғау мен оның құпиялылығын сақтау үшін **криптография** қолданылады.

Криптография - ақпаратты шифрлау және оны қолжетімсіз етудің ғылыми әдістері мен тәсілдері туралы ғылым. Ол ақпаратты тек арнайы кілт арқылы ғана оқуға мүмкіндік беретін жүйені жасайды. Криптографияның негізгі мақсаты – мәліметтердің қауіпсіздігін, олардың тұтастығын және түпнұсқалылығын сақтау.

Криптографиялық жүйелердің екі негізгі түрі бар: **симметриялық шифрлау жүйелері** және **асимметриялық шифрлау жүйелері**. Симметриялық жүйеде бір кілт шифрлау және дешифрлау үшін қолданылады, ал асимметриялық жүйеде екі түрлі кілт пайдаланылады – біреуі ашық, екіншісі жабық. Осы рефератта **ашық кілтті криптографияның концепциясы**, сондай-ақ **DES** (Data Encryption Standard) және **AES** (Advanced Encryption Standard) симметриялық шифрлау жүйелері талданады. Бұл әдістер ақпаратты қорғаудың негізгі құралдары болып саналады және олардың әрқайсысының өзіндік артықшылықтары мен кемшіліктері бар.

2 ***Ашық кілтті криптожүйелердің жалпы сипаттамасы***

Ашық кілтті криптожүйелер симметриялық криптографиядан ерекшеленеді. Егер симметриялық криптожүйеде бірдей кілт шифрлау және шифрды ашу үшін қолданылса, ашық кілтті криптожүйелерде екі түрлі кілт пайдаланылады:

- Ашық кілт (public key): Бұл кілт көпшілікке жарияланады және хабарламаны шифрлау үшін қолданылады.
- Жабық кілт (private key): Бұл кілт тек қабылдаушыда сақталады және шифрды ашу үшін пайдаланылады.

Ашық кілтті криптожүйелердің негізі – кері қайтарылмайтын математикалық функциялар және оларды кері есептеу қиынға соғатын есептер,

мысалы, үлкен сандарды жай көбейткіштерге жіктеу немесе дискреттік логарифм есебі. Ашық кілтті жүйелерде кілттерді қауіпсіз тарату мәселесі шешілген, бұл оны заманауи ақпараттық жүйелерде кеңінен қолдануға мүмкіндік береді.

RSA криптожүйесінің пайда болуы және оның ерекшеліктері

RSA криптожүйесі 1977 жылы Рональд Ривест, Ади Шамир және Леонард Адлеман ұсынған алгоритм. RSA атауы авторлардың есімдерінің алғашқы әріптерінен құралған. Бұл алгоритм үлкен сандарды жай көбейткіштерге жіктеу мәселесінің күрделілігіне негізделген. RSA криптожүйесі ақпаратты қорғауда, электрондық қолтаңба жасауда және сандық сертификаттар шығаруда кеңінен қолданылады.

RSA-ның ерекшеліктері:

1. Ашық және жабық кілттерді қолдануы.
2. Үлкен сандарды пайдалану арқылы қауіпсіздікті қамтамасыз ету.
3. Математикалық есептеулердің күрделілігі шабуылдарға төтеп береді.

RSA алгоритмінің жұмыс принципі

RSA алгоритмі бірнеше негізгі кезеңдерден тұрады:

1. Жәй сандарды таңдау:

Екі үлкен жәй сан ppp және qqq таңдалады. Жәй сандардың үлкен болуы қауіпсіздікті арттырады.

2. Модульді есептеу:

$$n=p\times qn = p \times qn=p×q$$

Бұл nnn шифрлау және шифрды ашу үшін қолданылады.

3. Эйлер функциясын есептеу:

$$\phi(n)=(p-1)(q-1)\phi(n) = (p-1)(q-1)ϕ(n)=(p−1)(q−1)$$

4. Ашық кілтті таңдау:

$$1<e<\phi(n)1 < e < \phi(n)1<e<ϕ(n)$$

eee және ϕ(n)\phi(n)ϕ(n) өзара жәй сандар болуы керек.

5. Жабық кілтті есептеу:

ddd жабық кілтін есептейміз, мұнда:

$$d\times e\equiv 1\mod \phi(n)d \times e \equiv 1 \mod \phi(n)d×e≡1modϕ(n)$$

6. Ашық және жабық кілттерді қалыптастыру:

Ашық кілт: (e,n)(e, n)(e,n), жабық кілт: ddd.

Шифрлау және шифрды ашу

RSA криптожүйесін қолдану барысында шифрлау мен шифрды ашу келесі формулалар арқылы жүзеге асырылады:

- Шифрлау:

Хабарламаны MMM шифрланған мәтінге CCC түрлендіру:

$$C=M^e\mod nC = M^e \mod nC=Memodn$$

- Шифрды ашу:

Шифрланған мәтін CCC-ны бастапқы хабарламаға MMM-ға түрлендіру:

$$M=C^d\mod nM = C^d \mod nM=Cdmodn$$

Мұндағы MMM – бастапқы хабарлама, CCC – шифрланған мәтін, eee – ашық кілттің көрсеткіші, ddd – жабық кілттің көрсеткіші, nnn – модуль.

RSA алгоритмін қолдану мысалы

1. Жәй сандарды таңдау:

p=61p = 61p=61, q=53q = 53q=53.

n=61×53=3233n = 61 \times 53 = 3233n=61×53=3233.

ϕ(n)=(61−1)(53−1)=3120\phi(n) = (61-1)(53-1) = 3120ϕ(n)=(61−1)(53−1)=3120.

2. Ашық кілтті таңдау:

e=17e = 17e=17 (өзара прост).

3. Жабық кілтті есептеу:

d×17≡1mod 3120d \times 17 \equiv 1 \mod 3120d×17≡1mod3120. Бұл жағдайда d=2753d = 2753d=2753.

4. Ашық және жабық кілттер:

Ашық кілт: (17,3233)(17, 3233)(17,3233), жабық кілт: 275327532753.

5. Хабарламаны шифрлау:

M=65M = 65M=65.

C=6517mod 3233=2790C = 65^{17} \mod 3233 = 2790C=6517mod3233=2790.

6. Шифрды ашу:

M=27902753mod 3233=65M = 2790^{2753} \mod 3233 = 65M=27902753mod3233=65.

RSA-ның қолданылу салалары

RSA криптожүйесі келесі салаларда кеңінен қолданылады:

1. Электрондық қолтаңба: Құжаттардың түпнұсқалығын растау үшін.

2. Сандық сертификаттар: Онлайн транзакциялардың қауіпсіздігін қамтамасыз ету үшін.

3. Деректерді шифрлау: Интернет арқылы құпия ақпаратты жіберу үшін.

RSA-ның артықшылықтары мен кемшіліктері

Артықшылықтары:

- Ашық кілтті жүйе болғандықтан, кілттерді қауіпсіз тарату мәселесі шешілген.
- Үлкен сандарды қолдану арқылы шабуылдарға төзімді.
- Электрондық қолтаңба жасау мүмкіндігі бар.

Кемшіліктері:

- Есептеу процесі күрделі, үлкен ресурстарды қажет етеді.
- Үлкен деректерді өңдеуде баяу жұмыс істейді.

Кванттық компьютерлер пайда болған жағдайда қауіпсіздігі әлсіреуі мүмкін.

Оқытудың техникалық құралдары: Компьютер немесе ноутбук, интерактивті тақта. Криптографиялық бағдарламалар немесе эмуляторлар (мысалы, CrypTool, OpenSSL, Python скрипттері) – DES және AES алгоритмдерінің жұмысын тәжірибе жүзінде көрсету.

Лекция оқудың тәртібі, оқыту әдістері мен түрлері:

Оқудың тәртібі:

- Лекция түрінде түсіндіру және мысалдар арқылы көрсету

- Шифрлау тәсілдерін кезең-кезеңмен талдау және тәжірибе жүзінде орындау
- Қорытынды сұрақтар мен талқылау

Оқыту әдістері мен түрлері:
- Түсіндірмелі-баяндамалық әдіс
- Көрнекілік және демонстрациялық әдіс
- Практикалық тапсырмалар орындау
- Интерактивті сұрақ-жауап және топтық талқылау

БӨЖ және ОБӨЖ тапсырмалары,олардың түрлері мен орындалуына қойылатын ұпайлардың үлестері:

БӨЖ: Ашық кілтті криптожүйелер: DES, AES, RSA арқылы шифрлау мысалдарын орындау, берілген мәтінді шифрлап және дешифрлап орындауы қажет. Бұл жұмыс жалпы бағалаудың 60-баллын құрайды.

БӨЖ бағалау критерийлері:
- Теориялық материалды түсіну және қолдану -20 балл
- Бағдарламаны дұрыс жазу немесе есепті шешу -25 балл
- Нәтижелердің дәлдігі мен түсіндіру сапасы -15 балл

Барлығы: 60 балл

ОБӨЖ: Ашық кілтті криптожүйелер: DES, AES, RSA арқылы шифрлау алгоритмін қолданып мәтінді шифрлау және әдістердің айырмашылығын талдау бойынша қысқаша есеп дайындау. Бұл жұмыс жалпы бағалаудың 40-баллын құрайды.

ОБӨЖ бағалау критерийлері:
- Тапсырманың толық және уақытылы орындалуы -15 балл
- Теориялық және практикалық түсіндіру сапасы -15 балл
- Топтық жұмысқа белсенді қатысу, сұрақтарға жауап беру-10 балл

Барлығы: 40 балл

Жалпы бағалау үлесі:
- **БӨЖ — 60% (60 балл)**
- **ОБӨЖ — 40% (40 балл)**

Пайдалынатын әдебиеттер тізімі:

Негізгі:

1. Г. Камалова, А. Х. Касымова, Л. Б. Диярова. «Ақпараттық қауіпсіздікті басқару». Оқу құралы. /- Алматы: Альманахъ, 2020. - 128 с.

2. Дүйсебекова, К. С. Ақпараттық қауіпсіздік және ақпараттарды қорғау. Оқу құралы /- Алматы: Қазақ университеті, 2013. - 156 с.

3. Нечаев В.И. Элементы криптографии основы теории защиты информации. / В. И. Нечаев. - М.: Высшая школа, 1999. - 109 с.

4. Г. А. Тюлепбердинова. Бағдарламалау технологиясы. Оқу-әдістемелік кешен. - Алматы: Альманахъ, 2021. - 148 с.

5. Дүйсебекова, К.С. Ақпараттық қауіпсіздік және ақпараттарды қорғау: Оқу құралы. . - Стер. бас - Алматы: Қазақ университеті, 2020. - 156 б. http://rmebrk.kz

6. Камалова Г.А., Диярова, Л.Б. Ақпараттық қауіпсіздік және ақпаратты қорғау : Оқу құралы. / Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университеті. - Алматы: Альманах, 2020. - 116б. http://rmebrk.kz

Қосымша әдебиеттер:

1. Ахметова, С. Бағдарламалау технологиясы : Лекция жинағы. / ЮКГУ им. М.О. Ауезова. - Шымкент: ОҚМУ, 2007. - 51 б. https://rmebrk.kz/book/50006

2. Ж.З. Сатмаганбетова. Бағдарламалау тілдері және технологиясы: Оқу-әдістемелік куралы. / Қостанай: А. Байтурсынов атындағы ҚМУ, 2014. - 64 б. http://rmebrk.kz