**№ 13 Лекция тақырыбы:** Ашық кілтті криптожүйелер. Ақпараттарды RSA криптожүйесін қолданып шифрлау және шифрларды ашу

**Лекцияның оқыту нәтижелері:** Ашық және жабық кілттерді, ассимметриялық криптография ұғымдарын түсінеді. RSA алгоритмінің математикалық негізін (тұрақты және модульдік арифметика, Эвклид алгоритмі) түсінеді. RSA үшін кілттерді генерациялау, хабарды шифрлау және шифрды ашу қадамдарын қолданып көрсете алады.

**Лекция мазмұны:**

1. Ашық кілтті криптожүйелер.
2. Ақпараттарды RSA криптожүйесін қолданып шифрлау және шифрларды ашу
3. Брандмауерлер.

**Желіде компьютерлік ақпаратты қорғау**

Компьютер желілерінің тез дамуы, ақпарат іздеудің жаңа технологияларының пайда болуы әртүрлі адамдар және мекемелердің интернет желісіне болған қызығушылығын арттырып отыр. Глобальды желіні коммерциялық мақсаттарда және құпия ақпараттарды өңдеуде қолдану тиімді ақпарат қорғау жүйесін құруды талап етеді. Локальды және корпоративті желіні интернет жүйесіне қосар кезде ол желінің ақпараттық қауіпсіздігін қамтамасыз етуіміз қажет.

Интернет глобальды жүйесі ашық жүйе ретінде құрылған. Сондықтан, интернет жүйесі әртүрлі деңгейдегі ақпарат қауіпсіздігін бұзушыларға көп мүмкіндіктерді береді.

Интернет желісі арқылы ақпарат бұзушысы мынадай іс-әрекеттерді орындай алады: мекеме ішкі желісіне еніп конфиденцияльды ақпараттарды, серверлер адрестерін, парольдерін, олардың мазмұнын көшіріп алуы мүмкін. Осы алынған ақпараттар арқылы мекеме бәсекелестігіне өте үлкен зиян келуі және клиенттер сенімін жоғалтуы мүмкін.

**Брандмауерлер**

Компьютерлік емес салада брандмауер (немесе firewall) деп – жанбайтын материалдардан дайындалған қабырғаға айтылады. Ал компьютерлік саладағы брандмауер деп – ақпарат қауіпсіздігін бұзушылардың ішкі желіге еніп, компьютерлердегі ақпаратттарды көшіру, өзгерту немесе жоюға қарсы тұратын бөгеттерге айтылады. Брандмауерлер сыртқы желіге қауіпсіз шығуды қамтамасыз етіп, ішкі желідегі қолданушылардың енуіне шектеу қояды және сыртқы желіден рұқсат етілмеген бағдарламалардың енуіне шектеу қояды. Ол бірнеше компоненттерден (мысалы, брандмауердің бағдарламашы жұмыс істейтін маршрутизатор немесе шлюз) тұратын қорғау бөгеттері болып табылады. Брандмауер ішкі желіге рұқсатты қауіпсіздік саясаты бойынша береді.

Барлық енетін және шығатын пакеттер брандмауер арқылы өтеді және ол тек авторазацияланған пакеттерді ғана өткізеді. Бірақ, ешқандай да брандмауер 100% қауіпсіздікті қамтамасыз ете алмайды. Көптеген

коммерциялық мекемелер үшін брандмауерді орнату ішкі желінің қауіпсіздігі үшін қажетті болып саналады.

Интернетте әртүрлі компьютерлер арасында байланыс орнатуды қамтамасыз ететін протокол TCP/IP протоколы. TCP/IP пакеттерді маршрутизациялауға мүмкіндік бергендіктен ол желіаралық протокол ретінде қолданылады. TCP/IP пакет тақырыптарындағы мәліметтер крекерлер тарабынан жиі шабуылданады.


**Интернет қызметтерінің кемшіліктері**

SMTP - (Simple Mail Transfer Protocol) протоколы интернетте почта тасмалдау қызметін атқарады. Бұл протоколды қолдану проблемаларының бірі почтаны қабылдаушы почта жіберішінің адресін тексере алмайды. Хакер ішкі желіге өте көп почталық хабарлар жіберіп, сервер жұмысын істен шығаруы мүмкін.

Интернетте кең тараған Send-Mail электеронды бағдарламасы өзінің жұмысында ақпарат жіберушінің IP адресін қолданады. Крекер Send-Mail арқылы жіберіліп жатқан хабарларды алып, адрестерді ауыстыру арқылы шабуылға шығуы мүмкін.

FTP - (File Transfer Protocol) файлдарды жіберу протоколы. Текстік және екілік файлдарды жіберуде қолданылады. FTP-серверлерде құжаттар, бағдарламалар, графика және тағы басқа ақпараттар сақталады.

DNS – (Domain Name Server) желідегі аттар қызметі. DNS-те желі туралы мәліметтер мысалы, әрбір IP-адресі бар компьютерлер саны туралы мәліметтер болады. DNS проблемаларының бірі бұл базаны бөгде қолданушылардан жасыру өте қиын. Нәтижеде DNS арқылы локальды желідегі компьютерлер саны және олардың аттарын біліп алады.

TELNET (алыс терминалды эмуляциялау қызметтері) алыс желілерге қосылу үшін қолданылады. Бұл қызметті қолдану үшін қолданушылар тіркеліп, парольдерін ендірулері керек. Алыс терминалдан тұрып қолданушы файл және бағдарламалармен жұмыс істеуі мүмкін. TELNET жүйесіне қосылып, бағдарлама қолданушыларының барлығының аттары және парольдері жазылып алынуы мүмкін.

WWW (World Wide Web) – интернетте әртүрлі серверлердің мазмұнымен танысуға мүмкіндік беретін жүйе. WWW-тің ең маңызды қасиетінің бірі бұл гиперсілтемелерді қолданады. Бірақ, мұның ең әлсіз жері де сол гиперсілтемені қолдану. Өйткені гиперсілтемеде бір беттен екінші бетке қалай өтетіндігі туралы мәліметтер бар. Крекерлер осы мәліметтерді біліп алып, жүйені бұзу мүмкін.

**Желілік қауіпсіздік саясаты**

Желілік қауіпсіздік саясаты екі бөліктен тұрады:

1. Желілік қызметтерге рұқсат алу саясаты;
2. Брандмауерлердің қолдану саясаты.

Желілік қызметтерге рұқсат алу саясатына сәйкес интернеттегі кейбір қызметтерді пайдалануға және интернетке қосылу жолдарына шектеу қойылған.

Мысалы, SLIP (Serial Line Internet Protocol) және PPP (Point to Point Protocol) интернетке шектеу қоятын (қосылу жолдарына) протоколдар. Интернеттегі пайдалануға тыйым салынған қызметтерді басқа жолмен пайдаланбауды көздейді. Желілік қызметтерге рұқсат алу саясаты келесі принциптердің біреуін пайдалана алады:

- интернеттен ішкі желіге рұқсатты болдырмау, ал ішкі желіден интернетке тығуға рұқсат жоқ;
- интернеттен ішкі желіге шектелген қызметтерге рұқсат беру, мысалы, почталық серверлерге.

Брандмауерлердің қолдану саясаты бойынша ішкі желі ресурстарына рұқсат алу әдістері анықталады. Ең алдымен қорғау жүйесі қаншалықты сенімді екенін анықтап алу керек. Басқаша айтқанда ішкі ресурстарға рұқсат алу мына принциптердің біреуіне негізделген болуы керек:

-ашық түрде рұқсат берілмеген барлығына тыйым салу;

-ашық түрде тыйым салынбаған барлығына рұқсат.

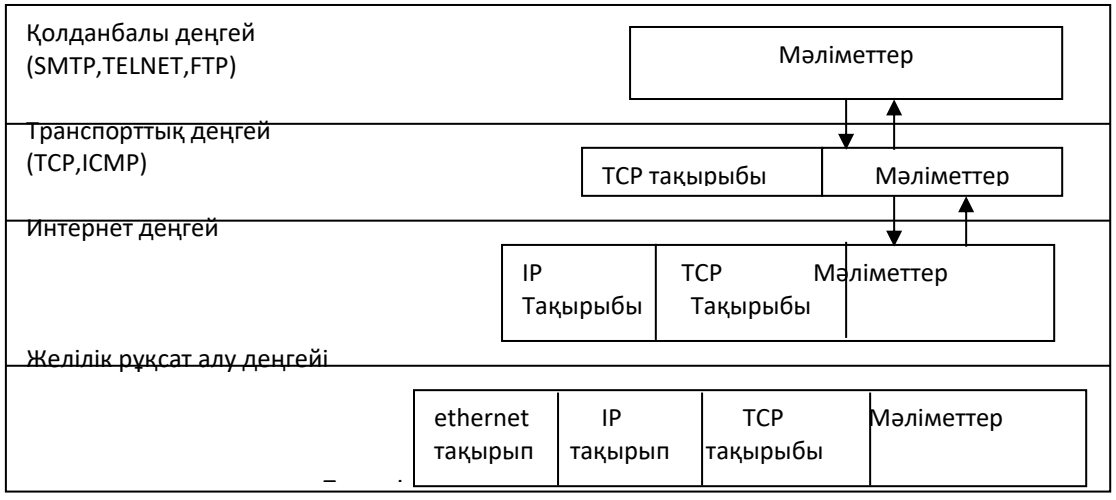
Брандмауерлердің бірінші принцип бойынша қолдану жоғары дәрежедегі қауіпсіздікті қамтамасыз етеді. Бірақ, бұл принципті қолдану қолданушыларға қиындықтар тудырып, орындалу қиынға түседі. Брандмауерлерді екінші принцип бойынша қолдану ыңғайлы және аз шығынды болғанымен ішкі желі қауіпсіздігі өз деңгейінде болмайды.

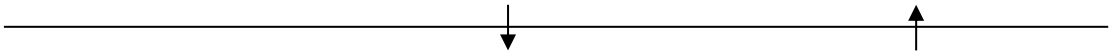
Брандмауерлердің компоненттері үш топқа бөлінеді:

1) Фильтрлеуші маршрутизаторлар;
2) Желілік деңгейдегі шлюздар;
3) Қолданбалы деңгейдегі шлюздар.

<u>Фильтрлеуші маршрутизаторлар</u>

Серверде орындалатын бағдарлама енуші және шығушы пакеттерді фильтрлеу пакеттердің IP-тақырыптарында орналасқан ақпарат бойынша орындалады.





Сурет 5- TCP/IP протоколына мәліметтерді жіберу және мәліметтерді қабылдау схемасы.

Фильтрлеуші маршрутизатор IP-пакеттерді пакет тақырыбындағы мына өрістердің мазмұны бойынша фильтрлеуі мүмкін:

1) жіберуші IP-адресі, яғни пакетті жіберген жүйе адресі;

2) қабылдаушы IP-адресі, яғни пакетті қабылдаушы адрес;

3) жіберуші порты, яғни жіберуші жүйесіндегі байланыс порты;

4) қабылдаушы порты.

Порт – клиент және сервер қолданатын бағдарламалық анықтама. Порт 16 биттік сан арқылы идентификацияланады. Фильтрлеу әртүрлі жолмен хост компьютерлер және порттармен байланыстарды болдырмау үшін қолданылуы мүмкін. Мысалы, сенімсіз деген компьютерлермен байланыстарды үзуге болады. Егер брандмауер TCP немесе UDP протоколымен байланысты болдырмайтын болса,онда брандмауер белгілі бір хост компьютерлермен байланысын өз қауіпсіздік саясаты бойынша жүргізуі мүмкін. Мысалы, ішкі желі белгілі бір жүйелерден басқа барлық жүйелерден енуші байланыстарды болдырмауы мүмкін.

Бұл жүйелер үшін кейбір қызметтер ғана рұқсат етілуі мүмкін ( SMTP – 1 жүйе үшін, TELNET және FTP басқа жүйе үшін). Фильтрлеуші маршрутизаторға мысал ретінде ішкі желімен 123.4.*.* адресі бойынша байланыс орнатушы қауіпсіздік саясатының орындалуын қарастырайық.

TELNET – байланыстар бір ғана 123.4.5.6 адресті хост компьютермен орнатылуы мүмкін.

SMTP – байланыстар 2 хост компьютермен 123.4.5.7 және 123.4.5.8 рұқсат етілген.

NNTP – (NetWork News Transfer Protocol) протоколы бойынша байланыс жаңалық сервері, адресі 129.6.48.254 болған сервер және ішкі желідегі 123.4.5.9 адресті компьютерге ғана рұқсат етілген.

Фильтрлеу әдістері

| Түрі | Жіберушінің адрес | Қабылдаушының Адрес | Жіберушінің порты | Қабылдаушының порты | Әрекет |
|---|---|---|---|---|---|
| TCP | * | 123.4.5.6 | >1023 | 23 | Рұқсат |
| TCP | * | 123.4.5.7 | >1023 | 25 | Рұқсат |
| TCP | * | 123.4.5.8 | >1023 | 25 | Рұқсат |
| TCP | 129.6.48.254 | 123.4.5.9 | >1023 | 119 | Рұқсат |
| UDP | * | 123.4.*.* | >1023 | >123 | Рұқсат |
| * | * | * | * | * | Рұқсат жоқ |

1-ші әдіс бойынша порт номері >1023 болған барлық инетернеттегі компьютерлерден пакеттерді 123.4.5.6 компьютерінің алуына рұқсат.

2-ші, 3-ші әдістер бойынша адрестері 123.4.5.7 және 123.4.5.8 компьютерлеріне SMTP пакеттерін 25-ші порт арқылы қабылдауға рұқсат.

4-ші әдіс бойынша 129.6.48.254 компьютерден 123.4.5.9 компьютерге пакеттерді қабылдауға рұқсат.

5-ші әдіс бойынша UDP протоколы бойынша байланысқа рұқсат бар.

6-шы басқа барлық әдістерге рұқсат жоқ.

Пакеттерді фильтрлеу әдістерінің құрылуы өте күрделі. Фильтрленген пакеттерді тестілеу құралдары жоқ. Кейбір фильтрлеуші маршрутизаторлардың протоколдау құралдары жоқ. Сондықтан, қауіпті пакеттер маршрутизатордан өтіп кетсе, олар өздерін танытқанға дейін танып-білуге болмайды.

Егер желі администраторы фильтрлеудің тиімді әдістерін қолдансада оның мүмкіндіктері шектеулі болып қала береді. Мысалы, администратор белгісіз болған адрестерден келуші пакеттерді ішкі желіге енуіне рұқсат бермейтін әдісті қолданады. Бірақ, хакерлер пакеттерді жіберу кезінде сенімді (авторизацияланған) клиенттердің адрестерін қолдануы мүмкін. Бұл жағдайда фильтрлеуші маршрутизатор жалған пакетті ажырата алмай өткізіп жіберуі мүмкін. Шабуылдың бұл түрі адрестерді өзгерту деп аталады.

**Оқытудың техникалық құралдары:** Компьютер, ноутбук, интернет. Python орнатылған (ұсынылатын: Python 3.8+). Жеке демонстрация үшін Jupyter Notebook / Google Colab (интерактивті демонстрациялар).

Қосымша: криптография кітапханалары (PyCryptodome) - теориядан кейін салыстыру үшін.

**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: 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: RSA арқылы шифрлау алгоритмін қолданып мәтінді шифрлау және екі әдістің айырмашылығын 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)**

**Пайдаланылған әдебиеттер тізімі**

**Негізгі:**

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

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

3. 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:**

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

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