Дәріс 1. Криптологияға кіріспе: анықтамалар, принциптер

Дәріс жоспары:

1. Криптография тарихы, принциптері
2. Атбаш шифры
3. Полибий шаршысы
4. Сцитал шифры

Криптография тарихы, принциптері

Криптография – бұл хабарламаны беру кезінде деректердің құпиялылығы мен тұтастығын сақтау, авторлықтың түпнұсқалығын тексеру және ақпаратты рұқсатсыз кіруден сенімді қорғауды қамтамасыз ету әдістерін зерттейтін ғылым. Криптография ақпаратты түрлендіру әдістерін жасайды және зерттейді, бұл рұқсат етілмеген пайдаланушыға деректерді ұстап алған жағдайда осы ақпаратты пайдалануға мүмкіндік бермейді [10]. Әрине, бұл жерде рұқсат етілмеген пайдаланушы түрлендірілген – шифрланған, яғни қорғалған хабарламаны ұстады деп болжанады.

Криптографияның тарихы бір мыңжылдықтан асады. Бұл көптеген мемлекеттік, әскери, дипломатиялық, коммерциялық, заңды және жеке құпиялармен байланысты. Ұзақ уақыт бойы жалғыз қолөнершілер криптографиямен айналысқан. Мұндай қарапайым криптографияны ұнататындардың арасында мемлекет қайраткерлері, дипломаттар, ғалымдар, қолбасшылар, тарихи тұлғалар, діни қызметкерлер, дәрігерлер, жазушылар болды. Осы кезеңде криптография бұл мәселені қажеттілікке немесе қызығушылыққа байланысты шешкен білімді қолөнершілердің тар шеңберінің кейбір жанама нәтижелері болды. Сондықтан криптографияны дамытудың бұл кезеңін – қолөнер кезеңін ғылымға емес, өнерге жатқызуға болады. Криптографияның дамуының бұл «ғылыми емес» кезеңі XX ғасырдың бірінші жартысына дейін ұзақ уақытқа созылды және ол 1949 жылы К.Шеннонның «Құпия жүйелердегі байланыс теориясы» еңбегі пайда болған кезде аяқталды деп санауға болады.

Ақпаратты қорғаудың дамуы деректерді рұқсатсыз кіруден және ағып кетуден қорғауды қамтамасыз ететін үш негізгі әдісті құруға әкелді. Бұл әдістердің әрқайсысының ақпарат түріне және қауіпсіздік қауіптерінің деңгейіне байланысты өзіндік ерекшеліктері мен қолдану салалары бар.

Қорғаудың физикалық тәсілі – құрылғыларға, ақпарат тасымалдаушыларға және ақпараттық жүйелерге физикалық қол жеткізуді болдырмауға бағытталған шараларды қамтиды. Бұл құлыптар, бейнебақылау жүйелері, үй-жайларды қорғау, сондай-ақ жабдықты қорғаудың әртүрлі тәсілдері болуы мүмкін, мысалы, медиадағы деректерді физикалық түрде жою. Физикалық қорғаныс әсіресе жұмыс процестеріне рұқсатсыз араласудың алдын алу және жабдыққа зақым келген жағдайда деректердің сақталуын қамтамасыз ету үшін өте маңызды.

Қорғаудың стенографиялық әдісі – бұл ақпаратты басқа, бір қарағанда зиянсыз объектілердің ішінде, мысалы, суреттерде, дыбыстық файлдарда

немесе мәтіндерде жасыру әдісі. Стеганография деректерді бөгде адамдар анықтамайтындай етіп жіберуге мүмкіндік береді. Қорғаудың бұл әдісі ақпаратты ұстап қалудан немесе танудан аулақ болу маңызды болған жағдайда жасырын түрде бөлісу үшін тиімді.

Қорғаудың криптографиялық тәсілі – ақпаратты тиісті кілтсіз немесе шифрды ашу алгоритмінсіз қабылдау мүмкін емес түрге түрлендіру үшін математикалық алгоритмдерді қолдану. Бұл әдіс деректерді беру кезінде де, сақтау кезінде де құпиялылықты, тұтастықты және шынайылықты қамтамасыз ету үшін кеңінен қолданылады. Криптография қорғаудың негізгі құралы болып табылады

Ақпаратты заңсыз қол жеткізуден қорғау үшін оны шифрлау әдістерін әзірлеумен криптография айналысады. Деректерді қорғауға бағытталған ақпаратты түрлендіру әдістері мен тәсілдері шифрлар деп аталады. Шифрлау-бұл шифрды қорғалған ақпаратқа қолдану процесі, яғни шифрға енгізілген белгілі бір ережелерді қолдана отырып, Ашық мәтінді шифрланған хабарламаға (Шифр мәтіні, криптограмма) түрлендіру. Шифрды шешу-шифрланған хабарлама шифрдағы бірдей ережелерді қолдана отырып, оқылатын ақпаратқа қайта түрлендірілетін кері шифрлау процесі.

Шифрлау міндеті тек жеке деректер, коммерциялық құпия, мемлекеттік ақпарат немесе құпия хабарламалар сияқты қорғауды қажет ететін ақпарат үшін туындайды. Шифрлау деректердің құпиялылығын, тұтастығын және шынайылығын қамтамасыз етеді, оларды рұқсатсыз кіруден, ағып кетуден немесе тасымалдау немесе сақтау процесіндегі өзгерістерден қорғайды. Криптографиялық Алгоритмдер ақпаратты оқылмайтын түрге айналдырады, тек шифрды шешудің кілті бар адамдарға қол жетімді. Бұл әсіресе банк қызметі, электрондық коммерция, мемлекеттік қызметтер және бетпе-бет байланыс сияқты салалардағы деректерді қорғау үшін маңызды болады. суперпозициясы сияқты шифрлардың жалпы құрылымын ұсынды.

1883 жылы Керкгоффс шифрлау жүйелеріне қойылатын алты талапты тұжырымдады:

1) жүйе, егер теориялық болмаса, кем дегенде іс жүзінде ашылмауы керек;

2) жүйені бұзу оны пайдаланушыларға қолайсыздық туғызбауы тиіс;

3) құпия кілт ешбір жазбасыз оңай есте сақталуы керек;

4) криптограмма телеграф арқылы берілетіндей нысанда ұсынылуы тиіс;

5) шифрлау аппаратурасы портативті және оған бір адам қызмет көрсете алатындай болуы тиіс;

6) жүйе қарапайым болуы керек. Ол ережелердің ұзақ тізімін немесе үлкен психикалық стрессті есте сақтауды қажет етпеуі керек.

Бұл ережелерді сол кездегі криптожүйелерді сертификаттаудың кейбір шарты ретінде түсіндіруге болады. Егер біз осы ескі шифрлау талаптарын талдайтын болсақ, қазіргі заманғы криптографиялық жүйелерде тек 3, 4 және 5-тармақтар ғана маңызды болмады. Олар заманауи ақпараттық технологияларда автоматты түрде орындалады деп айтуға болады.

Қазіргі жағдайдағы талаптардың бірінші тармағын шифрлардың шабуылдарға төзімділігі деп түсіндіруге болады. Алтыншы талапты келесідей түсіндіруге болады: құны бойынша қол жетімді криптографиялық жүйелерді құру бұл қарапайымдылықтың заманауи интерпретациясы құны. Алайда, криптографиялық жүйелерге қойылатын негізгі және мызғымас талап екінші талап болып қала береді. Бұл шарт Керкгофф ережесі деп аталады. Оның мәні криптографиялық жүйені құру кезінде жауға шифрлау алгоритмі белгілі екендігіне негізделуі керек. Шифрлаудың беріктігі тек шифрлау кілтіне байланысты екенін ескеріңіз, мысалы Энигма.

Криптографияда іргелі болып табылатын Керкгофф ережесі криптографиялық жүйенің қауіпсіздігі алгоритмнің құпиялылығына емес, тек кілттің құпиялылығына байланысты болуы керек дейді. Бұл шифрлау алгоритмі ашылған жағдайда да, егер кілт құпия болып қалса, жүйенің қауіпсіздігі қорғалады дегенді білдіреді. Криптографияда кеңінен қолданылатын шифрлардың әртүрлі кластарын қарастырыңыз:

1) Классикалық шифрлар – Цезарь шифры және Вижинер шифры сияқты әдістерді қамтитын шифрлардың ең көне түрі. Олар берілген ережеге немесе кілтке сәйкес мәтін таңбаларын басқа таңбалармен ауыстыруға негізделген. Бұл әдістер қазір ескірген деп саналғанымен, олар криптография тарихында маңызды рөл атқарды.

2) Симметриялы шифрлар – бұл шифрлар хабарламаларды шифрлау және шифрын ашу үшін бірдей кілтті пайдаланады. Мысалдарға DES және AES жатады. Бұл шифрлар жоғары жылдамдықты қамтамасыз етеді, бірақ кілтті берудің қауіпсіз әдісін қажет етеді, өйткені кілттің өзі осал жерге айналуы мүмкін.

3) Асимметриялық шифрлар, сондай-ақ ашық кілт шифрлары ретінде белгілі, ашық және жабық кілттер жұбын пайдаланады. Ашық кілт шифрлау үшін, ал жабық кілт шифрды ашу үшін қолданылады. Мұндай шифрлардың мысалдары: RSA және ECC. Асимметриялық шифрлар кілтті қауіпсіз беру мәселесін шешеді және интернет байланыстарында ақпаратты қорғау үшін кеңінен қолданылады.

4) Ағындық шифрлар – бұл шифрлар деректерді биттік түрде шифрлайды және әдетте деректер ағындарын шифрлау үшін қолданылады. Ағындық шифрлар дауыстық немесе бейне хабарламаларды шифрлау сияқты нақты уақыттағы деректерді өңдеуде тиімді.

5) Блоктық шифрлар – бұл шифрларда деректер белгіленген мөлшердегі блоктармен өңделеді. Әрбір деректер блогы бір кілтті пайдаланып бөлек шифрланады. Блоктық шифрлардың мысалдарына AES және DES жатады. Блоктық шифрлар қауіпсіздіктің жоғары дәрежесін қамтамасыз етеді және көбінесе үлкен көлемдегі деректерді қорғау үшін қолданылады.

Шифрлардың әр класының өзіндік ерекшеліктері бар және нақты пайдалану жағдайларына байланысты қауіпсіздіктің жоғары деңгейін қамтамасыз ете отырып, ақпаратты қорғау үшін әртүрлі салаларда қолданылады.

Ақпаратты қорғаудың криптографиялық әдістері Деректерді рұқсат етілмеген адамдар үшін оқылмайтын етіп түрлендіру үшін математикалық алгоритмдерді қолдануды қамтиды. Криптография шифрлау кілттерін, сандық қолтаңбаларды және хэш функцияларын қолдана отырып, ақпаратты беру кезінде де, сақтау кезінде де қорғауды қамтамасыз етеді. Ақпаратты қорғаудың криптографиялық әдістері цифрлық кеңістіктегі әртүрлі процестердің қауіпсіздігі мен сенімділігін қамтамасыз ететін қазіргі әлемнің ажырамас бөлігі болып табылады. Олар электрондық цифрлық қолтаңба, электрондық ақша, электронды жеребе, келісімшартқа отыру, бағалы қағаздар мен құжаттарды қорғау және электронды дауыс беру сияқты салаларда шешуші рөл атқарады.

– *Электрондық цифрлық қолтаңба* криптографияның ең көп қолданылатын түрлерінің бірі болып табылады. Ол электрондық құжаттардың түпнұсқалығы мен тұтастығын растау үшін қолданылады. ЭЦҚ құжатқа қол қойылғаннан кейін оның мазмұнындағы рұқсатсыз өзгерістерден қорғауды қамтамасыз етеді, бұл құжаттың қолдан жасалмағанына немесе өзгертілмегеніне көз жеткізуге мүмкіндік береді. ЭЦҚ асимметриялық шифрлауға негізделген, онда кілттер жұбы қолданылады-біреуі қол қою үшін, екіншісі қолтаңбаны тексеру үшін. Бұл қолтаңбаның белгілі бір адамға тиесілі екендігіне және құжаттың заңды түрде міндетті екендігіне кепілдік бере отырып, қауіпсіздіктің жоғары деңгейін қамтамасыз етуге мүмкіндік береді. ЭЦҚ әртүрлі салаларда, соның ішінде заңды және қаржылық транзакцияларда, сондай-ақ ақпаратты қорғаудың қатаң шаралары талап етілетін мемлекеттік басқару жүйесінде кеңінен қолданылады.

– *Электрондық ақша* немесе сандық валюта транзакциялардың қауіпсіздігін қамтамасыз ету және пайдаланушы деректерін қорғау үшін криптографиялық әдістерді қолданады. Деректерді шифрлау шоттарға рұқсатсыз кірудің алдын алуға көмектеседі, ал цифрлық қолтаңбалар транзакциялардың түпнұсқалығын қамтамасыз етеді. Криптографияны қолданатын Блокчейн технологиялары транзакция жазбаларының қауіпсіздігі мен өзгермейтіндігіне кепілдік береді, бұл электронды ақшаны интернетте қолдануға сенімді етеді.

– *Электрондық жеребе* процестің адалдығы мен ашықтығына кепілдік беру үшін криптографиялық әдістерді қолданады. Криптографиялық алгоритмдердің көмегімен жалған немесе болжау мүмкін емес кездейсоқ сандар жасалады. Бұл араласудан қорғалған кездейсоқ сандардың криптографиялық генерациясы арқылы қамтамасыз етіледі, бұл жеребені әділ етеді және нәтиженің қолдан жасалмайтындығына кепілдік береді.

– *Электронды түрде хаттамаларға* бір уақытта қол қою үшін процестің қауіпсіздігі мен заңдылығын қамтамасыз ету үшін криптографиялық технологиялар қолданылады. Әрбір тарап келісімшарт талаптарымен келісімді растау үшін өзінің цифрлық қолтаңбасын пайдаланады. Бұл қолдар Тараптардың әрқайсысы келісімшарттың шарттарына шынымен келіскенін және қол қойылғаннан кейін оның мазмұны өзгертілмегенін растайды.

– *Бағалы қағаздар мен құжаттарды қолдан жасаудан қорғау.* Қорғаудың криптографиялық әдістері бағалы қағаздар мен құжаттардың қолдан жасалуын болдырмау үшін қолданылады. Ол үшін цифрлық қолтаңбалар мен шифрлау қолданылады. Сандық қолтаңба құжаттың түпнұсқалығын растауға мүмкіндік береді және оның өзгеруіне жол бермейді. Сонымен қатар, криптографиялық алгоритмдермен біріктірілген су белгілері мен қорғалған мөртабандар сияқты технологиялар бұрмаланудан қорғау үшін қолданылады.

– *Электрондық дауыс беру.* Электрондық дауыс беруде криптография дауыстардың анонимділігі мен тұтастығын қамтамасыз етуде шешуші рөл атқарады. Шифрлау сияқты криптографиялық әдістер арқылы берілетін деректерді қорғау қамтамасыз етіледі, ал цифрлық қолтаңбалар арқылы дауыс берушілер мен дауыс берушілердің түпнұсқалығы расталады. Бұл дауыс берудің әділ, араласусыз немесе бұрмалаусыз жүргізілуін және нәтижелер өзгерістерден қорғалуын қамтамасыз етеді.

Осылайша, криптография әртүрлі қолданбалы салалардағы деректердің қауіпсіздігі мен тұтастығын қамтамасыз етуде шешуші рөл атқарады, бұл оларды қазіргі цифрлық қоғам жағдайында қауіпсіз және сенімді етеді.

Атбаш шифры

Атақты көне шифрлардың бірі – Атбаш [2, 92 б.]. Егер сіз орыс әліпбиінің таңбаларын қайта нөмірлесеңіз, онда шифрлау k нөмірімен таңбаны $(n-k+1)$ нөмірімен ауыстырудан тұрады, мұндағы n алфавиттің соңғы таңбасының нөмірі немесе алфавиттегі таңбалардың жалпы саны. Алфавит тек әріптерді ғана емес, мысалы, компьютер пернетақтасында қол жетімді барлық таңбаларды қамтуы мүмкін екенін ескеру қажет (1.1 - кесте).

1.1 – кесте. Орыс әліпбиін шифрлау

А	Б	В	Г	Д	Е	Е	Ж	З	И	Й
1	2	3	4	5	6	7	8	9	10	11
К	Л	М	Н	О	П	Р	С	Т	У	Ф
12	13	14	15	16	17	18	19	20	21	22
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
23	24	25	26	27	28	29	30	31	32	33

Бұл әліпбидегі әріптер саны $n = 33$. Ұсынылған әліпби үшін Атбаш шифрін қолданғанда *баба* сөзі *юяюя* сөзіне түрленеді (шифрланады).

Егер біз Атбаш шифрын талдайтын болсақ, онда ол алфавит әріптерінің бекітілген жаңа белгісін білдіреді. Сондықтан үлкен кернеумен бұл түрлендіру әдісін шифрлауға жатқызуға болады. Бұл әдісте кез келген мәтінді түрлендіру кезінде болуы керек кілт жоқ. Бұл түрлендіру әдісі үшін кілт жалғыз және оны мәтіннен мәтінге өзгерту мүмкіндігі жоқ. Бұл алгоритмде көптеген кілттер жоқ деп айту жақсы, бұл кез-келген криптографиялық жүйенің қажетті белгісі.

Полибий шаршысы

Шифрлаудың ежелгі тәсілдерінің бірін грек мемлекет қайраткері және тарихшысы Полибий б.з. д. 200 жыл бұрын ұсынған. 26 әріптен тұратын латын әліпбиі 5×5 ұяшықтан тұратын кестеде (шаршыда) орналасқан [2]. Бұл ретте барлық таңбаларды осы шектеулі өлшемге орналастыру үшін I әрпі J әрпімен сәйкестендірілді. Шифрланатын мәтіннің әр әрпі ол орналасқан квадраттың координаттарымен, яғни әріп орналасқан жол мен бағанға сәйкес келетін жұп сандармен ауыстырылды. Мысалы, «А» әрпін «11», ал «В» әрпін «12» және т.б. ауыстыруға болады. Бұл әдісті қолдану жеткілікті қарапайым болып шықты, бірақ сонымен бірге ақпараттың негізгі қорғалуын қамтамасыз етті. Полибий шифрының модификациялары, сондай-ақ оның әртүрлі типтегі хабарламаларды шифрлау үшін қолданылуы орта ғасырларда кеңінен қолданылды және одан әрі криптографиялық әдістердің дамуына әсер етті. Атап айтқанда, әр түрлі дәуірлерде бұл шифрдың жетілдірілген нұсқалары жасалды, бұл оны күрделі криптографиялық тапсырмалар үшін пайдалануға мүмкіндік берді.

Сцитал шифры

Сцитал шифры – бұл ауыстырылатын шифрлардың бүкіл класының негізі болған алғашқы физикалық құрылғылардың бірі. Бұл шифрлар шифрлауды қажет ететін мәтіннің әріптерін ауыстыру арқылы жасалады. Сциталдың шифры біздің эрамызға дейінгі V ғасырда Спартада ойлап табылған.

Мәтінді шифрлау үшін алдын-ала шартталған диаметрлі цилиндр қолданылды. Тар пергамент таспасы цилиндрге оралып, цилиндр осі бойымен ашық мәтін жазылды. Содан кейін таспа оралып, мақсатына қарай жіберілді. Хабарламаны алушы таспаны бірдей диаметрлі цилиндрге орап, содан кейін оны оқыды.

Бұл шифрлау әдісінің кілті цилиндр радиусының өлшемі екенін ескеріңіз. Бұл шифрды бұзу әдісі Аристотельге жатады [1, б. 43]. Бұзу әдісі келесідей болды: таспа ұзын конусқа оралып, содан кейін оны конус бойымен Жылжыта бастады. Мәтін әріптері сөздерді немесе буындарды құрған жерде конустың диаметрі цилиндрдің диаметріне сәйкес келді.

Сцитал шифры ауыстырылатын шифрлар класының өкілі болып табылады. Жалпы алғанда шифрлардың бұл класын келесідей сипаттауға болады. k саны 1–ден k–ге дейінгі $1, 2, \dots, k-1, k$ сандар тізбегін анықтасын. Осы $a_1, a_2, \dots, a_k$ сандарының ерікті алмастыруын орнатайық. k саны және тіркелген ауыстыру $a_1, a_2, \dots, a_k$ жүйенің құпия кілті болып табылады. Ашық деректерді одан әрі түрлендіру келесідей жүреді. Ашық мәтін топтарға бөлінеді, олардың әрқайсысында k әріптері бар. Әр топта әріптер таңдалған $a_1, a_2, \dots, a_k$ ауыстыруына сәйкес қайта реттеледі.

Мысал. «Встречай одиннадцатого марта» деген мәтін берілсін. $k = 6$ деп таңдайық. 1–ден 6–ға дейінгі сандарды ауыстыруды келесідей анықтаймыз: 3, 5, 1, 6, 2, 4. Мәтінді алты таңбадан тұратын топтарға бөлу

«Встреч, ай_оди, ннадца, того_м, арта.!»

Мәтіндегі «_» белгісі бос орынды білдіреді. Енді әр топтың үшінші әріпі бірінші орынға, бесіншісі екінші орынға, бірінші үшінші орынға, алтыншы төртінші орынға, екінші бесінші орынға, төртінші алтыншы орынға орналасады. Соңғы топта k әріптен аз болса, онда мәтінді толықтыру керек. Біздің жағдайда «.» таңбалары қосылды. және «!», өйткені олар ашық мәтіннің мағынасын өзгертпейді. Нәтижесінде ашық мәтін келесіге түрлендіріледі

«Тевчср, _дайё, атснанд, г_тмоо, т.а!ка».

Түсіндіруге ыңғайлы болу үшін әріптер тобын бөлетін үтірлерді алып тастасаңыз, біз келесі шифрланған хабарламаны аламыз:

Тевчср_даийоацнандг_тмоот.а!ка

Шифрды шешу кері тәртіпте жүзеге асырылады, атап айтқанда: шифрланған мәтіннің алты әрпінен тұратын топтың бірінші таңбасы үшіншіде, екінші таңба бесіншіде және т.б. болады, бекітілген пермутацияға сәйкес.

Компьютерде мұндай түрлендіру бағдарлама түрінде жүзеге асырылатындығын ескеріңіз, бұл алгоритм бойынша қолмен шифрлау көп уақытты қажет ететініне қарамастан.

Сценарийдің шифрын қолмен шифрлауға ыңғайлы басқа түсіндірмеде ұсынуға болады. Кейінірек талқыланатын бұл интерпретация шифрлау кестелерін немесе «маршрут» бойынша шифрлауды тудырады.

ҚОЛДАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Брюс Ш. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Шнайер, Брюс. – М.: Триумф, 2003. – 816 с.

2. Введение в криптографию. Под редакцией В.В. Ященко. / Под общ. ред. В.В. Ященко. – М.: МЦНМО, «ЧеРо.», 2018. – 272 с.

3. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. / Иванов, М. А. – М.: «Кудиц-образ», 2018. – 368 с.