№15 Лекция тақырыбы: Электронды цифрлы қолтаңба алгоритмінің архитектурасы. Кілттерді генерациялау. Хэш-функциялары

Лекцияның оқыту нәтижелері: Электронды цифрлы қолтаңба алгоритмінің архитектурасын сипаттай алады. Құпиялы және ашық кілттердің генерациялау принциптерін түсінеді. Хэш-функциялардың рөлі мен қасиеттерін ажыратады.

Лекция мазмұны:

1. ЭЦҚ алгоритмінің архитектурасы

Электронды цифрлы қолтаңба алгоритмінің архитектурасы

Маңызды құжатқа қойылған қолтаңбадан зиян шегу мүмкіндігін болдырмау үшін, қолтаңба қояр алдында нақты байқаулар жүргізу керек. Хаттаманы іске асыру жағдайында қолтаңба қоюшының құпиялы кілті, көшіруден қорғалған оның жеке дискетінде сақталады. Бірақ бұл жеткіліксіз болады, себебі дискетті ұрлап кетуі немесе жоғалтып алуы да мүмкін. Демек, құпиялы ақпаратты (кілтті) бөгде басқа адамдардың пайдалануларынан қорғау керек. Бұл проблеманы шешу үшін парольды қорғауды қолдану керек. Парольмен тек ЭЦҚ қою және кілт генерациялау жұмыстарын ғана емес, сонымен бірге желідегі қолданушылардың ашық кілттер каталогын өзгертетін және басқа да жұмыстарды жауып тастауға болады.

Жүйеде «криптовирустар» жоқ екендігін тексеру қажет. Мысалы, қолтаңба қою кезінде криптовирустар құпиялы кілтті ұстап алуы мүмкін (оны қажетті жерге көшіреді). Сонымен бірге қолтаңбаны тексеру кезінде олар қолтаңба дұрыс болмаса да жүйеге оны дұрыс деп «айтқызуы» мүмкін. Кейбір криптовирустар жүйеге кілт генерациялау кезінде бір рет ғана түсіп, жүйеге әлсіз кілттер генерациялауға «көмектесуі» мүмкін. Мысалы, егер кілттер, енгізілген таймерді қолданатын кездейсоқ сандар датчигі негізінде генерацияланатын болса, онда вирус таймер көрсеткіштерін өзгерте алады, одан соң «статус-квоны» қалпына келтіреді. Нәтижесінде бұл кілттер қарсыластармен оңай ашылуы мүмкін. Мұндай криптовирустардан тек бір ғана қорғаныс бар – таза жүйелік дискетіні және таза бағдарламаны қолдану.

Қолтаңбаны қою және тексеру

ЭЦҚ-ны нақты бір құжатқа қою үшін, үлкен көлемді есептеу жұмысын жасау керек. Бұл есептеулер екі бөлікке бөлінеді: кілттерді генерациялау және құжатқа қолтаңба қою.

Кілттерді генерациялау

Бұл сатыда әрбір қолданушыда екі кілт генерацияланады: құпиялы d және ашық e. Құпиялы кілт қолданушымен жасырын сақталады. Ол қолтаңбаны қалыптастыру үшін қолданылады. Ашық кілт құпиялы кілтпен байланысты, яғни $ed \equiv 1 (\mathrm{mod}\ \varphi(n))$. Ашық кілт желідегі басқа барлық қолданушыларға белгілі және қолтаңбаны тексеруге арналған. Оны

қолтаңбаның иесін (авторын) және электронды құжаттың дұрыстығын анықтауға мүмкіндік беретін, бірақ құпиялы кілтті есептеп шығаруға мүмкіндік бермейтін керекті құрал ретінде қарастыру керек.

Бұл этапты жүргізудің екі жағдайы бар. Қолданушының өзі кілттерді генерациялай алатын жағдайы тиімді болады. Бірақ белгілі бір жағдайларда бұл жұмысты құпиялы кілттерді әрбір қолданушыға генерациялап оларды тиімді таратумен айналысатын орталыққа берген орынды болады. Екінші варианттың көптеген әкімшілік артықшылықтары бар, бірақ кемшілігі де жоқ емес - қолданушыда оның жеке құпиялы кілті құпиялы екендігіне кепілдігі жоқ. Басқа сөзбен айтқанда барлық қолданушылар орталық «бөркінің астында» болады және орталық кез келген қолтаңбаны жасап алуы мүмкін.

Маңызды құжаттарға қол қою кезінде ақпараттың қауіпсіздігін қамтамасыз ету үшін қолтаңба қою процесінде нақты тексеру мен қорғау шаралары жүргізіледі.

Қолтаңба қоюшының құпия кілті көшіруден қорғалған жеке тасымалдағышта (мысалы, дискетте, токенде) сақталады.

Бірақ бұл да жеткіліксіз — себебі физикалық ұрлау немесе жоғалту қаупі бар. Сондықтан жүйеде **парольдік қорғау** мен **аутентификация** әдістері қолданылады.

Жүйенің қауіпсіздігін сақтау үшін:

- Криптовирустардың бар-жоғын тексеру қажет;
- Қолтаңба қою кезінде жүйе таза дискеттер мен сенімді бағдарламалар арқылы орындалуы керек;
- Кілттерді генерациялау және қол қою кезеңінде сыртқы зиянды бағдарламалардың қатысуы болмауы тиіс.

Криптовирустар кейде кілттерді ұрлап, әлсіз кілттер генерациялауға себеп болуы мүмкін. Сондықтан таза және тексерілген жүйелерді пайдалану – басты талап.

2. Қолтаңбаны қою және тексеру процесі

ЭЦҚ қою үшін үлкен көлемдегі есептеу амалдары орындалады. Бұл процесс екі негізгі кезеңнен тұрады:

- **Кілттерді генерациялау**
- **Құжатқа қолтаңба қою**

3. Кілттерді генерациялау

Әрбір пайдаланушы екі түрлі кілтке ие болады:

- **Құпиялы кілт (d)** – қолтаңба қою үшін қолданылады және тек қолданушыда сақталады;
- **Ашық кілт (e)** – жалпы қолжетімді және құжаттың дұрыстығын тексеруге арналған.

Ашық кілт арқылы қолтаңба иесі мен құжаттың түпнұсқалылығы анықталады, бірақ ол арқылы құпия кілтті қалпына келтіру мүмкін емес.

Кілттерді генерациялау әдістері:

1. **Жеке генерация** – қолданушы өз кілттерін өзі жасайды.

2. **Орталық генерация** – кілттерді арнайы уәкілетті орган (тіркеу орталығы) құрастырып, таратады.

Екінші тәсіл әкімшілік тұрғыда ыңғайлы болғанымен, қауіпсіздік тұрғысынан әлсіздік тудырады (қолтаңба орталық арқылы бұзылуы мүмкін).

4. Хэш-функциялары

Хэш-функция – хабарламаны қысқартып, тұрақты ұзындықтағы бірегей мән (хэш) алуға арналған математикалық түрлендіру.

Хэш-функцияның қасиеттері:

- Мәтіннің кез келген өзгерісіне сезімтал;
- Хэш мәнінен бастапқы хабарламаны қалпына келтіру мүмкін емес;
- Екі түрлі хабарламаның бірдей хэш мәнге ие болуы ықтималдығы аз.

Хэш-функция қолданысы:

1. Құжаттың тұтастығын тексеру.
2. ЭЦҚ жасау үшін бастапқы деректерді дайындау.
3. Қолтаңбаның қысқаша бейнесін алу.

ЭЦҚ хэш-функция көмегімен қысқартылған мәтінге қол қойылады. Хэш мәні құжатпен бірге сақталады немесе бөлек файлда тұрады.

Кең таралған хэш-функциялар:

- **MD (Message Digest)** алгоритмдері — Р. Л. Ривест жасаған, 128-биттік хэш бейнесін есептейді.
- **SHA (Secure Hash Algorithm)** — жоғары сенімділік пен қауіпсіздік деңгейін қамтамасыз етеді.

Оқытудың техникалық құралдары: Компьютер, ноутбук, интернет.

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: Электронды цифрлы қолтаңба алгоритмінің архитектурасы мен кілттерді генерациялау. Хеш-функцияларын орындауы қажет. Бұл жұмыс жалпы бағалаудың 60-баллды 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: Электронды цифрлы қолтаңба алгоритмінің архитектурасы мен кілттерді генерациялау. Хеш-функцияларын орындап, талдау бойынша қысқаша есеп дайындау. Бұл жұмыс жалпы бағалаудың 40-баллды 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. Кауфман Ч., Перлман Р., Спеснер М. *Network Security: Private Communication in a Public World.* – Prentice Hall, 2016.

3. Schneier B. *Applied Cryptography.* – Wiley, 2015.

4. Stallings W. *Cryptography and Network Security: Principles and Practice.* – Pearson, 2022.Таненбаум Э. Компьютерлік желілер. – Алматы: Эверо, 2019

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

Қосымша:

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