Әдістемелік нұсқаулардың титулдық парағы

Нысан

ПМУ ҰС Н 7.18.3/40

Қазақстан Республикасының білім және ғылым министрлігі

С. Торайгыров атындағы Павлодар мемлекеттік университеті

Есептеу техникасы және бағдарламалау кафедрасы

«Ақпараттық қауіпсіздік негіздері» пәні бойынша

5В070400 «Есептеу техникасы және бағдарламалық қамтама» мамандығының студентеріне арналған

Курстық жұмысқа

ӘДІСТЕМЕЛІК НҰСҚАУЛАР

Павлодар

Әдістемелік нұсқауларды

бекіту парағы

Нысан

ПМУ ҰС Н 7.18.3/41

БЕКІТЕМІН

ОІ жөніндегі проректор

_____ _____

(қолы) (аты-жөні)

20__ж. «___»_____

Құрастырушы: аға оқытушы _____Балгабаева Г.С.
(қолы)

Есептеу техникасы және бағдарламалау кафедрасы

«Ақпараттық қауіпсіздік негіздері» пәні бойынша

5В070400 «Есептеу техникасы және бағдарламалық қамтама» мамандығының студентеріне арналған

Курстық жұмысқа

әдістемелік нұсқаулар

Кафедраның отырысында ұсынылды

20__ж. «___»_____, №__ Хаттама

Кафедра меңгерушісі _____ О.Г. Потапенко
(қолы)

Факультеттің әдістемелік кеңесімен құпталған 2010ж. «__»_____№_____ хаттама

ӘК төрағасы_____ Ж.Г. Муканова 2010ж. «__»_____
(қолы)

МАҚҰЛДАНДЫ:

ЖжӘҚБ бастығы _____ Варакута А.А. 2010ж. «____» _____
(қолы) (аты-жөні)

Университеттің оқу-әдістемелік кеңесімен мақұлданды

20__ж. «___»_____ №____ Хаттама

Жұмыстың тақырыбы – кәсіпорынның ақпараттық қауіпсіздігінің жүйесінің жобалауы.

Курстық жұмыстың мақсаты - "Ақпараттық қауіпсіздіктің негіздері" курс бойынша студенттердің білімдерінің қуыс және бекітуі, жобалау, жасау және қазіргі есептеуіш техниктера құралдарының қолдануымен әр түрлі мақсаттың ақпараттық жүйелерінің пайдалануының жанында ақпараттық қауіпсіздіктің қамтамасыз етуі негізгі қағидалары туралы ұсыныстардың бекітуі.

Курстық жұмысқа тапсырма

Кәсіпорынның ұйымдық құрылымы, (өндірістік және диплом алдындағы тәжірибенің өтуін орынмен сәйкес шамамен) таңдаулы студентті талқыланып және кәсіпорынның ақпараттық жүйесінің схемасын жасауға керек. Қауіптердің талдауды негізінде, кәсіпорынның ақпараттық қауіпсіздігінің жүйесін жасай алды.

Жұмыста бірнеше біртіндеп шифрлау блоктерінің қолдануымен ақпарды кодтаудың негізгі алгоритмдарын криптоанализдың негізінде кәсіпорынның ақпараттық жұйесінің крипто қорғауын іске асыру үшін бағдарламаны объективті-хабар жол қолдана жасауға керек.

Кіру мәліметтері 4-ші әдістердің бірі көмегімен шифрлау. Шифрын анықтауды ескеру. Егер әдіс соңғы болып табылмаса, нышандық және қажетті қолданудың мақсаты бар кодтық тізбектерінің берілуі үшін тізбекті алынсын бұл басқа әдістің кіру мәліметтері.

Шифрлауды тізбек барлық 4-ші әдістердің қолдануымен өткізу.

Әдістердің қолдануын тізбек еркін қабылданады. Орындаудың жанында әрбір тапсырма жауаптың алуын әдіс толық сипаттауға керек.

Қолданылатын курстық жұмыстарда шифрлауының әдістері:

1. Цезарь шифры;
2. Баспалдақ шифр:
3. Тік орын ауыстыруды шифр:
4. Виженер шифры.

Теориялық мәліметтер

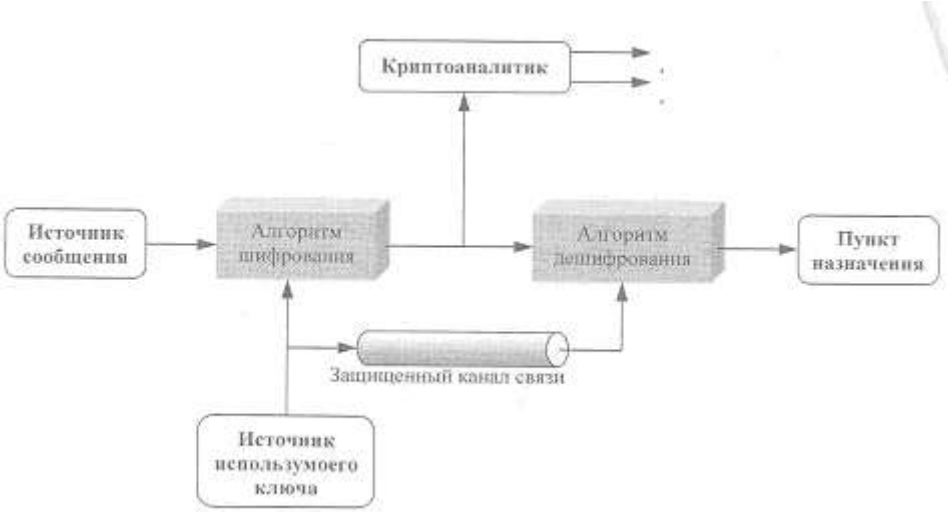
Компьютерлер және құралдардың автоматты мәліметтері пайда болумен және таратумен мәліметтің сақталатын компьютерлерімен тағы басқалар файлдардың автоматты қорғау құралдарындағы қажеттігі пайда болды. Қорғау құралдарындағы қажеттік әсіресе өткір көп қолданушы жүйелер, уақытты бөлуі бар сондай жүйелерде, сонымен бірге байланыстың кәдімгі телефон сызықтары немесе ашық компъютер желілері бойынша рұқсат алуға болған жүйелердегі сезіледі. Хакер әдістер және құралдардың жиынтығы, мәліметтердің қорғаныстығы және қарсы әрекеттің сипаттамалары үшін сондықтан, компьютер қауіпсіздігі терминді қолданыла бастады.

Абзалы, өзі маңызды желінің автоматты қорғау құралдары және коммуникациялар шифрлау болып табылады.

Оңаша берілу талап ететін қатынас ашық мәтінмен деп аталуға қабылдалған. Мақсаты бар ашық мәтіннің өрнектеуінің процессі үшін оның мағынасы бөтен тұмандандырсын (шифрлаумен) шифрлаумен деп аталады.

Қатынастар шифрлаудың нәтижесінде шифртекст пайда болады. Ашық мәтінге шифртекстаның кері өзгеруін процесс (айыбын ашумен) шифрын анықтаумен деп аталады. Заңсыз қолданушылардағы оның қорғауының мақсаты бар мәліметінің (шифрлау) өрнектеуінің әдіс үйретететін ғылым кртипографией деп аталады.

Сурет арқылы 1 дәстүрлі шифрлаудың негізгі сұлбаның элементтерін қарап шығамыз.



Сурет 1 – Криптожүйе дәстүрлі үлгісі

Көз Х/ Х=ның ашық мәтінінің формасындағы қатынасты құрады.Холар: Хм. Элементтермен

Х-шы ашық мәтіннің Х\сі кейбір түпкі әліпбидің нышандары болып табылады. Шифрлаулар үшін К=[К1, К2,...Кj] формадағы кілт шығарады. Х және шифрлаудың кілтінің қатынастары болған жағдайда бастапқы

мәліметтер ретінде Хі шифрлалған мәтін шифрлауы алгоритмы арқылы қалыптасады. Y - бұл формуланың түрінде жазып алуға болады

Көз X= [X1, X2, ..., Хм] олардың ашық мәтінінің формасындағы қатынасты құрады – элементтермен хо, ашық мәтіндер Х кейбір түпкі әліпбидің нышандары болып табылады. Шифрлаулар үшін К1 К=ны формадағы кілтті шығарады. Болған жағдайда бастапқы мәліметтер ретінде Х және шифрлаудың кілтінің қатынастары шифрлауы алгоритмы арқылы қалыптасады барлық сорпалардың шифрлалған мәтіні. Бұл формуланың түрінде жазып алуға болады

$$Y=Ek(X)$$

Осы өсиет білдіреді мәліметтің ашық мәтінге Е шифрлауды алгоритмды қолдануы қатынастың алушысы.

Кілтінің қолдануында К кілтімен орналастыра жолымен пайда болады кері өзгеру орындау мүмкіндігі алуы керек (қасында)

$$X=Dк(Y)$$

Рұқсатсыз рұқсат бірақ таныстыру мүмкіндік ие болатын жау А де. Х да. Х қалпына келтіруге талаптана алады немесе немесе екі бұл объекттер. Сонымен бірге жауды шифрлауды алгоритм білетінін жобаланады), және (Е) шифрын анықтауды алгоритм. Егер жау тек қана бір нақты қатынас айырып тануға қызықтырса, оған жау Х дегенмен тиісті бастапқы ашық мәтінге мүмкін құрастыру қалпына келтірудегі өз күштері Х жолымен жиірек жұмылдыру керек болады оқып отыру мүмкіндігінің алуында және барлық келесі қатынастар қызықтырған. Оның негізгі күштері осы жағдайда тиісті бастапқы кілтке мүмкін құрастыру қалпына келтіруде жолымен жұмылдыруы керек.

Х-шы мәндердің жасауын процесс немесе, немесе, және сол, тағы басқалар, криптоанализбен деп аталады. Адам, криптоанализбен шұғылданады, аналитиктермен деп атайды.

1. Крифтографиялық жүйелердің классификациясы

Негізі криптографиялық жүйелерінің жағдайының классификация келесі үш тәуелсіз мінездемелердің негізінде салады.

1.Ашық мәтінінің өрнектеуі бойынша операцияларының түрі шифрлалған. Шифрлаудың барлық алгоритмдары екі операциялардың қолдануларында тұрақтанады: алмастырулар ашық мәтіннің элементтерінің жүруді ретінің өзгеріс білдінетін кейбір басқа элементті (бит, биттердің әріп, тобы немесе әріптердің тобы) ашық мәтіннің әрбір элементінің орнын басу білдінетін, және орын ауыстыру. (барлық операцияларды қайтатындық яғни) мәліметтің жоғалтулардың жоқтығы бас талаппен сонымен бірге өйткені. Шифрлаулар нақты жүйелердің көпшіліктерінде қолданады, бір емес емес, алмастыру және орын ауыстырудың бірнеше операцияларының комбинация. Тиісті шифрлар продукция деп атайды.

2.Қолданылатын кілттердің саны. Егер жіберуші болса, және алушы ылғи бір кілт, жүйені қолданамын симметриялық, бір кілті бар жүйемен, құпия кілті бар жүйемен немесе дәстүрлі шифрлауды схемамен деп аталады.

Егер жіберуші және алушы әртүрлі Ключилер, жүйелерді қолданады асимметриялық деп аталса, екі кілттері бар жүйемен немесе шифрлауды схемамен ашық кілтпен.

3.Ашық мәтіннің өңдеуін әдіс. Блоктық шифрлау блоктердің ашық мәтінінің өңдеуін ойлайды, өңдеудің нәтижесінде әрбір блок дегенмен шифрлалған мәтіннің блогі пайда болады. Ағынды шифрлау ашық мәтіннің барлық элементтерін шифрлау дәйекті түрде түсінеді, біртіндеп, әрбір кезеңде не нәтижеде шифрлалған мәтіннің элементіне бір-бірдендері пайда болады.

2. 3.1-ші шифрлауды классикалық техника. Алмастыруларды қолдану

Ашық мәтіннің жеке әріптерінің алмастыруының жанында басқа әріптер немесе сандармен, немесе қандай болса да басқа нысандармен ауыстырылады. Егер ашық мәтін биттердің тізбегін сияқты қаралса, онда қойылу шифрлалған мәтіннің биттерінің тап қалған тізбектерінің ашық мәтіннің биттерінің тап қалған тізбектерінің алмастыруына апарады.

Цезарь шифры.

Белгілі қойылатын шифрлардың өзі ежелгі және ең онайы Юлий цезарь қолданған шифр болып табылады. Әліпбидің әрбір әрібі цезарь шифрында әліпби бұл бәрінен алыстың үш позицияда болатын әріппен ауыстырылады. Циклдік бұл әліпбиде болып есептеледі, яғни мен әріпке әрбір әріпке А

Егер әрібі шығады санмен көрсетілген (А= 1,Б = 2 және тағы басқалар) балама тағайындар еді. шифрлауды алгоритм бірде келесі формулалармен айқындауға болады. Р ашық мәтінінің әрбір әрібі шифрлалған мәтіннің әрібімен ауыстырылады:

$$C = E(P) = (P+3) \bmod (26).$$

Жылжу жағдайда бола алады, сондықтан Цезарь ортақ алгоритмы формуламен жазылады

$$C = E(P) = (P+к) \bmod (26).$$

қайда мән аралықта (қарастырылған әліпби үшін) 1-ден 31-ге аралығындағы қабылдайды. Сонымен бірге шифрын анықтауды алгоритм қарапайым:

$$P = D(C) = (C-к) \bmod (26).$$

Егер нақтылы мәтін Цезарь шифры арқылы шифрлағаны белгілі болса, онда барлық варианттар асып кетуі бос тұруы арқылы шифр өте оңай ашылсын - ол үшін болуы мүмкін кілттің 31 варианты тексеруге жеткілікті.

Барлық болуы мүмкін варианттардың біртіндеп асып кетуді әдісінің қолдануы осы шифрдың келесі үш маңызды мінездемелерімен ақтаған.

1. Шифрлау және шифрын анықтаудың белгілі алгоритмдары.
2. Жинағы 31 вариант сұрыптауға керек.
3. Ашық мәтіннің тілі белгілі және оңай танимыз.

Алгоритм белгілі ойлау мүмкін алгоритм белгілі ойлау мүмкін компьютер мәліметінің қорғауы туралы сөз болатындасы жағдайлардың

көпшілігінде. Жалғызы, біртіндеп асып кетуді әдістің негізінде іс жүзінде пайдасыз криптоанализ не істейді - бұл үшін кілттер өте көпті сұрыптауға керек болатын алгоритмды қолдану.

Моноалфавиттық шифрлар.

Болған жағдайда жинағы 31 цезарьнің шифрының кілттердің варианты болуы мүмкін болып есептелсін берік қорғал қалған болғандай етіп алыс. Кілттердің кеңістіктері маңызды кеңейту қолдану кез келген алмастырулар рұқсат етіліп қол жеткізуге болады.

Мысалы, егер Цезарь шифрында әліпбидің қолдану орын ауыстырулардың қайсысы болса да 31 нышандары мүмкін десе, жылжуға ғана емес нышан болса, онда біздерді 31 аламыз кілттер болуы мүмкін.

31 әсер жасалады дәл осылай емес кілттер (нені 8x10 асады) онда жай ғана сұрыптасын, және осы шифрға сенімділіктің биік дәрежесімен ие болады. Аналитика үшін дегенмен шабуылдың тағы басқа сызығы бар болады. Мысалы, егер аналитик ашық мәтіннің табиғаты туралы ұсынысты алса, ағылшын тіліненің мәтін сол, мынау не туралы тиісті тіліне мәтін тән сипатты белгілер туралы белгілі мәліметті қолдану мүмкін) қолдану мүмкін.

Мысалы, бір және ашық мәтіннің әрібі та кілттің ылғи бір әрібіне сәйкес келетіндігі, онда аналитик шифрын анықтауды бірінші кезеңде шифрланған мәтіндегі әріптердің қолдануы жиіліктің талдау жүргізуге және шифртекстаның нышандарының арасындағы шамамен сәйкестік орната алады және суреттің диаграммасына сәйкес әліпби 2. шифртекст тезірек жинағы, жиі қолданылатын нышан әріп Еге сәйкес келеді. Бұдан әрі сол өзі таралған (үш әріптерден комбинациясымен яғни) триграммамен ағылшын тілінде ашық мәтінді қалпына келтірген және шамаланған кілтте көз жеткізуге жартылай мүмкіндік беретін the болып табылған айғақ қолдануға болады. Дәл мәтіннің мазмұныды алу мүмкін талдау жалғастыра алу мүмкін.

Моноалфавиттық шифрлар біртума әліпбидің әріптерінің қолдануын жиіліктер оңай ашылып, өйткені мұра етеді. Контрмера бір әріп үшін қолдану осы жағдайда болып табылады, бір емес емес, (деп аталатын омофондар) бірнеше ауыстырғыш. Егер нышандардың сан болса. тағайындалған әріптер, бұл әріптің пайда болуын пропорционал жиілікке таңдау, онда шифрлалған мәтіндегі әріптердің қолдануды жиілігінің есептеуі мағнасыз болып қалыптасады. Мысалы, ашық мәтіндер тіпті бірақ әрбір элементке омофондарының қолдануында шифрлалған мәтіннің бір-ақ элементіне сәйкес келеді, сондықтан соңғы биграммалардың бірнеше әріптерінің комбинацияларының қайталауды жиілігінің тән көрсеткіштері бұрынғыша байқалуы керек. және криптоанализдың есептің нәтижесіндесін бұрынғыша болып қалады қарапайым жеткілікті.

Түпнұсқаның құрылымы алмастырулары әдістері арқылы кем айқындалды екі принципті әртүрлі жолдар қолдану мүмкін елеулі қолдану мүмкін шифрлалған мәтіну үшін. Солардың бірі емес, ашық мәтіннің жеке емес нышандары, бірнеше нышандардың комбинация емес, басқа жол бірнеше әліпбилердің шифрлауы үшін қолдану ойлағанында орнын басуда болады.

Плейфейер шифры.

Көп әріпті шифрлауын әдіс негізделетін өте белгілі шифрлардың бірі ашық мәтіннің биграммасында шифрлалған мәтіннің тап қалған биграмма өзгертілетін дербес бірліктерді сияқты қаралатын (Playfair) Плейфейер шифры болып табылады.

Плейфейер алгоритмі кілттік сөздің негізде кейбір жасалған өлшемге әріптердің матрицасының қолдануында 5x5 негізделген. Матрица кілттік сөз қолданылған әріптердің орналастыруы солдан оңға және жоғарыдан төменге жолымен жасалады. Содан соң әліпбидің қалған әріптері қалған жолдардағы табиғи ретінде және матрица бағаналары жайласады. I және J әріптер ылғи бір әріптермен болып есептеледі. (монархия) monarchy сөзінің Ключевоесі үшін мұндай матрицаның мысалы төменде келтірілген.

Ашық мәтін келесі ережелермен сәйкес әріптің екі-екідені үлестермен шифрлайды.

1. Мысалы, егер ашық мәтіннің қайталанатын әріптерінің несі шифрлау үшін бір буды құрастырады екен болса, онда бұл әріптердің арасындағы X-шы арнайы әріп-толтырғыш қондырылады. Balloon қалай мұндай сөз жеке алғанда ba lx lo опның түріне өзгереді.
2. Егер ашық мәтіннің әріптері матрицаның сол жолдарын тигізсе, олардың әрқайсылары әріппен ауыстырылады, сол жолдаға келесі онда оңнан солға - матрицаның соңғы жолдың элементінің алмастыруы үшін жол бірінші элемент сол қызмет көрсететін шартпен сол. ARның жоғары салынған матрицасына сәйкес RMны сияқты шифрлайды.
3. Егер ашық мәтіннің әріптері матрицаның сол бағаналарын тигізсе, олардың әрқайсылары матрицаның өздің төменгі бағана элементінің алмастыруы үшін бағана элемент сол ең жоғарғы алатын шартпен сол ол астында сол бағанада бірден тұратын әріппен ауыстырылады. MU мысалда жоғары сияқты шифрлайды қара.
4. Егер келтірілген шарттардың бір болса, ашық мәтіннің әріптерінің булары әрбір әрібі матрица және ашық мәтіннің екінші әрібінде болатын бағананың бұл әріп болатын жолының қиылысу болатын әріппен ауыстырылады. Мысалы. HS BPны сияқты шифрлайды. (немесе JM, шифрлаушы өз тілегімен).

Алфавиттық шифрлардың дәуір сенімдірек бос тұруларын Плейфейер шифры. Бір жағынан, әріптер жинағы 26. биграммалар - 26x26 = 676. сондықтан және одан тарлау биграмманы белгіленсін жеке әріпке қарағанда күрделірек. Басқа жағынан, жеке әріптердің пайда болуын салыстырмалы жиілік биграммалардың пайда болуын жиілікке қарағанда кең диапазоннан астам анағұрлым толқиды. бұл себептендерге қолдануды жиіліктің ол да өйткені күрделірек талдауының биграммаларының қолдануды жиілігінің талдауы сондықтан әріп Плейфейер шифры мүмкін емес сындыратынын. Ол уақытында бірінші әлемдік соғыстың Британдық Миясындағы шифрлауын стандартпен қызмет көрсетеді және екінші әлемдік соғыстың мерзіміне тіпті АҚШтың әскерінде және одақты әскерлерді жиі қолданылды.

Хилл шифры.

Тағы бір қызықты көп әріпті шифры 1929 жылдағы (Lester Hill) Хиллмен шифр, Лестердің игерілген математигімен болып табылады. Жататын алгоритмды оның негізінде m ашық мәтіннің біртіндеп әріптерінің әрбір шифрлалған мәтіннің әріптерімен алмастырады. Алмастыру әрбір нышан сызықты теңдеулермен анықталады санмен көрсетілген мән(A=0, B=1,..., Z=25) тағайындайды. Мысалы, а m= 3 жанында теңдеулердің келесі жүйесін аламыз:

$$C, = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \mod 26.$$
$$C_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \mod 26.$$
$$C_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p3) \mod 26.$$

Бұл жүйені вектордың шығармасы және матрицаның түрінде келесі жазып алуға болады түр:

Немесе:

$$C = KxP,$$

қайда және P - ұзындықтың векторлары 3. сәйкесінше сәйкесінше шифрлалған және ашық мәтін, - бұл 3x3-ші өлшемнің матрицасы, ұсынатын шифрлаудың кілті ұсынатын. Операциялар модул бойынша 26 орындалады.

Хилл жүйені түрде келесі формада жазып алуға болады:

$$C = E_K(P) = KP$$
$$P = D_K(C) = K^{-1}C=P$$

Сонымен қатар Плейфейер шифрдың жағдайында Хилланың шифрының артықшылығы сол тұрады. шифрдағы матрицаның өлшемі көбірек болған сайын не оны Хилланың шифры үшін кіруді жиілікті жеке әріп толық маскировка жасайды, шифрлалған мәтінде көбірек сол нышандардың басқа комбинацияларының пайда болуды жиілігі мәндеріндегі айырмашылықтар туралы мәлімет көзден таса болады. Осылай, 3x3-ші матрицасы бар Хилла шифр жеке әріптерғана емес, екі әріпті комбинациялар да пайда болуды жиілікті қашыртады.

Полиалфавиттық шифрлар. Инженердің шифры.

Алфавиттық шрифттың бос тұруын жетілдіруді басқа мүмкіндік ашық мәтін шифрлау барысында нақтылы шарттарға байланысты қолданылатын бірнеше алфавиттық алмастыруларды қолдануда болады. Мұндай шифрлаудың әдістерінің қолдану негізделген шрифттердің үй-ішісі шифрлармен полиалфавитными деп аталады. Шифрлаудың ұқсас әдістері келесі ортақ қасиеттермен ие болады.

1. Сабақтас алфавиттық алмастыруларды жиынды қолданылады.
2. Бойынша нақты анықталатын кейбір кілт болады

өрнектеу шифрлау үшін осы кезеңде қолданылуы керек.

Бәріне белгілі және бір уақытта ең оңай алгоритмынан өзі деп сондай (епиге л) Виженер шифры болып табылады. Бұл шифр жылжуы бар цезарьнің 26 шифрларымен (латынша әліпби үшін) 0 мен 25пен аралығындағы көрсетілген моно алфавиттық алмастырулардың ережелерінің жиынында негізделеді. Мұндай шифрлардың әрбірі ашық мәтін тиісті әріп

шифрлалған мәтіннің әріп болатын маңызды әріппен белгілеуге болады. Мысалы, жылжу үшін 3 тең цезарьнің шифры. Оның маңызды әрібімен белгі қояды.

Түсіну және бұл схеманың қолдануының жеңілдіктері үшін Виженер көрсеткіш тақта аталған матрица ұсыныс жасаған. Барлық 26 шифрлар барлық көлденең орналасады, және шифрлардың әрқайсылары шеткі бағанада сол жағында көрсетілген өз маңызды әрібіне сәйкес келеді. Әліпби, ашық мәтіннің тиісті әріптеріне, бірінші үстінде кестенің жолында болады. Шифрлауды процесс қарапайым - л* маңызды әріп бойынша және қасында ашық мәтіннің әрібіне холардың жолының қиылысуында және бағанада болатын шифрлалған мәтіннің әрібін табуға керек.қасында - осы жағдайда мұндай әріп V-шы әріп болып табылады.

Қатынас не ұзындықты тығызда болатын кілт өзі керек қатынасты шифрласын керегу үшін. Кілт әдетте қолайлы ұзындықтың жолын алыну үшін маңызды сөз рет қайталанатын керек сан болады.

Сонымен бірге мәтін жай ғана шифрды шешсін - кілттің әрібі жолды, шифрлалған мәтіннің бұл жол болатын әрібін анықтайды бағана, және кестенің бірінші жолында бағана бұны анықтайды ашық мәтіннің тиісті әрібінде болады.

Бұл шифрдың артықшылығы шифрлалған мәтіндегі ашық мәтіннің ылғи бір әрібінің ұсынысы үшін көп әр түрлі варианттарда болатын - сөздің Ключевоесінің қайталамайтын әріптерінің әрбіріне бір-бірден болғандығында. Сайып келгенде, керісінше қолдануын жиілігі әріп сипаттайтын мәлімет әдісі мәліметі арқылы дегенмен құрылымына шифрлалған ашық мәтінінің құрылымының ықпалын жабуға толық лажы болмауға көзден таса болады. Шифрдың сенімділігін жоғарылатылсын ұзындығы қатынастың ұзындығымен дәл келетін қолдану кілттер мәтіндік мінездемелер ашық мәтіннің тілінің үйреншікті мінездемелерінен барынша қисайтқан көмектеседі.

3.2. Орын ауыстыруларды қолдану

Әдістер барлық қарастырылған жоғары шифрлалған мәтіннің әр түрлі нышандарының ашық мәтіннің нышандарының орнын басуларында тұрақтанды. Өрнектеулердің принципті басқа сыныбы ашық мәтіннің әріптерінің орын ауыстыруларын қолдануда салу. Шифрлар орын ауыстырулар арқылы жасалған орны ауысатын шифрлармен деп атайды.

Баспалдақ шифр.

Мұндай шифрлардан қарапайым жәндіктері баспалдақ өрнектеуді пайдаланады содан соң ашық мәтін нақтылы (баспалдақтар) ұзындықтың бойлай көлбеген жолдары жазылған қорытушы көлденең жолма-жол салыстырылып оқылады.

Тік орын ауыстыруды шифр.

Криптоанализ үшін ерекше күрделіліктің баспалдағы шифрды ұсынбайды. Күрделі схемадан астамы бірдей ұзындықтың көлденең жолдарында және бағанаға бағананың мәтінінің келесі оқуы қатынастың мәтінінің жазуы ойлайды, бірақ орын-орнымен емес, бағаналардың кейбір

орын ауыстыруымен сәйкес. Сонымен бірге бағаналардың оқуын рет алгоритмды кілт болып қалыптасу. Бағаналар бойынша мәтіннің орын ауыстыруын сөйлемнің шифрлауын мысал төменде келтірілген»

Орны ауысатын шифрды өте оңай айырып тануға тұрып қал, ондағы әріп өйткені жиілікпен, ашық мәтіндегі не сол кездеседі. Мысалы, шифрдың талдауының бағаналарының орын ауыстыруымен шифрлаулары осы кәзір қарастырылған әдіс үшін орындасын жай ғана жеткілікті - матрицаның түріндегі шифрлалған мәтінді жазып алып және бағаналар үшін болуы мүмкін орын ауыстыруларды варианттар сұрыптауға керек.

Орны ауысатын шифры қорғал қалғанырақ шифрлау орын ауыстыруларды қолданып әлденеше орындап айтарлықтай жасауға болады.

Бұрылатын кереге шифр.

Бұрылатын кереге деп аталатын шифрдың қолданулары үшін 2/7 торшалардың олары 2 т өлшемді торлы қағаздың тік төртбұрышты парағынан трафаретінен өндіріледі. Трафаретте оның ойықтары оның төрт болуы мүмкін әдістермен сол мөлшердені таза қағаз парағына салуда парақтың барлық аудандарын толық жабатынның торшаларының птың холары т ойған.

Қатынастың әріптері ретке төрт оның болуы мүмкін жағдайларыдан алдын ала белгіленгенге әрбірінің жанында (жолдарға, әрбір жолда бойынша солдан оңға) трафареттің ойықтарында дәйекті түрде сыяды.

Керегені дәл сондай болатын қатынастар алушы түпнұсқа еңбексіз төрт әдістермен орын-орныменге шифртекстке керегені салып оқиды.

Демек, керегенің шифрдың кілттерінің санның трафареттерінің саны, = 4, бұл шифр тды құрайды n = 4 ттің ұзындықтың қатынастары үшін арналған. Болуы мүмкін керегелер енді 8х8 сан трафареттің өлшемінде 4 миллиардты асып түседі.

Мазмұнға және ресімдеуге талаптар

Есептеу нәтижесі (25 шақты парақтар) түсініктемені тұрды және программалық бөлік.

Түсініктеме келесі бөлімдер болуы керек:

1. Тапсырма (вариантпен сәйкес).
2. Кәсіпорынның ақпараттық жүйесінің талдауы.
3. Кәсіпорынның 1 ұйымдық құрылымы.
4. Ақпараттық жүйенің схемасының 2 өңдеуі.
5. Кәсіпорынның ақпараттық қауіпсіздігінің жүйесінің өңдеуі.
6. Крифтографиялық қорғаудың жүйесінің өңдеуі.
7. Талдау және қорытындылар.
8. Қолданылған әдебиеттің тізімі.

Әдебиет тізімі

Негізгі әдебиет

1 Шеннон К. Теория связи в секретных системах/Сб.: «Работы по теории информации в кибернетике». – М.: Иностранная литература, 1963. – С.333-402

2 Диффи У., Хеллман Н.Э. Защищённость и помехостойкость. Введение в криптографию.//ТИИЭР, 1979.-Т.667.-N3.-С.71-109.

3 Симионс Г.Дж. Обзор методов аутентификации информации//ТИИЭР, 1988.-Т.76.-n5.-С.105-125.

4 Борсуков В. Бизнес и безопасность связи//Монитор Аспект, 1993.-N1.-С.56-62.

5 Герасименко В.А. Защита информации в автоматизированных системах. Ч. 1,2. М.: «Высшая школа», 1995.

Қосымша әдебиеттер

6 Законодательные акты РК в области защиты и безопасности информации.

7 Нормативные документы РК в области защиты и безопасности информации.

8 Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации.-М.: «Яхстмен»,1996.-71 с.

9 Хореев А.А. Способы и средства защиты информации. Учебное пособие.-М.: МО РФ, 2000.- 316 с.

10 Уолкер Б. Дж., Блек Я.Ф. Безопасность ЭВМ и организация их защиты: Пер. с англ.-М.: Связь. 1980.-112 с.