ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ РА ЎРТА МАХСУС ТАЪЛИМ
ВАЗИРЛИГИ

НАМАНГАН МУҲАНДИСЛИК-ПЕДАГОГИКА
ИНСТИТУТИ

"Кадрлар тайёрлаш миллий дастури" ни
амалга оширишнинг II-сифат босқичи
вазифаларига бағишланган
магистрантларнинг анъанавий
III - илмий-амалий конференцияси

М А Т Е Р И А Л Л А Р И

I - ҚИСМ

НАМАНГАН - 2003 й

бўлинади: *синтактик* (матн ичидаги хатоликлар) ва *алгоритмик*. Синтактик хатоликларни (белгиларнинг алмашганлиги, тушириб қолдирилганлиги ва хоказолар) осон топилади. Алгоритмик хатоликларини топиш мушкулроқ кечади. Маълумотларни киритиш бир-икки бор такрорлангандан сўнг ҳам дастур тўғри ишласа, хатоликларини текшириш бўлими якунланган хисобланади.

Тестдан ўтказиш босқичи ўта мухим бўлиб, яратилган дастурдан бошқалар ҳам фойдаланиши ҳисобга олинади. Бу босқичда дастурни қанча кўп маълумотни кўтара олиши ва унда киритилиши мумкин бўлган нотўғри маълумотлар текширилади.

Юқорида келтирилган босқичлар ёрдамида ўқув жараёнига тегишли бўлган исталган жараённи автоматлаштириш мумкин.

Энди ўқув жараёнини автоматлаштириш масаласини кўриб чиқамиз:

Ушбу дастурдан фойдаланувчи жорий семестр ўқув жараёнининг боришини назорат қила олиши учун қуйидаги маълумотлар киритилиши лозим:

- гуруҳлар, талабаларнинг рўйҳати;
- ўрганилаётган фанлар рўйҳати;
- кафедра ўқитувчиларининг рўйҳати;
- ҳар бир гуруҳнинг назарий ва амалий машғулотлари ҳақида маълумотлар;
- ҳар бир ўтказилган машғулот бўйича топширилган имтиҳонлар (синовлар) натижалари.

Дастур шундай тузилиши лозимки, тузилган дастур ёрдамида фойдаланувчи қуйидаги маълумотларни олсин:

- «Гуруҳнинг имтиҳон варақаси» номли ҳужжат;
- ҳисоб-китоб йўли билан олинган талабаларнинг ўртача бали;
- имтиҳон топширмаган талабалр сонига қараб гуруҳдаги ўртача баҳони ҳисоб-китоб қилган ҳолда топширилган имтиҳонлар натижаларининг таҳлили;
- кафедра томонидан жорий семестрда ўтказилаётган машғулотлар соатларининг умумий миқдори ҳамда ўқитувчиларнинг ўртача вазифаси.

Фойдаланувчини мазкур ахборот билан таъминлаш учун маълумотлар базасида талабалар гуруҳлари, гуруҳлар таркиби, кафедралар ва уларнинг ўқитувчилар таркиби, талабалар ўрганилаётган фанлар ҳақида сўров маълумотлари, гуруҳларда ўтказилаётган машғулотлар ва талабаларнинг жорий семестрдаги ўзлаштирувчилари ҳақидаги ҳисобот маълумотлари сақланиши лозим.

Ўқув жараёнининг боришини ахборот объектлари билан таснифланиши қуйидаги жадвалда келтирилган:

Ахборот объекти	Реквизит номи	Аломат	Калит белгиси
1	2	3	4
ГУРУҲ	Гуруҳ рақами	ГР	Оддий калит
	Талабалар сони	ТСОН	
	Гуруҳдаги ўртача кириш рақами	ГКБАЛЛ	
ТАЛАБА	Гуруҳ рақами	ГР	Мураккаб калит
	Талабанинг рўйҳатдаги рақами	ТРР	
	Фамилияси, исми, шарифи	ФИШ	
	Туғилган йили	ТУҒЙ	
	Манзилгоҳи	АДРЕС	
	Талабанинг ўртача кириш бали	ТКБАЛЛ	
ФАН	Фан коди	ФК	Оддий калит
	Фан номи	ФН	
	Жами соатлар	СОАТЛАР	
	Маъруза соатлари	МАЪРС	
	Амалиёт соатлари	АМАЛС	
	Семестрлар сони	СЕМС	
	Курс дастури	ДАСТ	
1	2	3	4
КАФЕДРА	Кафедра коди	КАФК	Оддий калит
	Кафедра номи	КАФН	
	Телефон	ТЕЛ	
	Мудирнинг Ф.И.Ш.	МУД	
	Мудир фотосурати	ФОТО	
ЎҚИТУВЧИ	Рўйҳат рақами	ТАБР	Оддий калит
	Ўқитувчи Ф.И.Ш.	ФИШ	
	Илмий даражаси	ИЛМДАР	
	Илмий унвони	ИЛМУН	
	Кафедра коди	КАФК	

Маълумотларни мухофаза қилишда критографик усуллардан фойдаланиш афзалликлари

Магистрант Х.Мансуров, акад. М.Комилов, талаба Ф.Ирисқулов

Интернет технологияларининг яратилиши турли манбалардан тез ва осон йўл билан ахборот олиш имкониятларини ҳамма учун-оддий фуқародан тортиб йирик ташкилотларгача мисли кўрилмаган даражада ошириб юборди. Давлат муассасалари, фан-таълим муассасалари, тижорат корҳоналари ва алоҳида шахслар ахборотни электрон шаклда яратиб-сақлай бошладилар. Бу муҳит аввалги физикавий сақлашга нисбатан катта қулайликлар туғдиради: сақлаш

жуда иҳчам, узатиш эса бир онда юз беради ва тармоқ орқали бой маълумотлар базаларига мурожаат қилиш имкониятлари жуда кенг. Ахборотдан самарали фойдаланиш имкониятлари ахборот миқдорининг тез кўпайишига олиб келди. Бу албатта оммавий ахборот ва ҳамма билиши мумкин бўлган ахборот ҳақида гап борганда ўта ижобий ҳодиса. Лекин, пинхона ва маҳфий ахборот оқимлари учун интернет технологиялари қулайликлар билан бир қаторда янги муаммолар келтириб чиқарди. Интернет муҳитида ахборот ҳавфсизлигига таҳдид кескин ошди:

- ахборот ўғирлаш;
- ахборот мазмунини бузиб қўйиш, эгасидан изнсиз ўзгартириб қўйиш;
- тармоққа ва серверларга ўғринча суқулиб кириш.

Ахборот ҳавфсизлигини таъминлаш қуйидаги уч асосий муаммони ечишни назарда тутади. Булар:

- пинхоналик;
- бутунлик;
- қобиллик.

НИСТ 7498-2 ҳалкаро стандарти асосий ҳавфсизлик ҳизматларини белгилайди. Унинг вазифасига очик тизимлар алоқаси моделининг ҳавфсизлик йўналишларини аниқлаш киради. Булар:

1. Аутентификация. Компьютер ё тармоқ фойдаланувчисининг шаҳсини текшириш;
2. Киришни бошкариш. Компьютер тармоғидан фойдаланувчининг руҳсат этилган киришини текшириш ва таъминлаш;
3. Маълумотлар бутунлиги. Маълумотлар массиви мазмунини тасодифий ё қасддан беруҳсат усуллар билан ўзгартиришларга нисбатан текшириш;
4. Ахборот пинҳоналиги. Ахборот мазмунини изнсиз ошкор бўлишдан ҳимоялаш;
5. Инкор эта олинмаслик. Маълумотлар массивини жўнатувчи томонидан уни жўнатганлигини ёки олувчи томонидан уни олганлигини тан олишдан бўйин товлашининг олдини олиш.

Тармоқни компьютер тажовузларидан ҳимоялаш доимий ва ўз-ўзидан ечилмайдиган масаладир. Лекин қатор оддий ҳимоя воситалари ёрдамида тармоққа суқулиб киришларнинг кўпчилигини олдини олиш мумкин.

Тажовузкорлар кўпинча тармоққа унинг аҳамиятга молик жойларидан ўтувчи трафигини тинглаш орқали, трафикдан фойдаланувчиларни ва уларнинг паролларини ажратиб олиш ёрдамида суқулиб кирадилар. Шунинг учун олисдаги машиналар

билан боғланишлар парол билан ҳимояланганда шифрланиши шарт. Бу айниқса, боғланиш интернет каналлари орқали амалга оширилганда ёки аҳамиятли сервер билан боғланилганда зарур. Интернет муҳити билан бирлашган интранетда ахборот оқимини ва ресурсларни энг ишончли ҳимоялаш воситаси носимметрик ва симметрик криптотизимлардан биргаликда фойдаланишдир.

Криптографик тизим, ё қисқача, криптотизим шифрлаш ҳам шифрни очиш алгоритмлари, бу алгоритмларда ишлатиладиган калитлар, шу калитларни бошқарув тизими ҳамда шифрланадиган ва шифрланган матнларнинг ўзаро боғланган мажмуасидир.

Криптотизимдан фойдаланишда матн эгаси шифрлаш алгоритми ва шифрлаш калити воситасида аввало дастлабки матнни шифрланган матнга ўгиради. Матн эгаси уни ўзи фойдаланиши учун шифрлаган бўлса (бунда калитларни бошқарув тизимига хожат ҳам бўлмайди) сақлаб қўяди ва керакли вақтда шифрланган матнни очади. Очилган матн асли (дастлабки матн)га айнан бўлса сақлаб қўйилган ахборотнинг бутунлигига ишонч ҳосил бўлади. Акс холда ахборот бутунлиги бузилган бўлиб чиқади. Агар шифрланган матн ундан қонуний фойдаланувчига(олувчига) мўлжалланган бўлса у тегишли манзилга жўнатилади. Сўнгра шифрланган матн олувчи томонидан унга аввалдан маълум бўлган шифр очиш калити ва алгоритми воситасида дастлабки матнга айлантирилади.

Бунда калитни қандай ҳосил қилиш, алоқа қатнашчиларига бу калитни маҳфийлиги сақланган холда етказиш, ва умуман, иштирокчилар орасида калит узатилгунга қадар ҳавфсиз алоқа каналини ҳосил қилиш асосий муаммо бўлиб туради. Бунда яна бошқа бир муаммо аутентификация муаммоси ҳам кўндаланг бўлади. Чунки, дастлабки матн(ҳабар) шифрлаш калитига эга бўлган кимса томонидан шифрланади. Бу кимса калитнинг ҳақикий эгаси бўлиши ҳам, бегона (мабодо криптотизимнинг сири очилган бўлса) бўлиши ҳам мумкин.

Алоқа иштирокчилари шифрлаш калитини олишганда у чиндан ҳам шу калитни яратишга ваколатли кимса томонидан ё тажовузкор томонидан юборилган бўлиши ҳам мумкин.

Бугунги кунда ахборот ҳавфсизлигини таъминлашда анъанавий қўлланилиб келган ёндашувлар ва воситалар етарли бўлмай қолди. Бундай шароитда ахборот ҳимоясининг энг ишончли ва синалган усули бўлган криптографиянинг аҳамияти янада ошди.

Криптология икки илмий ирмоққа ажралади. Булар криптография ва криптотаҳлилдир.

Криптография - криптография амаллари асосида ахборот ҳавфсизлигини таъминлаш фани бўлиб, асосан тўрт ҳил ҳавфсизлик муаммоси ечимларини топиш билан шуғулланади. Булар:

- пинҳонийлик;
- ахборот бутунлиги;
- аутентификация:

- ахборот эгасини аутентификацияси - ахборот юборган шахснинг асл шахслигини текшириш;
- ахборот асл нусхасини аутентификацияси - олинган ахборот ўз аслига айнанлигини текшириш.

▪ алоқа қатнашчилари назорати:
- инкор этаолмаслик - ахборот йўллаганликни ё уни (умуман ё ўз вақтида) қабул қилиб олганликни бўйнига олмасликни олдини олиш.

Криптография амалларининг энг асосийлари шифрлаш ва шифрни очишдир. Шифрлаш - шифрлаш калити иштирокида берилган (дастлабки) ахборотни бегона олиб тушунмайдиган шаклга, яъни шифрланган ахборотга айлантиришдир. Шифрни очиш - шифрланган ахборотни уни очиш калити ёрдамида дастлабки ахборотга айлантиришдир. Шифрни бузиб очиш - шифрланган ахборотни шифрни очиш калитини билмаган ҳолда дастлабки ахборотга айлантиришдир.

Шифрлаш пинҳонийликни таъминлаб, ахборотни бегоналардан маҳфий сақлаш имконини беради. Шифрланадиган ахборот, умуман олганда матн, овоз ёзуви ва тасвир шаклида, ё бўлмаса аралаш шаклда берилиши мумкин. Амалиётда шифрланадиган ахборот асосан матн шаклида берилади ва шифрланган матнга айлантирилади.

Криптография усуллари алоқа тизимининг ҳавфсизлигини таъминлаш учун қўлланилганда у алоқа мазмунинигина, яъни узатилаётган ахборотнинг ўзинигина ҳимоялайди, алоқа мавжудлигини, шу жумладан алоқанинг кимлар орасида ва қандай интенсивликда содир бўлаётганини эса ҳимоя қилолмайди.

Ахборот узатиш ва сақлаш жараёнларининг рақамлаштирилиши узлукли (нутқ) ва узлуксиз (матн, факс, тасвир, анимация) ахборотларни ҳимоялаш учун ягона алгоритмлардан фойдаланиш имконини беради. Бундан буён шифрланадиган ахборот матн шаклида берилиши назарда тутилади.

Симметрик криптотизимларда ахборот алмашиш уч босқичда юз беради:
- ахборот жўнатувчи уни олувчига ўзаро маҳфий калитни, яъни икковларидан ўзга ҳеч кимга маълум бўлмаган калитни топширади;
- жўнатувчи ўзаро маҳфий калит билан ахборотни шифрлаб уни олувчига жўнатади;
- қабул қилиб олувчи ахборотни олиб унинг шифрини ўзаро маҳфий калит билан очади. Умуман олганда иккала томон бу калитдан бир неча бор қайта фойдаланишлари мумкин.

Шу калитдан алоқа учун қайта фойдаланилганда ёки калит ахборот эгасининг ўзи ишлатадиган матнни шифрлаш учун тузилган бўлса, албатта, шифрланадиган ахборот миқдори билан тенг калитдан фойдаланиш ҳар доим ҳам қулай бўлавермайди. Биринчи босқичга ҳожат бўлмайди. Агар ҳар куни ва ҳар бир алоқа сеанси учун янги

ноёб калит ишлатилса, криптотизимнинг ҳавфсизлиги юқорироқ бўлади.

Носимметрик криптотизимларда ахборот алмашиш қуйидаги босқичларда юз беради:
- ахборот қабул қилиб олувчи томон уни тайёрлаб жўнатувчига ўзининг шахсий ошкора калити маълум бўлишига эришади, бу калит бошқа кимсаларга ҳам маълум қилиниши мумкин;
- жўнатувчи томон ахборотни уни қабул қилиб олувчининг шахсий ошкора калити билан шифрлаб уни олувчига жўнатади;
- қабул қилиб олувчи томон шифрланган ахборотни олиб, унинг шифрини ўзининг шахсий маҳфий калити билан очади. Бу шифрланган ахборотни ошкора калит эгасидан ўзга ҳеч ким очаолмайди, чунки уларда бунга мос маҳфий калит йўқ.

Умуман олганда, битта ошкора калитдан бир неча киши кўп маротаба фойдаланиб, ягона манзилга-шу ошкора калит эгасига турли ахборотлар жўнатишлари мумкин. Кўпчилик шу ошкора калитдан унинг эгаси рақамли имзо чеккан ҳужжатларнинг унга тегишли эканига ишонч ҳосил қилиш мақсадида ҳам фойдаланиши мумкин. Чунки, бу ошкора калит билан фақаттина унинг эгаси ўз маҳфий калити билан имзолаган ҳужжатлардаги имзоларнигина шифрини очиш мумкин.

Амалиётда икки хил тизимни биргаликда ишлатиш юқори самара беради: симметрик тизимдан кўп ҳажмли ахборотларни шифрлашда, носимметрик тизимдан симметрик тизим калитини шифрлаб тарқатишда фойдаланиш қулай.

Чегаравий масалаларни ечишда С.К.Годуновнинг ортоганал хайдаш усули афзалликлари

Магистрант М.Дадамирзаев, доц.С.Ирисқулов

Амалий масалаларнинг математик моделлари кўпинча қуйидаги биринчи тартибли дифференциал тенгламалар системаси учун ёзилган чегаравий масала орқали ифодаланади:

$$\frac{dy}{dx} = [A(x)]y + b(x) \qquad (1)$$

чегаравий шартларни умумий ҳолда қуйидагича ёзиб оламиз:

$x = x_0$ (интеграллаш оралиғини чап чегараси) нуқтада

$$\|C_0\|y = \|C_0\|y^{(0)} \qquad (2)$$

$x = x_0$ (интеграллаш оралиғини ўнг чегараси) нуқтада

$$\|C_1\|y = \|C_1\|y^{(n)} \qquad (3)$$

бу ерда