Құпия сөзбен қорғау

Орындаған: Орманбек Н.
Толеушова А.
Толуғазы Р.

Пароль

- **Пароль** (фр. *parole* – сөз)1) қарауылдық қызметті атқаруда қолданылатын бекітілген құпия сөз. Қарауылдық және гарнизондық қызмет жарғысында ол әрбір жеке қарауылға, әр күн сайын қандай да бір атау сөз түрінде бекітіледі. Пароль ауысымға келген қарауылдың дәл сол мақсатқа жіберілгенін және тиісті бастықтар бұйрығы бойынша келген ресми тұлға екенін дәлелдейді. Әскери қызметтің басқа міндеттерін атқару барысында рұқсаттама және жауап сөздері қолданылады. Пароль басқа мемлекеттердің қарулы күштерінде қарауылдық қызметті атқару барысында да, сондай-ақ барлау мен күзет қызметтерінде де қолданылады. 2) компьютердің жұмыс істеуін жалғастыру үшін теруді қажет ететін құпия сөз.

- **Пароль** (*Password, parole, watchword*) - желімен байланысу үшін немесе құпиясөзбен қорғалған ресурстардағы мәліметтерді, файлды оқу мақсатында енгізілетін құпия код (сөз); сондай-ақ бағдарламалар мен мәліметтерді рұқсатсыз пайдаланудан қорғау амалы; желіге кіру үшін рұқсатсыз пайдалануға болмайтын файлдарды оқу үшін қолданылатын жасырын бүркеме атау. Ол кез келген символдар комбинациясынан тұрады да, ұзындығы көбінесе **15 символдан аспауы тиіс**. Парольді енгізіп жатқанда оның символдарының орнына экранда жұлдызшалар *(*)* бейнеленеді.

Криптография – (Грекшеден аударылғанда Cryptos – құпия деген мағынаны береді) – бұл ғылым және шифрлау технологиясы мәліметтерді өзгертуге және авторлық құқықты сақтайды. Криптография тек қана тексттерді шифрланған формаға аударып қана қоймайды, сонымен қатар, жүйеде жұмыс жасап отырған кезде қолданушының аутентификациясын және идентификациясының берілуін қадағалап отырады.

- Криптография ең басты қауіпсіз комуникация болып табылады. Біз жүйеде жұмыс жасаған кезде тек қана адамдармен сөйлесіп қана қоймаймыз, сонымен қатар басақада қызметтер барысында араласатынымыз бізге мәлім. Мысалға, біз қандай да бір серверден программа көшіретін болсақ, біз үшін осы сервер шығарушы – фирманың сервері ма, әлде біздің компьютерімізге вирус болып түсетін пираттық фирманың сервері емес па деген ойлар келеді. Жіберу кезінде құжатты жеке және публикалық кілттер арқылы шифрлауға болады., ал оның шифрын екі пардағы кілттер арқылы ашуға болады. Құжатты шифрлап жеке кілт арқылы жіберсе, оның шифрын публикалық кілт арқылы ашуға болады, және де керісінше. Жеке кілт тек қана иесіне белгілі оны басқа біреуге беруге болмайды, осы уақытта публикалық кілт барлық корреспонденттерге ашық жария етіледі.

- Қазіргі есептеуіш машиналарының кеңінен қолданылуы адамның еңбек ету салаларын түгелдей қамтиды. Бұл жағдай баршамызға едәуір жеңілдіктер әкеліп, жаңа есептерді туындатты. Олардың бірі – ақпаратты қорғау. Компьютерлік жүйелерде ақпаратты қорғау бүгін ғылымның ерекше саласы болып табылады. Төмендегідей ақпаратты қорғау әдістері белгілі:
- - Жүйе компоненттерінің физикалық қатерсіздігін ұйымдастыру тәсілдері;
- - Бақылау, есепке алу, қатынауды басқару;
- - Ақпаратты қорғаудың криптографиялық тәсілдері;
- - Заңдылық шаралары;
- - Әкімшілік шаралары.

Қос кілттер

жеке

публикалық

Оларды аутентификация және құпияны сақтау үішн қолдануға болады.
Екі адамның мәлімет алмасуы үшін екі қос кілттер болуы қажет.

- Шифрлау кезінде қос кілттің арқасында сіз публикалық кілтті корреспонденттерге жіберіп отыру қажет емес. Бұл кілтті жүйеге ашық жазып қою сізге ыңғалы болады. Сол кезде барлық адамдар осы кілтті өздеріне жазып алып, сіздерге құпиялы мәліттерді жібере алады.


Username:
Username
Password:
Remember Password
Login
Cancel

Симметриялық және асимметриялық кілттер арқылы шифрлау.

- Әрбір уақытта ассиметриялық шифрлау симметриялық шифрлаудан эффективалық жағынан жеңіліп қалады,сондықтанда көптеген адамдар шифрлау жүйесінде ассиметиялық және дәстүрлі симметриялық шифрлау жүйесін қолданады. Ашық кілтпен шифрлау симметриялық кілт қолданылады, бұл жіберілген мәліметті ширлау үшін қолданылады.

Цифрлық қолтаңба

- Цифрлық қолтаңбаның механизмін түсндіру үшін, бір жақты хэш функияны енгізу қажет. Біржақты хэш функция бұл функция, шығарылған мәліметтің ұзындығын белгілі ұзындыққа айналдрады, оны жіберу дайджесті деп атайды. 16 байттық хэш функцяны шығару кезінде сіз 16 байттық мәлімдеме аламыз.

- Қазіргі криптографиялық жүйелер келесі Керкхофф ережесі бойынша қарастырылады:
- 1. алгоритмде қолданылатын түрлендірулер механизмі жалпыға белгілі деп саналады;
- 2. алгоритмнің сенімділігі тек қана құпия кілтке байланысты деп саналады.

- Бұл ереженің мағынасын, менімше, Брюса Шнайердің «Applied Cryptography» кітабындағы мысалы жақсы түсіндіреді: «Егер мен хатты мысалға Нью-Йорк қаласында, сейфке тығып қойып, сізге тап десем, онда бұл қауіпсіздік емес. Бұл нағыз түнек. Ал енді мен хатты алып, оны сейфке жауып, сізге сол сейфті барлық спецификацияларымен бірге тапсырайын. Тіпті жүздеген осындай сейфтерді әлемдегі ең епті ұрыларға берейін. Осы жағдайда да сіз менің хатымды сейфтен алып оқи алмасаңыз, онда бұл шын мәнінде де қауіпсіздік болады».

Ашық кілтті жүйелер

- Криптографиялық жүйелер қанша қиын әрі сенімді болғанымен, олардың істе жүзеге асуындағы әлсіз жері – кілттердің таратылу мәселесі. Пайдаланылатын жүйенің екі субъектісі арасында жасырын ақпараттар алмасуы мүмкін болуы үшін кім олардың біреуімен бірге таралып, содан кейін қалайда жасырын тәртіпте басқасына қайтадан берілген болуы тиіс. Яғни, жалпы жағдайда кілт берілуі үшін тағы да қандай да бір криптожүйелердің пайдаланылуы талап етіледі. Нәтиже негізінде бұл мәселенің шешілу үшін классикалық және қазіргі заманға алгебрамен алынған ашық кілтті жүйелер ұсынылған болатын. Олардың мәні пайдаланылатын жүйенің әр мекен – жай иесіне нақты бір ереже бойынша өзара байланысты екі кілт таратылатындығында. Бір кілт ашық боп, ал екіншісі жабық боп жарияланады.

- Ашық кілт жария етіледі және хабарлама жібергісі келетін кез келгені пайдалана алады. Құпия кілт жасырын сақталады. Бастапқы мәтіннің шифры мекен – жай иесінің кілтімен ашылады да соған беріледі. Негізінде шифрленген мәтіннің шифры сол кілтпен ашылмайды. Хабарлама шифрының ашылуы тек мекен – жай иесіне ғана белгілі жабық кілт пайдаланушымен ғана мүмкін.

Сондықтан ақпараттың сенімді қорғанысына кепіл болу үшін ашық кілтті жүйеге екі маңызды әрі айқын талаптар қойылады:

- 1. Бастапқы мәтіннің түрленуі кері қайталанбайтын болуы және оның қалпына келтірілуін ашық кілт негізінде шығарып тастауы тиіс.
- 2. Ашық кілт негізінде жабық кілт анықталуы сондай-ақ қазіргі технологиялық деңгейде мүмкін емес болуы тиіс. Оған қоса шифрды ашу қиындығы нақты төменгі баға.

Кілтпен басқару.

- Нақты пайдаланылатын жүйеге қолайлы криптографиялық жүйені таңдаудан басқа маңызды мәселе – кілттермен басқару. Криптожүйенің өзі қанша қиын әрі сенімді болғанымен ол кілттердің қолданылуына негізделген. Егер ақпараттармен жасырын алмасуды екі пайдаланушы арасында қамтамассыз ету үшін кілттермен алмасу езбе процесс болса, онда кілттермен басқаруды пайдаланушылар саны ондап жүздеп болатынпайдаланылатын жүйеде – қиын мәселе. Кілтті ақпараттың астарында пайдаланылатын барлық жұмыс істейтін кілттердің жиынтығы деген түсінік жатыр. Егер кілтті ақпараттың сенімді басқаруы айтарлықтай қамтамассыздандырылмаған болса, онда оны қолға түсіріп алып, қара ниетті барлық ақпаратқа шектеусіз ене береді.