ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы

АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Басқару жүйелері және ақпараттық технологиялар институты

кафедрасы

«Қорғауға жіберілді»
Кафедра меңгерушісі
с.ғ.к., доцент Бердібаев Р. Ш.
(аты-жөні, ғылыми дәрежесі, атағы)
_____ «_____» _____ **20___ ж.**
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: Бір кезеңді модульмен көбейту құрылғысын әзірлеу

Ақпараттық қауіпсіздік жүйелері

мамандығы бойынша

Орындаған Әділбай Байәділ Айдарұлы СҮБк-14-1
(аты - жөні) (тобы)

Жетекші Тоғымбаев С.Т. доц. к.т.н.
(аты-жөні, ғылыми дәрежесі, атағы)
_____ «_____» _____ 20___ ж.
(қолы)

Кеңесшілер :

Экономикалық бөлім бойынша :
аға оқытушы Ғалым Р.Т.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «16» наурыз 20 18 ж.
(қолы)

Өмір тіршілігі қауіпсіздігі бойынша:
аға оқытушы Байзакова С.М.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «24» 05 20 18 ж.
(қолы)

Есептеу техникасын қолдану бойынша :
Тоғымбаев С.Т. доц. к.т.н
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____ 20___ ж.
(қолы)

Мөлшер бақылаушы:
Ширигунова Елена Александровна
(ғылыми дәрежесі, атағы, аты-жөні)
_____ « 1 » июня 20 18 ж.
(қолы)

Пікір жазушы : Капалова Нургуль Жарамаровна к.т.н.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ « 1 » июня 20 18 ж.
(қолы)

Алматы 2018

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы
АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Ғарыштық инженерия және телекоммуникациялар институты
Радиотехника, электроника және телекоммуникациялар мамандығы
Телекоммуникациялық желілер және жүйелер кафедрасы

жобаны орындауға берілген

ТАПСЫРМА

Студент Зілбай Байәріл Айдарұлы
(аты - жөні)

Жоба тақырыбы Бір кезеңді модульмен көбейту құрылғысы

ректордың «23» 10.2017 №155 бұйрығы бойынша бекітілген.

Аяқталған жұмысты тапсыру мерзімі: «5» маусым 2018 ж.

Жобаға бастапқы деректер (талап етілетін жоба нәтижелерінің параметрлері және нысанның бастапқы деректері)

Шифрлеу құрылғысының тиімділігін, тұрақтылығын, бағдарламалық шифрлеу әдісіне қарағанда, жұмысын тез істейтіндігін қарап дәлелденген. Есептеулермен блок құрылымын көрсетіліп қарастырылған.

Диплом жобасындағы әзірленуі тиіс сұрақтар тізімі немесе диплом жобасының қысқаша мазмұны:

1. Сандарды модульмен көбейту әдісінің құрылғы жүзінде іске асыру
2. Конвейр әдісімен сандардың модульмен көбейту, бұл жағдайда көбейту үшін разрядты көбейткіштерден басталады.
3. Модульмен толық көбейткіштің көптірілмейтін толық матрицалық құрылымы

Сызба материалдарының (міндетті түрде дайындалатын сызуларды көрсету) тізімі:

Сурет 2.1 – функционалдық құрылымдағы модульмен көбейту және де сол жолдағы бір санмен ауыстыру арқылы құрылғы модулінің функционалдық схемасы көрсетілген.
Сурет 2.2 – СМІ құрылымы
Сурет 2.3 – ФКО құрылымы
Сурет 2.3 – 2

Негізгі ұсынылатын әдебиеттер

1. Тынымбаев С.Т. Мырзабекова К.К. Синтез умножителей с повышенной разрядностью на множительно-суммирующих блоках
2. Методы дискретной математики в криптологии.
3. «Digital asymmetric encryption» M. Bellare
4. «Digital signatures with RSA and other public-key cryptosystems»

Жоба бойынша бөлімшелерге қатысты белгіленген кеңесшілер

бөлімшелер	кеңесші	мерзімі	қолы
Экономика	Касым Р.Т.	16.05.18	[signature]
ӨТ. К.	Байзакова С.М	24.05.18	[signature]
Техниканың бөлім	Тынымбаев С.Т.	24.05.18	[signature]

диплом жобасын дайындау

КЕСТЕСІ

№ р/с	Тарау аттары, әзірленетін сұрақтардың тізімі	Жетекшіге ұсыну мерзімдері	Ескерту
1	криптографияның әдістеріне	01.04.18	
	шолу, түрлерін таңдау		
2.	Жинақты көбейту алгоритмдерін	17.04.18	
	таңдау, кілттің тиімдісін таңдау		
3	модуль бойынша сан көтеру	01.05.18	
	әдістерін қарастыру		
4	Тіршілік қауіпсіздігі	20.05.18	
5	Экономика	03.06.18	

Тапсырманың берілген уақыты «______»___________________20___ж.

Кафедра меңгерушісі ____________ с.ғ.к., доцент Бердібаев Р. Ш.

(қолы) (аты-жөні, ғылыми дәрежесі, атағы)

Жоба жетекшісі __________ Ташимбаев С.Т. доц. к.т.н.

(қолы) (аты-жөні, ғылыми дәрежесі, атағы)

Орындалатын тапсырманы қабылдаған студент __________ Әділбай Байәділ Айдарұлы

(қолы) (аты -жөні)

Андатпа

Бұл дипломдық жобада шифрлеу құрылғысының тиімділігі, тұрақтылығы,бағдарламалық шфрлеу әдісіне қарағанда неғұрлым тез істейдінділігі қаралып дәлелденген. Жобада есептеулермен блок құрылымы көрсетіліп қарастырылған. Осы күнгез аман талабына сай жана, тез істейтін құрылғы болып табылады.

Дипломдық жобада экономикалық және еңбек қауіпсіздігі есептеулері жүргізілді. Экономикалық есептеулер, құрылғының шығыны мен пайдасы есептелінді. Еңбек қауіпсіздігінде өмір қауісіздігі мен жұмыс істеуге қолайлы жағдайын жасау шаралары жүргізілді.

Аннотация

Данный дипломный проект расматривает эффкутивность аппарата по шифрованию и его стойкости, сравнив с программным шифрованием аппарат работает намного быстрее, чтобы доказать то что аппарат эффективнее были привеедены примеры по расчетам и блок схемы. Чтобы быть в ногу со временем был придуман этот метод и задуман аппарат который будет актуален.

Данный дипломный проект рассматривает экономическую часть так же меры охраны труда. В экономической части были расчитаны расходы на аппарат и доход после его реализации. Чтобы создать условия работы и меры безопасности были проведены расчеты.

Annotation

This diploma work examines the efficiency of the device by encryption and its durability, comparing with software encryption, the device works much faster to prove that the device was more efficient, there were examples of calculations and block diagrams. To be in step with the times this method was invented and the device that will be relevant is planned.

This diploma project considers the economic part of the same labor protection measures. In the economic part, the expenses for the apparatus and the income after its realization were calculated. To create working conditions and security measures, calculations were made.

Мазмұны

Кіріспе

Құпиясыз мемлекет болуы мүмкін емес. Құпиялар ғылымның, техниканың және саясаттың негізін құрайды. Бірнеше ғасыр бұрын ойлап табылған жазудың жалпы қол жеткізерлік қасиеті бар. Хабар алушыға байланысты бұл қасиетті пайдалы немесе зиянды деп қарауға болады. Жазумен қатар құпия хат (грек тілінде криптография) дамиды. Құпия хат хабардың мағынасын адамдардан жасыруға және оны тек белгілі бір ғана тұлғалар қол жеткізе аларлықтай істеуге арналған. Кез келген қоғам ақпарат өндірмей, жинақтамай және айырбастамай дами алмайды. Нақтылы ақпарат арналған адамдар шеңберіне шек қою қажеттілігі әрқашанда болған. Сондықтан, ақпарат арналмаған адамдардан хабарды жасыру тәсілдері туралы ғылым, яғни криптография пайда болған.

Соған орай шифрлеу құралы үлкен мүмкіндіктер береді тез ары тұрақты, үлкен мөлшерде өңдеу операциаларын жүргізе алад. Құрылғы:

- жұмыс өңімділігінің нығайтады.
- крипто тұрақтылығы мықты.
- шифрлеу жылдамдығының артуы .
- неғұрлым көп мөлшерде ақпаратты өңдеу.
- құрылғы сенімділігі.

Осы сапаларына қарап құрылғы үлкен мүмкіндіктерге ие екендігін көрсе болады.

1 Криптология тарихы және бүгінгісі

1.1 Шифрлардың пайда болуы

Ежелден бері біз кейбір шифрлау жүйелеріне келдік. Олар төртінші мыңжылдықта дүниеге келді. Құпия хат-хабар әдісі Египет, Шумер, Қытай секілді ежелгі қоғамдарда өздігінен ойлап табылды. Рәміздер Бабыл мен Ассирияда белгілі болған, ал ежелгі мысырлықтар (мысырлықтар) кемінде үш криптографиялық жүйені қолданған.

Ежелгі Үндістан, Египет және Месопотамиядағы ежелгі өркениеттердің тарихи құжаттары шифрланған жазу жүйелері мен әдістер туралы ақпаратты қамтиды. Ежелгі үнді қолжазбаларында мәтінді түрлендірудің 64 жолы бар. Қолжазбалар ерікті, белгілі бір ережелерге сәйкес жазылған. Осы әдістердің көпшілігі шифрлау деп санауға болады. Криптографиялық жүйелерді пайдалану туралы ең дәл деректер ежелгі грек мемлекеттерінің дәуірі болып табылады. Бұл дәуірде кодтауды қолдануда әкімшілер мен діни органдар болды.

Араб елдерінің гүлдену дәуірінде (б.э.д. 8 ғасыр) дәуірінде шифрлау дамудың жаңа артықшылығын алды. «Шифрлау» және «Нөмір» араб сөздері. 855 жастағы «Ерте жазба еңбегі» атты кітабы криптографиялық жүйелердің сипаттамаларын сипаттайды. 1412 жылы 14 томдық энциклопедия Шейх әл-Кушан шығарған. Бұл энциклопедияда шифрлау бөлімі бар.Ол авторға барлық танымал шифрлау әдістерін қалай декодтау керектігін және ашық және кодталған мәтіннің жиіліктік қасиеттеріне негізделген шифрлау жүйесіндегі кодтарды талдауды ұсынады. Энциклопедияның бұл бөлімі Қасиетті Құранның мәтініне негізделген оқу жиілігіне негізделген араб әріптерінің тізімін қамтиды.

Фонетикалық жазуды дамыту жалпы жазуды оңайлатуға ықпал етті. Екінші мыңжылдықта ежелгі семит алфавитінде бір-біріне жақын 30-ға жуық белгілер болған, мәтіндер қарапайым көлік құралдарымен кодталған. Алғашқы таңба орнына, алфавиттің соңғы таңбасы екінші таңбаның орнына - алдыңғы сипатта және екіншісінде теріледі. Бұл әдіс шақырылады

Келесі шифр ақпарат жіберуші мен қабалдаушыға мәлім белгілі бір ереже бойынша хабар әріптерінің орнын ауыстырумен байланысты. Біздің дәуірге дейін (б. д. д.) V-VI ғасырда (грек мемлекеттерінің бірі) Спартада дамыған криптография болған. Дәл осы уақытта шифрлауға арналған арнаулы таяқ (“сцитала”) пайда болған. Ол орын ауыстыру шифрында қолданылған. Сыртына таспа (папирус жапырағының тілімі) оратылатын таяқтың атына сәйкес бұл шифр сцитала деп аталған. Шифрлау алгоритмі мынадай: таяққа таспаны орайды және оралған таспаның үстінен таяқтың бойымен ашық мәтінді жазады. Оралған таспада шифромәтін жазылып шығады - ыңғайлы және жылдам. Шифрдың кілті - таяқтың жуандығы және әліпби.

Ежелгі грек ғалымы Аристотель (б. д. д. 384 – 322 ж.) криптографияда сцитала шифрын ашу тәсілінің авторы ретінде белгілі: таяқтың дәл диаметрін білмей-ақ, Аристотель конус тәрізді таяққа шифрланған таспаны ораған және мәтін дұрыс оқылып басталғанша таспаны таяқ бойында әрлі-берлі жылжытқан.

Ежелгі грек тарихшысы, Polybium (шамамен 200-120 BC) немесе Polybid Squar келесі шифрлеу алгоритмі болған. 5 × 5 шаршы ұяшық грек алфавитінің таңбаларына толтырылған (9-сурет). Шифрлау кілті квадрат толтыру тәртібі болып табылады. Бұл қораптар заманауи шифрлау жүйелерінде кеңінен қолданылады.

Гай Юлий Цезарьдың (б. д. д. 102 немесе 100-44 ж.) шифры қарапайым ауыстыру шифрының бір түрі болып келеді және мына алгоритмге сәйкес құрылған: бірінші әріптің орнына төртінші әріпті оқу керек (3-кесте). Шифрдың кілті – ығыстыру аралығы және әліпбидің өзі. 26 әріптен тұратын әліпбиде Цезарь шифрын қолданғанда VENI VIDI VICI (келдім, көрдім, жеңдім) ашық мәтінінен YHQL YLGL YLFL шифрмәтіні алынады.

Шифрлауға арналған құралдар ертедегі заманда да бар болған. Мәселен, б. д. д. V ғасырда Спарта мемлекетінде құпия әскери байланыс жүйесі болған. Бірінші криптографиялық құрылғы (сцитала) көмегімен олар, қарапайым ауыстыру әдісін қолдана отырып, хабарларды шифрлаған. Б д. д. IV ғасырда римдіктер шифрлау процедурасын оңайлату үшін шифрлауыш тегеріштерді қолдана бастаған.

1.1 Криптология ғылымының қалыптасуы

Рим империясының құлағаннан кейін, Еуропадағы жағдай құлады. Мен өркениеттің үздік жетістіктерін, шифрлаумен қатар, жоғалттым. Орта ғасырдың соңында ғана кодтау қайта пайдаланылады. Ерте кодтау тәжірибесі қалпына келтіріледі және олардың бір тобы одан әрі дамиды.

Сол кездің қол шифрларында кестелер жиі қолданылады. Олардың көмегімен хабардағы әріптердің орнын ауыстырудың қарапайым шифрлауыш процедуралары жүзеге асырылады. Кілт ретінде кесте өлшемі, орын ауыстыруды көрсететін сөйлем немесе кестелердің арнайы ерекшелігі қолданылды. Жалғыздалған кілтсіз орын ауыстыру - ең қарапайым шифрлау әдістерінің бірі. Жалғыздалған орын ауыстыру шифрының алгоритмі сцитала шифрының алгоритміне ұқсас, тек қана ашық мәтін көлденең емес, кестеге тігінен жазылады (10-сурет). Шифрдың кілті ретінде кестенің өлшемі алынады. Мәселен, КОМПЬЮТЕРЛІК ЖҮЙЕЛЕРДІ ҚОРҒАУ КЕРЕК хабарын шифрлағаннан кейін КЬРЖЛІҒЕ ОЮЛҮЕҚАР МТІЙРОУЕ ПЕКЕДРКК шифрмәтіні алынады.

Шифрлау үшін, кілт сөз кестенің бірінші жолына қосылады және кілт сөздердің жүйелі сандарына сәйкес бағандарды ауыстырады. Бұл шифрлау әдісі бір кілтті беруді анықтайды (19-сурет). Мысалы, компьютерлік жүйелерді

тек шифрланған кілтпен шифрлағаннан кейін сіз LOGISTIC LOGISTICS шифрлауының DEPECRACY қабылданады.

Қосымша шифрлау үшін шифрланған хабарламаны қайтадан шифрлай аласыз. Бұл тәсіл қосарланған ауысым деп аталады. Бірінші кестеде бағандар ауыстырылады, ал екінші кесте жолдарында жолдар бар (сурет 20). Бірақ қос кодталған шифрлау - бұл өте жеңіл шифрлау түрі, ол оқуға оңай.

Орта ғасыр ғалымдары қатарлар және бағандар (және әрбір диагональ) бойынша саналған сандардың сомасы бір мәнге тең болып келген квадраттардың сиқыршылық күші бар есептеген. Олар осындай сиқырлы квадраттарды деректерді шифрлау үшін пайдаланған (20-сурет). АҚПАРАТ ҚОРҒАУ мәтінін 4х4 сиқырлы квадратпен шифрлау нәтижесінде ААРРҚ ОПАҚУ ҒАЫТТ шифрмәтіні алынған. Бір қарағанда сиқырлы квадраттар саны өте аз сияқты. Бірақ олардың саны квадрат өлшемі артуымен өте жылдам өседі. Мәселен, 3х3 өлшемді кестеде бір сиқырлы квадрат бар, 4х4 өлшемді кестеде - 880, 5х5 өлшемді кестеде - 25000. Кілттердің мүмкін болатын барлық варианттарын жеңіл сұрыптап шығуға болатындықтан бұл шифрлау алгоритмін сәтті деп айтуға болмайды. Бірақ үлкен өлшемді сиқырлы квадраттардың барлық кілттерін қолмен есептеу шығу, әрине, өте қиын.

Орта ғасырларда сауданың кеңінен дамуы ерекше шифрларды талап етті. Мысалы, келу датасын немесе тауар бағасын керекті адамдарға білдіру үшін көпестер пайдалана алатындай өте қарапайым және ыңғайлы шифрлар қажет болды. Кілттік сөз негізінде құрылған мұндай қарапайым шифрлар цифрларды әріптерге ауыстыру деп аталады. Шынында, бұлар – кодалар (шифрлар емес), бірақ бір кезде белгісіз кодалау кестесімен қолданылған кода өз қасиеттері бойынша шифрға ұқсас болады. Саудагерлер алдын ала әріптері цифрларға сәйкес келетін ортақ кілттік сөзді қолдануға келіскен. Мәселен, МАДӘНКЕПІЛ кілті үшін 0 цифры М әрпін білдіреді, 1 цифры А әрпін білдіреді, 2 цифры Д әрпін білдіреді және тағысын тағыда. Абонент ДӘМЕЛІ КЕЛЕДІ хабарын алып оны 23/06/98 КЕЛЕДІ деп түсінеді.

Гронсфельд шифры (1734 жылы бельгиялық Хосе де Бронкхор, граф де Гронсфельд жасаған) Цезарь шифрының өзгертілген бір түрі болып келеді. Бұл алгоритмде ығыстыру аралығы тұрақты сан арқылы емес, кілт (гамма) арқылы беріледі. Шифрмәтін құру үшін ашық мәтін әрпісінің орнына әліпбидің кілт цифрына жылжытылған әрпі таңдап алынады (4-кесте). Мәселен, ҰЛЫ ЖІБЕК ЖОЛЫ мәтіні 2718 кілті арқылы ФРІ НЭЗЖП ИҰМБ болып шифрланады. Осындай шифрлау тәсілі қысқа периодтық гамма деп те аталады. Гронсфельд шифрының (мысалы, шифрқұжаттың мәтінін басқа әліпби әріптерімен жазу, әр түрлі кілттермен екі рет шифрлау сияқты) бірнеше түрі бар.

Бұл шифрлардан басқа көбінесе қарапайым ауыстыру шифры қолданылған. Мұнда хабардың әрбір әрпі шифрдың оған сәйкес әрпімен ауыстырылады. Мұндай шифр қарапайым кода болып келеді және шифрқұжаттың ұзындығы 20-30 әріп болғанда оны ашу мүмкіндігі пайда болады, ал 100 артық символы бар мәтін өте қарапайым есеп болып табылады.

Күрделі ауыстыру шифрлары көпәліпбилік деп аталады, себебі негізгі хабардың әрбір символын шифрлау үшін өзінің қарапайым ауыстыру шифры қолданылады. Көпәліпбилік ауыстыру шифрын итальян ғалымы Леон Батист Альберти (1404-1472) ұсынған. Оның 1466 жылы жазылған “Шифр туралы трактат” кітабы криптология саласындағы (араб қолжазбаларын есептемегенде) әлемдегі бірінші ғылыми еңбек болып саналады. Бұл кітапта әр түрлі шифрлау тәсілдері қарастырылған. Олардың ішінде ашық мәтінді кейбір қосалқы мәтінде жасыру әдісі де бар. Криптологиядағы Альбертидің негізгі жетістігі - шифрқұжаттың ашуға беріктілігін арттыруға мүмкіндік берген көпәліпбилік ауыстыру шифрын ойлап табу. Ол шифрдан басқа оны жүзеге асыруға арналған айналатын доңғалақтардан тұратын құрылғыны (шифрлайтын тегерішті) толық сипаттап берген. Шифрлау алгоритмінің мәні кілтке сәйкес бірнеше ауыстыруды қолдану болып табылады. Кейінірек Альберти қайта шифрлау кодасын ойлап тапты. Мұндай шифр Еуропа елдерінде тек 400 жыл өткен соң ғана қолданыла басталған.

Бұл шифрлау кестесі (кейде Wigener кестесі деп аталады). Блейз Виньен (1523-1596) француздық дипломат болып табылады, ол шифрлау жүйесін жетілдіреді. Айналдыру кестесінің әр жолы - Y белгісімен толтырылған алфавит. Цезарь коды сияқты ауыстыру белгілерінің біріне сәйкес келеді (14-сурет). Ақпарат шифрлау үшін ашық мәтіннің әрбір әрібінің астына кілттің әріптері жазылады. Одан кейін ашық мәтіннің әрпіне сәйкес келетін бағанмен кілттің әрпіне сәйкес келетін қатардың қиылысындағы символ табылады. Мұндай операция хабар мен кілт символдарының ASCII кодаларын белгілі бір модуль бойынша қосу болып табылады. Мәселен, ЕГЕМЕН ҚАЗАҚСТАН мәтінін ЖЕРҰЙЫҚ кілті көмегімен шифрлағанда МЙХЯОИҮЖНРЭЩҢҚУ мәтіні алынады (15-сурет). Виженер шифры 400 жыл бойы кері шифрланбайтын шифр деп саналған, сондықтан әскери шифр ретінде кеңінен қолданылған.Бұл кодтың түрі біздің күндерімізге жетті. Егер кесте күрделі болса (мысалы, бір сөзден екінші сөзге дейін), шифрлау қауіпсіз болады. Бірақ бұл күрделі кестелер компьютерде жинақталуы керек. Көп деңгейлі кіру шифрлауы үшін кілттің ұзындығы мен күрделілігіне сену қажет. Шифрлау және кері кодтар жеңілдетілген, сондықтан құпия Viziner кестесін сақтаудың қажеті жоқ.1518 жылы Германияда баспадан криптография жайында бірінші кітап шықты. Иоганнес Трисемус өзінің “Полиграфия” деп аталатын кітабында бірталай шифрлар жайында мәлімет келтірген. Олардың біреуінде ол көпәліпбилік ауыстыру идеясын одан әрі дамытады. Сонымен қатар ол осы трактатта бірінші болып кездейсоқ ретте әліпбимен толтырылған шифрлауыш кестелерді қолдануды жүйелі түрде сипаттаған. Өлшемі 6х7 кестені қолдана отырып (11-сурет) АҚПАРАТТЫ ҚОРҒАУ мәтінін БҮРКІТ кілтінің көмегімен шифрлағаннан кейін ЖПЦЖГЖЕЕҮАПХГҚЖШ шифрмәтіні алынған. Шифрлау бір-бір әріп бойынша жүргізілетін болғандықтан мұндай кестелік шифрлар монограммалы шифрлар деп аталады. Трисемус бірінші болып бір уақытта екі-екі әріптен шифрлауға болатынын байқаған. Мұндай шифрлар

биграммалы деп аталады. Ең белгілі биграммалы шифрдың мысалы ретінде Плейфер шифрын келтіруге болады. Бұл шифрды Ұлыбритания бірінші дүниежүзілік соғыста қолданған. Биграммалар арқылы шифрлау шифрлардың ашуға беріктілігін күшейтті.

1553 жылы Италия «Belazo Sinyor's Encryption» атты кітабын шығарды. Ол «құпия сөз» деп аталатын сөзді немесе сөз тіркесін пайдалануды ұсынады. Қалыпты мәтін бойынша жазылған немесе жазылған. Құпия сөз құпия сөз үшін пайдаланылатын нөмірді білдіреді. 1563 жылы итальяндық Джованни Порта өзінің кітабында «Құпия хат» деген жұп алфавит негізінде Киелі кітап кодын шифрлауды сипаттайды.

Шамамен сол жылдары итальян математигі және философы Джераломо Кардано криптография жайында бірнеше кітап жазған және трафареттер әдісін сипаттап берген. Мысалы, 22-суретте 4х4 торымен шифрлау үрдісі көрсетілген. ЕГЕМЕН_ҚАЗАҚТАН мәтінін шифрлаған соң ЕСЕА ТНЗГ АЕА_ МҚҚН шифрмәтіні алынған. Мұндай торлардың саны олардың өлшеміне байланысты тез өседі: 2х2 торы жалғыз, 4х4 торы 256, ал 6х6 өлшемді торлардың саны жүз мыңнан асады. Тор тәріздес шифрлар жеңіл ашылатын болғандықтан олар дербес шифр түрінде қолданылмайды. Бірақ олар өте ыңғайлы және тәжірибе жүзінде ауыстыру шифрларын күшейту үшін ұзақ уақыт қолданылған.

XV және XVII ғасырларда криптографияны талдау және декодтау үшін математикалық негіз пайдаланылды. Шифрлау басты шифрлау құралы ретінде пайдаланылды. Сондықтан он сегізінші ғасырдың басында кодтау тәуелсіз ғылым түрінде дамыды. Дипломатия саласындағы кәсіби крифтологтар мен шифрлердің болуына және әскери мәселелерді жалғастыруға қарамастан, барлық дәйексөздер осы кезеңде аяқталмады, тек кейбір дарынды адамдар ғана қатысты.

Bigrampy (Playfair) кодтауды кодтау үшін мәтін ашық мәтінге (жұптық жұппен) бөлінеді, содан кейін кілтті кілтке сәйкес шифрлайды және белгілі бір ереже бойынша кодталады (11-сурет). PHR коды PINK шифрлау пернетақтасы арқылы шифрланады.

1894 жылы ағылшын Чарльз Уитстон “қос квадрат” деп аталатын биграммалармен шифрлаудың жаңа әдісін тапты. Бұл оқиға криптогрфиядағы жаңа бір кезеңнің ашылуы болып саналады. Полибий әдісінен айырмашылы - “қос квадратта” бір уақытта көлденең орналасқан екі кесте қолданылады, ал шифрлау Плейфер шифрындағы сияқты биграммалар арқылы жүргізіледі (16-сурет). Мәселен, БҮГІН ЖАҢБЫРЛЫ КҮН хабарын қазақ әліпбиінің сиволдары кездейсоқ орналасқан екі кестенің көмегімен шифрлағанда ІЧЕФСЕУЭИУШЕИАРЙУР шифрмәтіні алынған.

Бирамаллар көмегімен шифрлау өте жоғары және қарапайым шифрлауды қамтиды, ол сол кезде үлкен жетістікке жетеді. Қосарлы шаршы алаңды бұзу 30-дан астам сызықты қажет етеді.Шифрларды талдау мен жасауда математикалық әдістер баяғыдан бері қолданылса да тек XX ғасырдың

қырқыншы жылдарында қолданбалы математика дамуында болған сапалы серпіліс қана криптографияны ғылым ретінде қарауға мүмкіндік берді.

Криптографияның осы кезеңі тарихының аяқталуы математик Элвуд Шеннон атымен байланысты. Ол математикалық әдістермен шифрлаудың сенімділігін зерттеген. Осы зерттеулердің нәтижесі: символдардың кездейсоқ тізбегі ешқандай мәнді алып жүрмейді, ал ақпараттанудың криптологиямен байланысы шифрқұжаттың, кілттің және хабардың табылған статистикалық қасиеттерін хабарды кері шифрлау (яғни хабардың нақты мазмұнын табу) үшін қолдануға мүмкіндік береді.

Криптографияның дамуына ықпалын тигізген теориялық жаңалықтар американдық инженер К.Шеннонның “Құпия жүйелердегі байланыс теориясы” деп аталатын жұмысында және радиотехник-ғалым В. А. Котельниковтың “Автоматты түрде шифрлаудың негізгі қағидалары” деген жұмысында берілген болатын. Осы жұмыстарда шифр жүйесінің кері шифрланбауына қажетті және жеткілікті шарттар тұжырымдалған және дәлелденген болатын. Оларға сәйкес, дұшпанның шифрмәтінге ие болуы қолданылатын кілттердің ықтималдық-тарын өзгертпейді. Сонымен қатар мыналар анықталған: кері шифрланбайтын жалғыз-ақ шифр – ашық мәтінді сондай ұзындығы бар кездейсоқ кілт арқылы шифрлайтын (бір реттік пайдаланылатын таспа деп аталатын) шифр. Бірақ мұндай абсолютті берік шифрды қолдану өте қымбатқа түседі.

1.2 Шифрлау процесін автоматтандыру

1790 жылы Томас Джефферсон (АҚШ болашақ үшінші президенті) цифрлық шифрлауыш доңғалақ ойлап тапқан. Мұндай машиналардың жұмыс істеу ұстанымы арифмометрге өте ұқсас. Хабар мәтінін ұзын кілт арқылы көпәліпбилік ауыстыру әдісі қолданылған. Бұл машинада айналымдарының периодтары 13, 15, 17, 19 тең 4 доңғалақ болған. Қысқа хабарлардың кері шифрлауын өте қиындатқан .

1891 жылы Этьен Базери анағұрлым анайы құрал ұсынды - Базери цилиндрі. Ол құрсауына кездейсоқ түрде әліпби қондырылған 20 тегеріштен тұрған. Шифрлау алдында тегеріштер кілтке сәйкес анықталатын тәртіппен ортақ белағашқа орналастырылған. Мәтіннің алғашқы 20 әрпін цилиндрлерде бір қатарда теріп алған соң барлық цилиндрлерді бірге бұрған, одан кейін келесі қатардан шифрланған хабар оқылған. Ашық мәтіннің келесі 20 әрпі де осылайша шифрланған. Сөйтіп барлық хабар шифрланып біткенше үрдіс қайталанған.

1920 жылдары шифрлау және кері шифрлау үрдісін автоматтандыру үшін көптеген механикалық құрылғылар әзірленді. Олардың көпшілігі таза мәтінді енгізу үшін пернетақтадан және роторлардан тұрады. Роторлар - бұл қарапайым кілттері бар арнайы айналмалы дөңгелектер. Гильберт Верхам, тәжірибеде қолдануға арналған алғашқы координатор 1917 жылы ғана енгізілген.

Дүниежүзілік соғыстар аралығында барлық алдыңғы қатарлы елдерде электромеханикалық шифрлауыштар пайда болған. Олар коммутациялық

тегеріштер (немесе роторлар) және күпшекті тегеріштер негізінде жасалған. Шифрлауыштың бірінші түрінің мысалы ретінде ″Энигма” шифромашинасын, ал екіншісінің мысалы ретінде американдық М-209 шифромашинасын кетіруге болады [14].

1917 жылы Эдвард Хеберн ойлап тапқан роторлық машина қазіргі заманның криптографиялық машиналардың негізін салушысы деп саналады. Бұл машина кейінірек Энигма (немісше enigma – жұмбақ) деп аталатын болды. Екінші дүниежүзілік соғыс кезінде Германия өздерінің хабарларын құпиялау үшін ″Энигма” шифрлауышын қолданды. Алғашында бұл машина бір белағашта айналып тұратын 4 барабаннан құралған. Барабандардың ағымдағы жайы қарапайым ауыстыру шифрының миллионнан артық вариантын қамтамасыз еткен. Құпия кілт - барабандардың өзара бұрыштық орналасуы және олардағы мәліметтер. Барабанның әрбір жағында (әлипбидегі әріптер санына сәйкес) 25 түйіспе орналасқан. Түйіспелер барабанның екі жағынан екі-екіден кездейсоқ түрде 25 сыммен қосылған. Жұмыс істеп бастар алдында барабандарға кілттік сөз орналастырылған, ал перне басылған және кезекті символды кодалаған кезде оң жақтағы барабан бір адымға бұрылған. Ол толық айналым жасаған соң, келесі барабан бір адымға бұрылған. Сонымен хабар мәтінінің өлшеміне қарағанда ұзындығы үлкен кілт қалыптастырылады. Кері шифрлауды қиындату үшін күннен күнге барабандардың орындарын ауыстырып немесе барабанды алмастырып тұрған. Машинаны одан әрі жетілдіру үшін барабандардың санын алдымен 5-ке, ал сонан соң 6-ға дейін көбейтілген. Машинаның барлық құрылғысы бір портфельге сыятын болған.

1942 жылы көптеген компьютерлерді Алан Тьюринг жасағанға дейін Enigma нөлдерін бұзу қиынға соқты. Бұл әлемдегі алғашқы компьютер, «Жабык» деп аталатын, нөлдерді бұрмалайтын маман.

Американдық М-209 шифромашинасы өлшемі 26, 25, 23, 21, 19 және 17-ге тең алты доңғалақтан құралған. Олардың әрқайсысында шеңбер бойынша шығыңқы жерлер (күпшектер) орналасқан. Осындай шошақтардың алтыөлшемдік қисындасуы (олардың саны - 64) механикалық құрылғының көмегімен санға айналдырылған. Ашық мәтіннің әрпі осы санға ығыстырылған. Тегеріштердің бұрыштық қалпын өзгерту оларды біркелкі айналдыру арқылы жүзеге асырылған. Осылайша шифрлауыш гаммалау шифрын іске асырған.

Бұрынғы Кеңес Одағы шифромашиналардың екі түрін де өндірген, ал жапондар (“қара қошқыл жәшік” деп аталатын) үш доңғалақты шифромашинаны қолданған.

XX ғасырдағы электрондық-есептеу машиналар шифрларға және оларды кері шифрлауға деген көзқарасты толық өзгертуге мәжбүр етті. Өз құпияларын қорғауды тілеушілер бұрын армандамаған мүмкіншіліктерге ие болды, ал қаскөйлердің қарамағында бөтен құпияларға енуге арналған құралдар пайда болды.

1.3 Криптография және криптоанализ

Дипломатиялық, әскери және өнеркәсіптік құпиялар әдетте шифрланған түрде жіберіледі немесе сақталады. Бұл құпия хат пен шифрдан айырмашылығы: хабардың жасырылғаны және парольдер ашық түрде жіберілуі және олардың мазмұны тек жасырын.

Криптографиялық түрлендіру арқылы құпия хабарларды тасымалдаудың классикалық сұлбасы мынадай. Жіберуші жақта хабар белгілі бір кілт арқасында шифрланады, одан кейін осылайша даярланған шифрқұжат қабылдаушыға ашық байланыс арнасымен тасымалданады, ал кілт болса (құпиялыққа кепілдік беретін) жабық арнамен жіберіледі. Қабылдаушы жақ өзіне белгілі кілт арқылы шифрқұжатты кері шифрлайды. Сөйтіп, келген хабарды бастапқы қалпына келтіреді. Құпиялау мақсатына байланысты бұл сұлба біршама өзгертілуі мүмкін.

Шифрлау түрлендіру ақпараттық қорғауда екі мақсатты көздейді. Алдымен, кілттері бар адамдар ақпаратқа қол жеткізе алмайтындығына көз жеткізіңіз, Екіншіден, негізсіз бұрмалаумен (рұқсат етілмеген) дұрыс ақпаратты табыңыз.

Ақпарат қорғаудың басқа әдістерімен салыстырғанда классикалық криптография тек мынадай шарттар орындалғанда ғана қорғанышқа кепілдік береді:

- тиімді криптографиялық алгоритм қолданылған;
- кілттің құпиялылығы және тұтастылығы сақталған.

Криптология ақпаратты түрлендіру арқылы оны қорғаумен шұғылданады. Криптология ғылымы ақпаратты шифрлау және кері шифрлау, сондай-ақ, шифрларды әзірлеу, шифрды ашу мәселелерімен шұғылданады. Криптология kryptos (құпия) және logos (ғылым, ой) деген грек сөздерінен шыққан. Оны шартты түрде криптография және криптоанализ деп екі бағытқа бөлуге болады. Бұл екі бағыттың мақсаттары қарама-қарсы.

Криптография (cryptographic) ақпаратты заңсыз пайданаушылардан қорғау мақсатымен оны түрлендіру әдістері жайындағы ғылым. Ол ақпаратты оқу (бұрынғы қалпына келтіру) тек оның кілтін білген кезде ғана мүмкін болатындай етіп түрлендіреді. Криптография ақпаратты түрлендірудің математикалық әдістерін іздеумен және зерттеумен, яғни, жасырын деректерді шифрлаумен және кері шифрлаумен шұғылданады. Сонымен қатар, криптография ақпарат бұрмалаудың алдын алу немесе оның пайда болу себебін растау үшін де қолданылады. Өзге адамдардан ақпараттың құпиясын сақтап қалу криптографияның негізгі мақсаты болып табылады. Ақпаратпен заңсыз таныспақшы болған адамдарды қаскөйлер (қаскүнемдер) деп атайды.

Криптоанализ (криптоталдау) көбінесе шифрқұжатты оның кілтін білмей-ақ қалайша кері шифрлау керек мәселесімен және, кей кезде, қолданылып жүрген шифрлау жүйесін бұзып-ашумен айналысады. Сонымен, криптоанализ шифрланған хабардың бастапқы ашық мәтініне қол жеткізуге

бағытталған. Сәтті жүргізілген криптоаналитикалық зерттеулер негізінде хабардың бастапқы ашық мәтінімен қатар оның кілтін де ашуға болады. Криптоаналитик шифрланған хабарды, немесе кілтті, немесе екеуінде оқуға мүмкіндік беретін криптожүйенің осал жерлерін іздеумен шұғылданады. Сонымен, криптоаналитик деп шифрды ашу мүмкіндігін зерттейтін адамды атайды. Шет елде олар өздерін кодаларды бұзып-ашушылар (breaker), шабуылшылар (attacker) және ұрылар (sneaker) деп те атайды. Криптоанализ әрекеті шабуыл деп, ал табысты аяқталған криптоаналитикалық шабуыл бұзу-ашу немесе ашу деп аталады.

Сонымен, криптографтар құпиялықты қамсыздандыруға, ал криптоаналитиктер оны бұзуға-ашуға ұмтылады.

Криптографиялық жүйе (криптожүйе) – шифрлау алгоритмі, сондай-ақ, алуан түрлі кілттердің, ашық және шифрланған мәтіндердің жиынтығы.

Шифрлау алгоритмі (шифрлау немесе шифрлау алгоритмі) шифрлауды және шифрлауды шифрлау үшін қолданылатын есептеу функциясын білдіреді. Дәлірек айтқанда, бұл функция біреуі үшін: екіншісі шифрлау, ал екіншісі шифрлау үшін.

Криптографияда K әрібімен белгіленетін кілт қолданылады. Кілт (key) – ақпаратты шифрлау және кері шифрлау, сондай-ақ, оған қол қою үшін арналған цифрлық кода. Ол барлық мүмкін варианттардан криптографиялық түрлендіру алгоритмі үшін тек бір вариантты таңдауды қамтамасыз етеді. Кілттің ортақ, жеке меншік және құпия деп аталатын түрлері болады.

Шифрлау E функциясы да, кері шифрлау D функциясы осы кілтке тәуелді болады:

$$E_K(P) = C,\ D_K(C) = P. \qquad (1.9)$$

Сонда мына тепе-тендік әділ болады: $D_K(E_K(P)) = P$.

Бұл жерде, P (plaintext) - ашық мәтін, ал C (ciplertext) - E функциясы мен K кілті арқылы шифрланған мәтін (шифромәтін).

Шифр (cipher) – қаскөйде мәлімет (құпия ашу кілті) болмаған жағдайда, ашық ақпаратты бастапқы қалпына келтіре алмайтындай етіп түрлендіру үшін қолданылатын шартты белгілер тізбегі. “Шифр” терминінің түбірі араб сөзінен шыққан. XV ғасырдың басында жарық көрген *“Шауба Әл-Аша”* деп аталатын араб энциклопедиясында шифрлар жайында арнаулы бөлім болған.

Шифрлаудың шифрлау кодының басты ерекшелігі. Белгісіз кілт кезінде шифрлау күшін анықтайды (яғни криптоанализ). Бұл сипаттама әдетте кодты декодтау үшін қажетті уақытты анықтайды. Классикалық криптографияның негізін қалаушы Клод Шеннон төзімділіктің екі түрін көрсетеді: теориялық және практикалық.

Шифрланған хабарларда кездейсоқтықтарды зерттеу олардың криптоберіктілігін анықтау үшін өте маңызды. Криптограммада статистикалық заңдылықтар мен корреляциялардың болуы критоанализді жеңілдететінін

белгілі. Криптоберіктілікті жоғарылату үшін криптограмманың үлестірім заңын мүмкіндігінше бірқалыптыққа жақындату керек.

Шифрлау (ciphering, encryption) - белгілі бір адамнан басқалар оқи алмайтындай етіліп ақпаратты математикалық, алгоритмдік (криптографиялық) түрлендіру әдісі. Қабылдаушы жақ бұл ақпаратты дұрыс оқу үшін оны кері шифрлауы (decryption) керек. Шифрлау бөлшекті (әрбір кезекті бөлшек тәуелсіз шифрланады) және ағынды (әрбір таңба бір-бірінен тәуелсіз шифрланады) түрде жүргізілуі мүмкін.

Кейбір дәстүрлі шифрлар өздерінің белгілі бір артықшылықтарына байланысты әлге дейін қолданылып жүр. Орын ауыстыру шифрында ашық мәтіннің барлық әріптері өзгеріссіз қалады, тек олардың ашық мәтіндегі орындары ғана ауыстырылады. Анаграмма (дыбыстардың орнын ауыстыру арқылы сөздердің мағынасын өзгерту) - орын ауыстыру шифры. Ауыстыру шифрында, керісінше, шифрқұжатта әріптердің орны өзгеріссіз қалады (ашық мәтіндегі сияқты), бірақ символдары ауыстырылады. Осы екі шифрдың қисындасуы практикада қолданылатын классикалық шифрлардың әр алуан түрін береді.

Криптографиялық техникаға шифрлау және кері шифрлау алгоритмдерінен басқа құпия кілттер де жатады. Кілттерді қол жетпестей ету үшін, ал олардың оқылғанын белгілі ету үшін әр түрлі айлалар қолданылады. Кілттерді криптографиялық қойын дәптерлерде (блокноттарда) сақтайды. Көбінесе қойын дәптерлерге кілттердің өздерін емес, тек олардың шифрмәтінін жазады, ал кілтті шифрлаушы адам жадында сақтайды. Құпия кілттермен айырбас жасау бірқатар жағдайда проблема болып табылады. Сондықтан соңғы жылдары ашық кілтті шифрлау жүйелерді қолдану бағытында қарқынды зерттеулер жүргізілуде.Мұндай жүйелерде шифрлау үшін ашық кілт, ал кері шифрлауға арналған құпия кілт болады.

Криптографияны екі жағдайда қолдануға болады: деректер тасымалдау кезінде оларды қорғау және деректерді сақтау кезінде оларды қорғау .

Деректер тасымалдау кезінде оларды қорғау. Бұл кезде құпия ақпарат жіберуші жақта шифрланады, ал қабылдаушы жақта - кері шифрланады. Қаскөйлер байланыс арнасында оны ұстап алса да кілттік ақпараты (кілттері) болмағандықтан олардың шифромәтінді кері шифрлауға мүмкіншіліктері болмайды.

Барлық криптографиялық алгоритмдер симметриялық және асимметриялық болып бөлінеді. Симметриялы алгоритмдерде деректер бірдей пернелерді пайдаланып шифрланады және кодталады, яғни жіберуші мен қабылдаушы тарап бірдей негізгі ақпаратқа ие. Бұл ақпарат абоненттерге құпия түрде берілуі керек және келесі екі тәсілмен жасалуы мүмкін:

- кілттер физикалық түрде (электрондық кілттер, пластикалық кәртішкелер, әкімші жекеше хабарлайтын құпиясөздер түрінде, т. б.) апарылады;
- кілттер шифрланған түрде байланыс арнасымен жіберіледі;
- кілттерді тарату проблемасы күрделі болудың себебі.

Шифрлаудың беріктілігін жоғарылату үшін оларды мүмкіндігінше жиірек ауыстыру қажет, ал ол кілттерді физикалық түрде жеткізуге кететін шығындардың өсуіне әкеледі және жүйенің бәрін «баға/сапа» тұғырынан қарағанда тиімсіз етеді. Сондықтан тәжірибе жүзінде әдетте қисындастырылған үлгілер қолданылады: абоненттерге ұзақ уақыттық кілттерді физикалық түрде жеткізіледі, олардың көмегімен сеанстық деп аталатын кілттер шифрланады және тасымалданады, осыдан кейін ғана оларды қолдана отырып құпия ақпарат шифрланады.

Асимметриялық алгоритмдер (ашық кілтті алгоритмдер) екі бөліктен тұрады: шифрлауға арналған кілт және кері шифрлау үшін керек кілт. Бірақ шифрлау кілті белгілі болса да шифрды ашу кілтін практика жүзінде есептеп шығару мүмкін емес. Асимметриялық шифрлау үлгісі мынадай: Айбота деген абонент кілттер жұбын генерациялайды, шифрлау кілтін ашық (керек деушілердің бәріне жария) етеді, ал кері шифрлау кілтін құпия түрде қалдырады. Ержан деген абонент, Айботаға хабар жіберу үшін оны Айботаның ашық кілтімен шифрлайды да байланыс арнасына жібереді. Айбота хабарды қабылдап алған соң оны өзінің құпия кілтімен кері шифрлайды.

Ашық кілттер алгоритмдерін пайдаланудың негізгі қауіпі зиянды пайдаланушы ресми ашық кілтті өшіруі мүмкін, содан кейін ол жолдан алынған шифрланған хабарламаларды оқи алады. Осындай шабуылдардан қорғау үшін ашық кілт тәсілдері (сертификат) әзірленді.

Асимметриялық шифрлардың басқа бір кемшілігі олардың төмен өнімділігі және есептеу қорларына қоятын жоғары талаптары болып келеді. Бұл мәселенің шешімі - дәстүрлі симметриялық және жаңа асимметриялық крипто-жүйелерді бірге қолдану: деректер симметриялық алгоритммен шифрланады, ал шифрлауға арналған кілттер асимметриялық алгоритммен жабылады және сеанс басталар алдында байланыс арнасымен серіктеске жіберіледі.

Шифрлар кілттерді тарату ұстанымынан басқа шифрлау тәсілі бойынша да (мысалы, блоктық, ағындық, т. б.) жіктелетінін айта кетейік.

Деректерді сақтау кезінде оларды қорғау. Архивте сақталынған ақпаратты қорғау да маңызды мәселенің бірі болып табылады. Бұл – қаскөй-лердің компьютерлерге немесе ақпарат сақталатын сыртқы құрылғыларға заңсыз қатынас құру қауіп-қатерімен байланысты. Сақталатын ақпаратты шифрлау кезінде кілттерді таратудың қажеттігі болмайды: шифрлауды да, кері шифрлауды да бір адам жүзеге асырады (тасымалданатын деректерді қорғаудан айырмашылығы). Осы себептен сақталатын ақпаратты криптографиялық қорғау үшін баяу асимметриялық алгоритмдер қолданылмайды.

Сақталған деректерді шифрланған қорғау мәселесі екі түрлі жолмен қаралуы тиіс: компьютерлік ақпараттарды толығымен жабу және бағалы ақпараттың тек қана қатты медиада немесе сыртқы сақтау құралдарында ішінара кодтауы. Бірінші нөмір нақты жылдамдықты талап ететін

криптографиялық жүйелерден ерекшеленеді: Шифрлау және кері шифрлау (пайдаланушы сезінбеген) жылдам болуы керек.\

1.4 Криптоанализ элементтері

Қолмен шифрлау мен машиналық шифрлау әдістерінің арасындағы айырмашылықтар бар. Кіру кодтары басқаша болуы мүмкін. Сонымен қатар, олар үшін жабық хабарламалар салыстырмалы түрде қысқа. Осы себепті кері нөлдер адамдармен тиімдірек болады. Машина жүздері шифрланған хабарламаларды өте күрделі және өте ұзақ уақыт бойы жабуға арналған. Бұл хабарламаны қолмен теруге тырысудың қажеті жоқ. Бұл жағдайда басты рөл криптологиттермен ойнайды. Шифрлау түрі және хабардың тілі әрдайым белгілі: олардың анықтамасы алфавитке және кодтың статистикалық қасиеттеріне байланысты. Сондықтан, кілт тек белгісіз деп саналады, бірақ оны бұзу керек.

Нөлдің жекелеген түрлерін бұзуға бірнеше тәсілдер бар. Дәстүрлі кодты талдау жүйелерінен криптоанализді талдау бұзушылардың біліктілігіне байланысты көптеген қылмыскерлерге әкелуі мүмкін. Криптоналитика дискретті математика, нумерология, дерексіз алгебра, статистика және кодтаумен байланысты басқа математикалық пәндер бойынша жақсы білімі болуы керек және кемсітушілік сезіміне ие болуы керек.

Криптоанализдың жетістігі шифрлау алгоритмімен анықталады – шифрды бұзып-ашу қиындығы тек оның құрылмасына тәуелді. Сондықтан, кез келген шифрларды бұзып-ашу үшін қолдануға жарамды криптоанализдың жалпы ұстанымдары өте аз және автоматты түрдегі криптоанализді тек алгоритмдердің өте шектеулі сыныбында қолдану тиімді. Шифрды бұзып-ашуға неғұрлым көп уақыт қажет болған сайын оны берік деп санауға себеп көп. Бірақ шифрдың беріктілігі міндетті түрде оның қауіпсіз шифр екендігін білдірмейді. Бұл шифрды бұзып-ашу әдісі әзірше табылмағанын немесе табылған әдіс жария етілмегенін білдіруі де мүмкін. Тасымалданатын ақпарат беріктілігі жайындағы ұғымды алғашқы рет Актуаном Россиньол (Францияда құрылған шифрлау бөлімінің бастығы) былайша тұжырымдаған: “Әскери шифрдың беріктілігі бұйрықты орындауға қажетті мезгіл ішінде құпиялықты қамтамасыз етуі керек. Дипломатиялық шифрдың беріктілігі құпиялықты бірнеше он жылдық бойы қамтамасыз етуі керек”.

Қазіргі шифрлауда шифрлау күшін тек пайдаланылатын құпия кілтпен анықтайды. Бұл ойынның бірінші қатысуы А.Кирхоффс (1835-1903) шифрлау тетігі (кілтдің мағынасынан басқа) жаудың криптоаналитикасы үшін жақсы белгілі екендігі туралы айтады.

Криптографиялық алгоритмдерге бүгін қандай талаптар қойылады? Негізгілері - сенімділік, бұзу-ашу әрекеттеріне тұрақтылық. Бірақ, адам нені жапса, соны адам аша да алады. Сондықтан, бұзып-ашылмайтын шифрлар жоқ. Тек барлық шифрлау жүйелері шифрқұжаттарды бұзу-ашуды немесе хабар ішіндегі ақпараттан әдейі қымбат істейді, немесе бұзу-ашу уақытын өте үлкен

мезгілге ұзартады. Шифрды әзірлеген кезде қабылдауға болатындай бағаны немесе бұзу-ашу уақыты тағайындалады. Шифрдың пайдаланылу (өмір) уақытын 25 жылдан көбірек алу орынды емес. Мәселен, Британияда үкіметтің өте құпия шешімдері осы мезгіл өткесін тарихшылар үшін жария етіледі. Қазақстан Республикасының заңнамасына сәйкес мемлекеттік құпиялар болып саналатын мәліметтерді құпиялау мезгілі 30 жылдан аспауы керек.

Криптографиялық алгоритмдерге жасалынатын шабуылдардың мүмкін болатын стратегиялары да, әр түрлі шифрларды бұзып-ашу келістері де жеткілікті . Шифрды ашудың ең қарапайым әдісі - кілттердің барлық варианттарын бірінен соң бірін таңдап алып, солардың әрқайсысымен криптограмманы кері шифрлау және алынған нәтижелерге талдау жасау. Бұл ең баяу, сонымен қатар ең сенімді жол және оны дәстүрлі шифрлау алгоритмдердің бәріне қолдануға болады. Шифрды осы әдістің көмегімен ашудан қорғаудың бір тәсілі: мүмкін болатын кілттердің саны мен ұзындығын олардың барлығын тексеріп шығу үшін қабылдауға болмайтындай өте көп уақытты талап ететін шегіне жеткізу керек. Сонымен, құпия кілттің ұзындығы шифрдың сенімділігін бағалау өлшемелерінің өте маңыздыларының біреуі болып табылады.

Кілттерді жаппай тексеріп шығу әдісінен басқа криптографиялық алгоритмдерді ашудың біраз аналитикалық келістері бар. Олар криптографиялық алгоритмдердің осал жерлерін қолдануға бейімделген.

Криптографиялық алгоритмдерге жасалынатын шабуылдардан қорғану үшін құпия кілттің ұзын болғаны жақсы дегенбіз. Бірақ неғұрлым қолданылатын кілт ұзын болса немесе криптографиялық алгоритм неғұрлым күрделі болса, есептеу қорларына қойылатын талаптар да солғұрлым жоғары болады. Осы арадан шифрларға қойылатын екінші талап шығады, яғни жұмыс істеу жылдамдығы.

Қазіргі заманғы криптографиялық алгоритмнің қанағаттандыруға тиісті соңғы шарт – бағдарламалық немесе аппараттық түрде болсын жүзеге асырудың қарапайымдылығы.

1.5 Криптографиялық жүйелер

Қазіргі замандағы криптография төрт ірі бөлімнен тұрады: симметриялық криптожүйелер, ашық кілтті криптожүйелер, электрондық қолтаңба жүйелері және кілттерді басқару.

Криптографиялық әдістерді қолданудың негізгі бағыттары мыналар: жасырын ақпаратты байланыс арналары (мысалы, электрондық пошта) арқылы тасымалдау, жіберілген хабарлардың түпнұсқалығын анықтау, ақпаратты - (құжаттарды, дерекқорларды) шифрланған түрде тасуыштарда сақтау.

Ақпаратты кодалау үшін пайдаланылатын таңбалардың шектеулі жиынтығы әліпби (алфавит, alphabet) деп аталады. Жалпы түрде кез келген әліпбиді былай көрсетуге болады: $\Sigma=\{a_0, a_1, a_2, ..., a_{m-1}\}$.

Белгілі бір ереже бойынша (әліпбидегі әріптерді біріктіру арқылы жаңа әліпби құруға болады:

- (a0a0, a0,a1, ..., am-1am-1) m^2 биграммалары бар Σ^2 әліпбиі;
- (a0a0a0, a0a0a1, ..., am-1am-1am-1) m^3 үшграммалары бар Σ^3 әліпбиі.

Жалпы жағдайда, n әріптері бойынша біріктірсек, онда m^n n-граммалары бар $\sum^n$ әліпбиі шығады.

Мәселен:

- Σ={ABCDEFGH ... WXYZ} ағылшын әліпбиіндегі m=26 әріптерді біріктіру арқылы
- 26^2=676 (AA, AB, ..., XZ, ZZ) биграммалары бар әліпби;
- 26^3=17576 (AAA, AAB, ..., ZZX, ZZZ) үшграммалары бар әліпби.
- криптографиялық түрлендіруді орындау кезінде әліпби әріптерін бүтін сандарға 0, 1, 2, 3, ... ауыстыруға пайдалы.

Мысалы:

- қазақ әліпбиі $\Sigma_{қаз}$={АӘБВГҒДЕ ... ЮЯ}, $\bar{z}_{42}$ = {0, 1, 2, …, 41};
- орыс әліпбиі $\Sigma_{орыс}$={АБВГДЕ ... ЮЯ}, $\bar{z}_{31}$ = {0, 1, 2, …, 30};
- ағылшын әліпбиі $\Sigma_{ағыл.}$={ABCDEF ... YZ}, $\bar{z}_{26}$ = {0, 1, …, 25}.

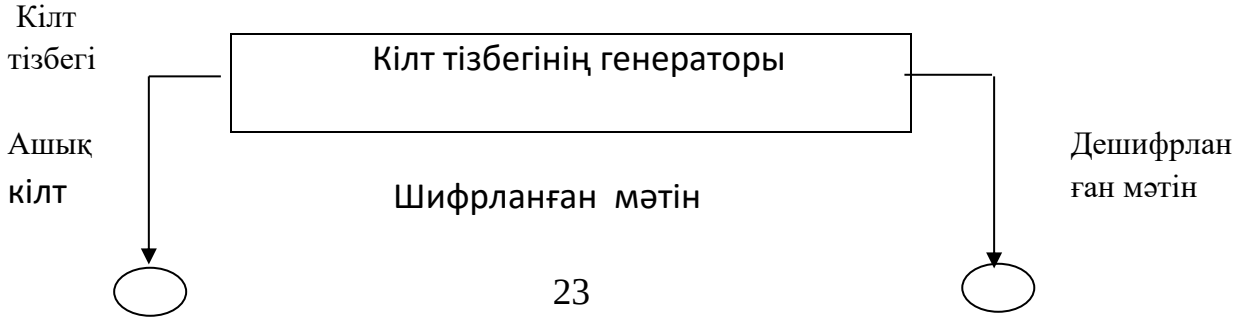
Қазақ тілінің метаалфавиті (цифрлар және тыныс белгілері ескерілген әліпбиі)

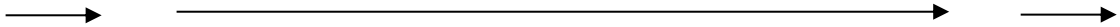
1.6 Симметриялық криптожүйелер

Симметриялық криптожүйеде шифрлау және кері шифрлау үшін бір кілт пайдаланылады (шифрлау кілтін білу шифрды ашу кілтін білуге мүмкіндік береді).

1.7 Ағындық шифрлар

Егер блоктың шифрлау алгоритмдері мәтінді блоктарға бөліп оларды бір бірден ретімен шифрлайтын болса, ағынды шифрлау алгоритмі мәтінді бөліктемей әр элементін шифрлап ағынды күйде жіберіледі. Шифрлау және дешифрлау негізінен 2 модулі бойынша ашық және кездейсоқ кілт тізбегін қосу операциясын қолданады. Тарихи бірінші ағынды шифр Вернам шифры. Вернам шифрының ерекшелігі оның кілт тізбегінің шифрлауында. Бұл шифрдың практикалық қолданылуы өте ұзын кілт тізбектерінен жасалуына байланысты қолайсыз деп есептеледі.





Сурет 1.1 - Вернам шифрының сүлбесі.

Синхрондық шифр. Синхрондық шифрда кілт тізбегі ақпаратта ағынына байланыссыз жасалады. Хабар алушы және хабар жіберуші жағында кілт тізбегі генераторының жұмысы синхрондалған болу керек. Әйтпесе бір бит мәліметін жоғалып кетуі қалған символдардың қате дешифрлауына әкеледі.

Өзіндік синхроноанатын шифры. Шифрдың бұл түрінде ашық мәтін символдары алдыңғы n символға байланысты шифрланады. Ол алдыңғы символ кілт тізбегінің жасалуына қатысады. Синхрондану режимы әрбір шифрмәтін символынан кейін автоматты түрде орындалады.

1.8 Құрама шифрлар

Құрама шифр алгоритмінде блоктық және ағындық шифрлау тәсілдері бірге қолданылады. Практикада құрастырма шифр DES алгоритмінің әр түрлі режимдарында пайдаланылады.

- біркелкі таралу заңдылығымен шын мәнінде кездейсоқ тізбек болып табылатын кілт қолданса;
- кілт ұзындығы бастапқы хабардың ұзындығына тең болса;
- кілт бір ғана рет қолданса;
- шифр абсолют сенімді болады деп дәлелдеді.

Бұл үш талаптың бірден орындалуы әрине қиынға түседі. Дегенмен абсолют сенімді шифр бар және ол біржолғы блокнот деп аталады (onetime pad). Шифрді 1917 жылы Мэйнджер Джозеф Моборн және Гильберт Вернам ойлап тапқан. Кілттің кездейсоқ символдарының тізбегі блокнот беттеріне жазылады. Хабар жіберуші шифрлау үшін кілтті осы блокноттан алып шифрлау процедурасын аяқталғаннан кейін қолданған бетті жояды. Хабар жіберушінің де тура сондай блокнотты болуы тиіс. Шифрмәтінді дешифрланғаннан кейін ол да қолданған бетті жояды.

OTP тәсілінің қызықты қасиетіне тоқталайық. Келесі сөйлемді:

- we hold these truths to be self – evedent.

Вижинер кестесін қолданып шифрлайық. Кілт төмендегідей кездейсоқ символдардан тұрады:

- al lstu dents includ in gp ostg – raduate;

Сонда мынадай шифрмәтін аламыз:

- wp sgex wlrlw bewebv bb htgwel – vvlxegx;

Енді басқа кілт тізбегін таңдап алайық:

- qr pglx jhnie pakqkx bj zo fuxh – vkdrreu;

Шифрмәтін былай дешифрланады:

- My data needs memory as if byte – aligned;.

Демек, сіздің таңдап алынған кілтіңіздің мағынасы бар мәтін беретіндігі, сіз нағыз кілт немесе нағыз мәтін тапты дегенге кепіл бола алмайды.

Теоретикалық тұрғыдан алгоритм сенімді, бірақ оны практикада қолдану қолайсыз. Кілттің ұзындығы мәтіннің ұзындығымен тең болуы керек. Кілт шын мәнінде кездейсоқ болуы керек. Бұл талаптардың қазіргі ақпараттық жүйелерде орындалуы қиын әрі қымбатқа түседі. Бұл тәсілді шын мәнінде өте құпия хабарлар үшін қолдануға болад.

1.9 Асиметриялық криптожүйелер

Криптографиялық қорғау жүйелерінің арасында асимметриялы шифрлау жүйесі ең тиімді болып табылады. Ашық кілт шифрлеу жүйелері деп аталады. Мұндай жүйелерде деректерді шифрлау үшін бір кілт қолданылады, ал басқа кілт деректерді шифрлау үшін қолданылады (мұнда асимметриялық деп аталады). Бірінші кілт ашық және барлық деректерді шифрлауды қалайтын барлық пайдаланушылар үшін қол жетімді болуы мүмкін. Жалпыға қолжетімді деректерді резервтік көшіру үшін жалпыға қол жетімді кілт (жарнамалық кілт) жарамсыз.

Шифрланып келген деректерді кері шифрлау үшін қабылдаушы жақ екінші кілтті пайдаланады. Ол құпия кілт (private key) деп аталады. Сөйтіп бұл криптожүйеде екі түрлі кілт қолданылады: $К_В$ - жіберушінің ашық кілті, $k_В$ - қабылдаушының құпия кілті. Құпия кілтті қорғалмаған арна арқылы жібермеу үшін кілттер генераторын хабар алушы жағында орналастырған тиімді болады. $k_В$ құпия кілтін белгілі $К_В$ ашық кілт бойынша ашу шешілмейтін мәселе болуы керек.

Ассиметриялық криптожүйелерге тән ерекшеліктер:

- $К_В$ ашық кілті мен С криптограммасы қорғалмаған арна бойынша жіберіледі, яғни қарсы жаққа $К_В$ және С белгілі;
- шифрлау және кері шифрлау алгоритмдері $E_В$:М→С, $D_В$:С→М ашық болады;
- ассиметриялық криптожүйелердегі ақпаратты қорғау $k_В$ кілтінің құпиялығына тікелей байланысты;
- У.Диффи және М.Хеллман ассиметриялық криптожүйелерінің қауіпсіздігін қамтамасыз ететін талаптарды атап өтті;
- қабылдаушы үшін бастапқы жағдай негізінде ($К_В$, $k_В$) кілттер жұбын есептеп шығару қарапайым болу керек;
- А жіберуші $К_В$ ашық кілтін және М хабарын біліп, криптограмманы өте оңай есептей шығара алады: $С = E_{Кв}(М) = E_В(М)$;
- В қабылдаушы $k_В$ құпия кілтін және С криптограммасын пайдаланып бастапқы хабарды оңай қалпына келтіре алады;

$$М=D_{Кв}(С)=D_В(С)=D_В[E_В(М)]. \qquad (1.9)$$

- қарсы жақ $К_В$ ашық кілтін біліп құпия $k_В$ кілтін есептеп табу кезінде шешуге болмайтын есептеу проблемасына кез болады;

- қарсы жақ ($К_В$, С) жұбын біліп бастапқы М хабарын есептеп табуды ешқандай жолмен шеше алмайды;

Ашық кілтті ассиметриялық криптожүйелер концепциясында бір бағыттық функцияларды қолдану көзделген. Х және Y - берілген кез келген жиын дейік. Егер барлық $x \in X$ үшін y=f(x) оңай есептеп табуға болатын болса (мұнда $y \in Y$), онда f: $X \rightarrow Y$ функциясы бірбағытты деп саналады.

1.10 RSA криптожүйесі

RSA алгоритмі бірінші ашық кілттер алгоритмі болып табылады. Деректерді шифрлау режимі мен сандық қолтаңба режимін қосуға болады. Алгоритмнің сенімділігі үлкен сандардың күрделілігіне және жеке логарифмдерді есептеудің күрделілігіне байланысты.

RSA криптожүйесінде $К_В$ ашық кілті, $k_В$ құпия кілті, М хабары және С криптограммасы Z_N ({0, 1, 2, ..., N-1} бүтін сандар жиынына жатады. Мұнда N-модуль: N=P*Q, ал Р және Q - кездейсоқ, үлкен қарапайым сандар. Максималды қауіпсіздікті қамтамасыз ету үшін Р және Q сандарының ұзындығын бірдей қылып таңдап алып, оны құпияда ұстайды.

$К_В$ ашық кілтін келесі шарттар орындалатындай етіліп кездейсоқ түрде таңдап алады:

$$1< К_В \le \varphi(N), \quad НОД(К_В, \varphi(N)=1, \quad \varphi(N)=(P-1)(Q-1). \qquad (2.0)$$

мұнда φ(N) - Эйлер функциясы. Эйлер функциясы 1-ден N-ге дейінгі аралықтағы N санымен өзара қарапайым оң бүтін сандардың санын көрсетеді.

Жоғарыда көрсетілген екінші шарт $К_В$ ашық кілті мен φ(N) Эйлер функциясы өзара қарапайым болу керек екенін көрсетеді.

Әрі қарай, кеңейтілген Евклид алгоритмін пайдаланып $k_В$ құпия кілтін есептейді:

$$k_В * К_В \equiv 1 \pmod{\varphi(N)} \text{ немесе } k_В = К_В^{-1} \pmod{(P-1)(Q-1)}. \qquad (2.1)$$

Бұл алушы (Р, Q) сандар жұптарын білетіндіктен және φ (N) функциясын оңай табуы мүмкін болғандықтан жасалуы мүмкін. КВ және Н қарапайым болуы керек. КБ ашық кілті деректерді шифрлау үшін пайдаланылады, ал KW құпия кілті деректерді шифрлау үшін пайдаланылады.

С криптограммасын ($К_В$ ашық кілт және М хабар жұбы арқылы) келесі формулаға сәйкес табуға болады:

$$C = E_{Кв}(M) = E_В(M) = M^{Кв} \pmod{N}. \qquad (2.2)$$

$C=M^{K_B} \pmod N$ функциясын кері түрлендіру, яғни M мәнін белгілі C, K_B және N мәндері бойынша $N=2^{512}$ рет есептеу арқылы анықтау мүмкін емес. Дегенмен, кері есепті яғни C криптограммасын кері шифрлау есебін (k_B құпия кілт және C криптограмма жұбын пайдалана отырып) келесі формуламен шығаруға болады:

$$M = D_{k_B}(C) = D_B(C) = C^{k_B} \pmod N. \quad (2.3)$$

Кері шифрлау үрдісін былайша жазуға болады:

$$D_B(E_B(M)=M \quad (2.4)$$

(2.4)-ке (2.2) және (2.3) мәндерін қойсақ:

$$(M^{K_B})^{k_B} = M \pmod N \text{ немесе } M^{K_B k_B} = M \pmod N \quad (2.5)$$

φ(N) шамасы Эйлер теоремасында өте маңызды рөл атқарады. Эйлер теоремасы бойынша: егер НОД(x, N)=1, онда

$$x^{(N)} \equiv 1 \pmod N \text{ немесе } x^{n*(N)} \equiv 1 \pmod N \quad (2.6)$$

(2.5) және (2.6) өрнектерін салыстыра отырып, мынаны аламыз:

$$K_B * k_B = n*\varphi(N)+1 \text{ немесе } K_B * k_B \equiv 1 \pmod{(N)} \quad (2.7)$$

Сондықтан k_B құпия кілтін есептеу үшін (1.1) өрнегін пайдаланады.

Осылайша, егер $C=M^{K_B} \pmod N$ криптограммасын k_B дәрежесіне шығарсақ, онда оның нәтижесінде ашық M мәтіні алғашқы қалпына келеді, өйткені:

$$(M^{K_B})^{k_B} = M^{K_B k_B} = M^{n*(N)+1} \equiv M \pmod N. \quad (2.8)$$

Сөйтіп, хабар алушы екі параметрді қорғайды: k_B құпия кілтті және көбейтіндісі N модулін беретін (P, Q) сандар жұбын. Екінші жағынан, хабар алушы N модуль мәнін және k_B ашық кілтті ашады.

Қарсы жаққа K_B және N мәндері белгілі. Егер ол N санын P және Q көбейткіштеріне жіктей алса, онда "құпия жолды", яғни {P, Q, K_B} үш санын білер еді. Әрі қарай φ(N)=(P-1)(Q-1) Эйлер функциясының мәнін есептеп табар еді және ол арқылы k_B құпия кілтінің мәнін анықтар еді. Бірақ мәні өте үлкен N санын көбейткіштерге жіктеу мүмкін емес (егер P және Q сандарының ұзындығы 100 ондық таңбадан кем болмаса).

2 Сандарды модульмен көбейту әдісінің құрылғы жүзінде іске асыру.

Асимметриялық криптожүйелерде модульдік операциясы көбейту жұмыс модулін орындау арқылы орындалады. Сондықтан шифрлау

құрылғысының техникалық сипаттамалары модуль бойынша мультипликатордың сәтті құрылысына байланысты.

Классикалы модульмен көбейту әдісінде екі сатыда орындалады: бірінші сатыда сандарды көбейту әдісі орындалады, (C= A·B), ал екінші кезеңде C сан P модулю арқылы жүзеге асырылады.

Заман талабына сай сандық жүйелерде тез аралық сызбалар Браун, Уалесс, Дада, Карацуба т.б. сызбалары арқылы іске асырылады.

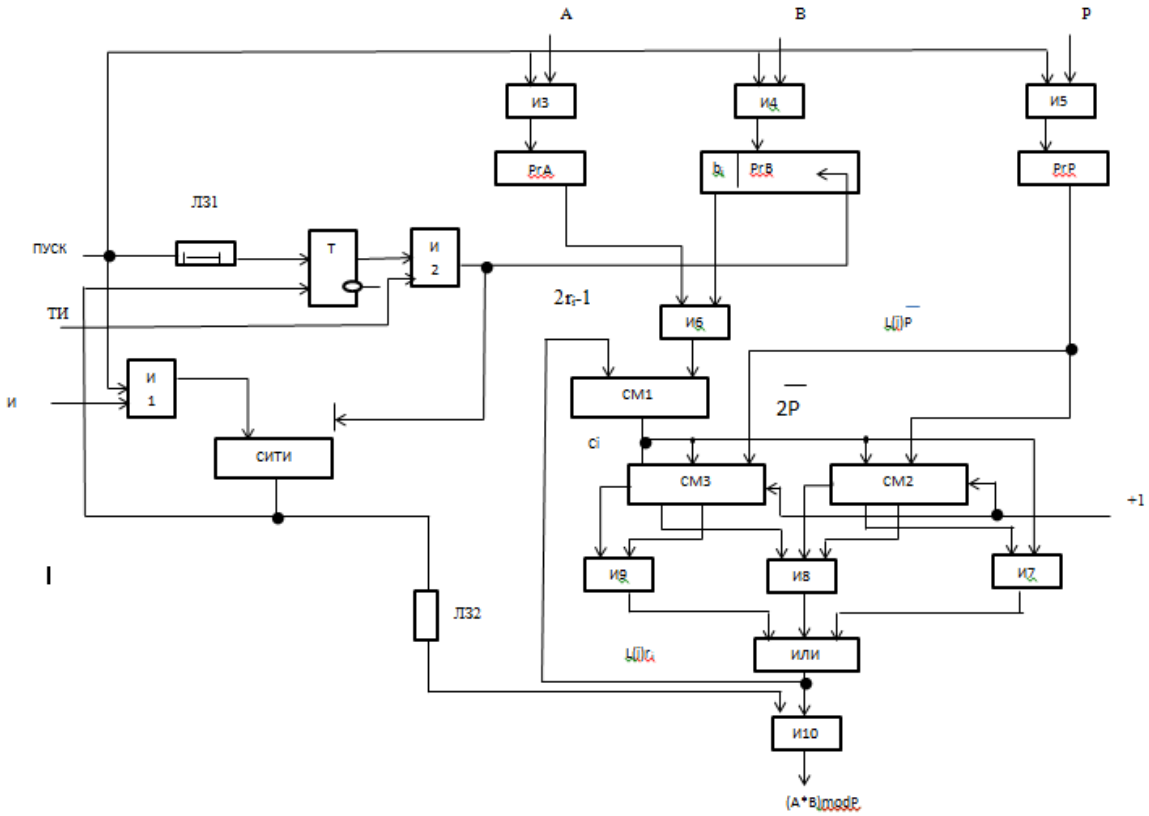
С көбейту модулімен нәтижесінде P шығарғаннан кейін модульмен жұмыс істеу барысы кезінде. Қосымша модуль кодын қолдану арқылы жүзеге асырылады.

Классикалық тәсілдің жетіспеушілігі - үлкен оперативті операндалар үшін мультипликаторды іске асырудың күрделілігі. Сонымен қатар, өнімнің биттері модульдің бит торынан асып кетеді, бұл қалған модульді қалдықпен қалыптастыру процесін баяулатады.

Осы кемшіліктерді жою үшін біз көбейту модулін P әдісін ұсынамыз, ол бұрынғы ri-1 қалдықтарын бір есеге дейін ескіге қарай жылжыту және көбейтілген A өніміне осы коэффициенттің P модулін одан әрі төмендету арқылы B коэффициентінің би-биттік битінің биттен қосып, ағымдағы кезеңнің кезең-кезеңімен қалыптасуына негізделген.

Мұндай қадамдардың саны B бит кобейтіндісінің саны бойынша анықталады. Жоғарыда келтірілген ri мәндердің формула бойынша анықталады.

$$r_{i-1} = (2r_{i-1} + Ab_i) \bmod P, \text{ где } b_i\{0,1\} \text{ и } A < P \text{ и } B < P \qquad (2.9)$$



Сурет 2.1 - функционалды құрылымында модульмен көбейту және де сол жаққа бір санмен ауыстыру арқылы мультипликатор модулінің функционалдық схемасы көрсетіледі

Көбейту құрылымында РгА, РгВ, РгР және де РгR регисторлары,үш сумматордан, сағаттық импульсті контроллерлер – СчТИ, Т триггер кешігу сызығы L.31 және L.32, сол жаққа бір разрядқа екі қолзғатқыш (Сдв(L1), құрылымы И1-И11 және ИЛИ құрылымы.

Регистр РгА А көбейтіндісін сақтауға арналған, РгВ қолзғатқыш регистры, бір битке ауысатын тізбегі бар В көбейткішінің сақтайды, регистр РгР Р модулінің биттерін сақтауға қызмет етеді, РгR регистры , ағымдағы ri-1 қалдықтарын және көбейтудің R модуль қалдықтарын сақтауға қызмет етеді.

СМ1 қосқышы қосарланған мәнді есептеу үшін қызмет етеді бұрынғы қалдық 2ri-1 bi = 1 үшін екілік көбейткішінің коды бар. bi = 1 үшін Ci = 2ri-1 + A шамасы СМ1 тартқыштың шығуында қалыптасады. сумматорлар СМ2 және СМ3 Ci модулінің Р мәнін келтіру үшін қызмет етеді. Осы мақсатта, СМ1 шығуынан Ci мәні СМ2 және СМ3 сол кірістеріне беріледі. Бұл жағдайда СМ2 екінші кірісі модульдің кері кодының модулін екі есе азайтады, яғни, 2p ¯c шығатын Сдв(L1) 1-нің шығуынан P¯ мәніне РгР. тіркелімінің инверттелген шығуынан шығатын кірістерге дейін.

СМ3 қабылдағышының екінші кірістері РгР шығуынан P ¯c мәнімен беріледі. СМ2 және СМ3 кіші разрядты сумматорларға төменгі сандарында +1 деңгейі жеткізіледі, осылайша СМ2 қосқышында Ci + 2P¯ + 1 операциясы

орындалады. СМ3 сумматормен қатар Сі + Р¯+ 1 операциясы орындалады . Сі<Р мәндері үшін СМ1 және СМ3 нәтижелері теріс белгілері бар сандарды құрайды, СМ2 және СМ3 қосқыштарының шығуындағы белгілер ЗН1 = ЗН2 = 1, П2 және П3 тиісті аударымдары 0 мәнін қабылдайды, СМ2 және СМ3 шығуын бұғаттайды.

Бұл жағдайда Сі мәні ИЛИ1 шығуына И10 схемасы арқылы жіберілген кезінде өзгермейді, яғни ri-1қалдығы болып есептеледі. 2р ≥Сі≥Р мәндерінде СМ3 сумматорының шығуында оң қалдық пайда болады.

Бұл жағдайда П3 =1 және ЗН3=0. П3 сигналы бойынша СМ3 тізбегінің И9 арқылы шығатын оң қалдықы ИЛИ1 тізбегінің кірісіне шығады. П2=0 теріс сигналы СМ. Шығу жолдарын бұғаттайды. ЗН3=0 сигналы бойынша Сі тізбектің шығуына И10 шығысы бұғатталады. 2р ≤ Сі шығу мәндерінде СМ2 және СМ3 жиынтықтарының шығуында оң айырмашылық белгілерімен қалыптасады, бұл жағдайда, П2 = П3 = 1 және, тиісінше, ЗН2 = ЗН3 = 0. П2 сигналы бойынша Сі-2р айырмашылығы И8 тізбегі арқылы ИЛИ1 тізбегінің шығуына шығарылады, ЗН2 = 0 сигналы СМ3 қабылдағышының И9 және ИЛИ1 тізбегінің шығуына дейінгі айырмашылықтардың шығуына жол бермейді, және ЗН3 = 0 сигналы Сі мәнін И10 және ИЛИ1 тізбектерінің шығуына бұғатталған.

ИЛИ1 тізбектерінің шығуынан ағымдағы қалдықтар қалған РгR регистрмен тіркеледі. РгR мазмұны кернеу тізбегінің кірістеріне Сдв(L1) 2-ден солға қарай бір разряд арқылы беріледі, шығу кезінде 2ri-1 мәні қалыптасады, ол W1 схемасы арқылы жеткізіледі, ол И7 құрылымы арқылы СМ1 сол жақтағы кірісі арқылы беріледі Сондай-ақ, РгR регистрінің шығысы «операциялардың соңы» сигналы арқылы есептің нәтижесін шығару үшін И11 тізбегінің кірістеріне беріледі.

Мультипликатор модулі келесідей жұмыс істейді. «СТАРТ» белгісінде көбейту және А, В көбейтісінде және Р модульдері И3, И4, И5 тізбектерінің көмегімен РгА регистрлерінде, РгВ және РгВ, n коэффициентінің (К = log2n) биттер санының екілік кодынан бөлек сағаттық сигналдар санауышында (СчТИ) И2 тізбегі арқылы «СТАРТ» сигналымен бір мезгілде жазылады. «СТАРТ» сигналының әрекет етуі кезінде СМ2-нің дұрыс кірістері 2р¯кодымен беріледі, Р¯модулінің кері мәні СМ3 дұрыс кірістеріне беріледі, И6-ден шығу үшін СМ1-ден bi = 1 үшін дұрыс кірістерге РгА-ның шығуынан А мәні.

СМ1-нің сол кірістері «0» -мен беріледі. СМ1 шығу кезінде С0 = А қалыптасады, өйткені И10 және ИЛИ11 схемалары бойынша РгR шамасының R регистрінде Рr мәні алынды, ал r0 ... Сдв (L1) 2 тізбегінің кірістеріне беріледі.

«СТАРТ» сигналы L.3.1 сигналының кідірту уақыты РгА тіркелімінде, И6 схемасында, СМ1 плеерде, И10, ИЛИ1 схемаларында, РгRтіркеліміндегі кодты жазу уақытында анықталады.

Шығу И1-тен Т11 РgВ тізбегінің ауысатын кіруін бір битпен солға жылжытады,Би-1 биттік мәні тіркелімінің үлкен биіктігін орнату. Би-1 = 1 болғанда, А саны СМ1-ті енгізудің дұрыс кірістеріне беріледі. ТІ1 L.3.2

кідірісінен кейін, тізімді ақпаратқа ауыстыру уақытында PrB тізбегінің басқару элементі И7- ге өтеді , Cdv (L1) 2 тізбегінің шығуының 2А (2r0) өтуін СМ1-дің сол жақ кірісіне өтуге мүмкіндік береді. СМ1, Ci = 2ri-1 + A□bi-1 қалыптасады. Содан кейін СМ2 және СМ3 көмегімен С1 модуліндегі мәні 2Р немесе Р формадағы PgR шамасындағы p1. Әрбір СчТИ есептегіш сигналы бар біреуден тағайындалады. Регрессиялық импульстің ТИ2 тіркелуінен кейін PgR формуласы r2 және т.б.

N-го ТИ импульсінен кейін PgR формуласы ри-1-ге бөлінеді және счетчикте «0» орнатады және сигнал «Бірлескен операция». Тығыздағышты Т тегістеу жағдайында орнатады, ол келесі схемалардан шығу импульсінің келуіне жол береді.Сигнал «Конец операций» схема арқылы PgR тіркеуші И11 шығуға кетеді.

Мысал :

Кестеде $A=75_{10}$ бұл мәйтін; $B=46_{10}=101110_2$ кілт; Р=143 модуль; 2Р=286 екі еселенген модуль;

Номері	Екі биттік мәні	Такттар	Такктық ретінің есептелуі	Есептелу жолы
1.	$b_5=1$	ПУСК	$C_0=0+A=75$	75mod143=75 75mod286=75 $r_0=75$
2.	$b_4=0$	ТИ1	$C_1=2r_0+A=75\times2=150$	150mod143=7 150mod286=150 $r_1=7$
3.	$b_3=1$	ТИ2	$C_2=2r_1+A=14+75=89$	75mod143=89 89mod286=89 $r_2=89$

жалғасы

4.	$b_2=1$	ТИ3		253mod143=110

			$C_3=2r_2+A=89\times2+75=253$	253mod286=253 $r_3=110$
5.	$b_1=1$	ТИ4	$C_4=2r_3+A=220+75=295$	295mod143=152 295mod286=9 $r_4=9$
6.	$b_0=0$	ТИ5	$C_5=2r_4+0=18$	18mod143=18 18mod286=18 $r_5=R=18$

2.1 Конвейер әдісімен сандарды модульмен көбейту, бұл жағдайда көбейту үлкен разрядты көбейткіштерден басталады.

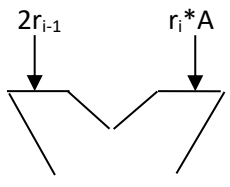
Матрицалық санды модульмен келтірілмейтің полином кобейткішінде өз бір әуелеті бар, ол коверизация мүмкіндігі өңімділігін арттырады . Конверизация кезінде бүкіл есептеу процесі біткен өадам реттілігіне бөлінеді. Әр-қайсы кезендердің рәсімі конвейердің өз кезенінде полином көбейткіші орындалады , барлық деңгейлер қатарлас жұмыс істейді.

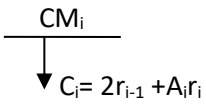
I-n дәрежесінде алынған нәтижелер ары қарай келесі (i-1) дәрежесіндегі конвейрге оңдеуге жіберіледі. Ақпаратты дәрежеден сатыға ауыстыру орталарында орналасқан буфер жады арқылы іске асырылады.

Өз операциясын саты орындаған кезінде нәтижесін буфер жадына сақтап ,келесі ақпаратты өңдеуге кірісе алады , сол уақытта келесі конвейр дәрежесі конвейр ретінде бастапқы кірісіндегі буфер жадында сақталған ақпаратты қолданады .

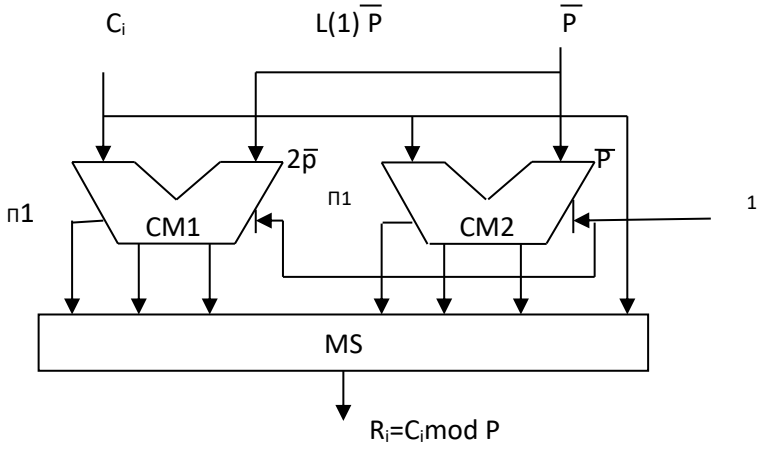
Сурет 3 - Санды модульмен көбейту үшін конвейердің құрылымдық сызбасы келтірілген . көбейту үлкен разрядты құрылымды талдау көбейткіштерінен орындалады.

Сурет 3- Санды модульмен көбейту үшін конвейердің құрылымдық сызбасын А қосымшада көре аламыз.





Сурет 2.1 - CM_i құрылымы.



Сурет 2.2 - ФИО құрылымы.

Конвейр К-1 сатысынан турады. Бірінші саты $И_0$ логикалық құрылымынан тұрады , логикалық көбейткіш n разрядты сан А үлкен разряд b_{n-1} көбейткіші. b_{n-1} =1болған жағдайында А= r_0 саны $P_r r_0$ регистрына жазылады және 1 сатысына $P_r r1$ кіреді, ол PrB-дан разрядсыз b_{n-1} ол ТИ 1 берілген кезінде көшіріліп жазылады , Қалған конвейр сатылар құрамына $И_i$ логикалық блог құрылымы кіреді ,бұл жағдайда Ас Bi логикалық жолмен көбейтіледі. Сонымен қатар ар сатыда екілік суматор бар,) C_i =2$_i r_i$+A *r_i операциясы орындалып , әр сатынын соңында ФИО құрайды бұл жағдайда Сі саны Р модулімен келтіріледі r_i жартылай қалдық есептеледі.

$$r_i = C_i \bmod P. \qquad (2.10)$$

Басқа да атап өтілген логикалық блогы әрқайсы сатысы $P_r r_I$ және PrB-дан тұрады,бұл буфкрлық I регистр сатысынан тұрады.

К – 1 тактық импульсін R регистрге берген кезінде К – 1 сатысында А және В Р модулімен нәтижесі қалыптасады, содан кейін Т командасы PrP шығуынан санды модульмен көбейту нәтижесін алады.

Конвейр тиімділігін есептеу санды модульмен көбейту, конвейр тиімділігінің әсерін сипаттау үшін конвейрлік есептеу жылдамдық көрсеткіш арқасында сипатталады.

Жылдамдықты жеделдетуді түсіну үшін уақыттан ауытқу конвейірсіз өңдеу және уақытты конвейр болуымен өңдеу. Теориялық тұрғыда ең жақсы кіру ағыны уақыты (A(x),B (x) , P(x)) N нан мәні T_{NK} конвейірінде К

сатысында және $T_к$ тактты қ кезеңінде, қайда $T_к = T_И + T_{СМ} + T_{ФИО} + T_{Pr}$. ($T_И$, $T_{СМ}$, $T_{ФИО}$, T_{Pr} кешіктіру уақыт құрылымы И,СМ, ФИО, және БРr) анықталады. Формула TN фактісін көрсетеді ,конвейрдын шығуындапайда болмай турып өндеу нәтижесі К тактан өту қажет, ал келесі нәижелері әр тактте орындалады.

Матрицалық көбейткіште конвейерсіз орташа орындалу уақыты NKT_K құрайды.Осылайша есептеулер S жеделтету конвейеризаця есептеулері аркасында формуламен сипаттаймыз.

$$S = \frac{NKTk}{(K+(N-1))Tk} = \frac{Nk}{K+(N-1)} \qquad (2.11)$$

N→∞ осы жағдайда тыныштық К биіктігіне ұмтылады, конвейердегі саты санына тен.

Жұп сандардын модульмен кобейтіндісінін саны N =100 тен болсын,конвейер саты саны К =30 , сонда матрицалық құрылымында санды көбейту орташа уақыты (конвейерсіз) NK *Tk = (100*30)Tk = 3000 Tk аркылы анықталады.

Конвейерлік өндеумен $T_{NK} = (K + (N – 1)) T_k = (30 + 99)Tk = 2970Tk$ сонда $S = \frac{NK}{K+(N-1)} = \frac{3000}{129} = 23.2$ санын ұлғаюмен N S () к30.

2.2 Модульмен полином көбейткішінің келірілмейтін полином матрицалық құрылымы.

Полиномалды Позициалық емес құрылғы есептеуіш жүйелерінде полиномдарды келтірілмейтін полиномдарды модульмен көбейту құрылғысы, бұл жағдайда күрделі есептеулер ақпаратты шифрлеу және дешифрлеу жүргізіледі.

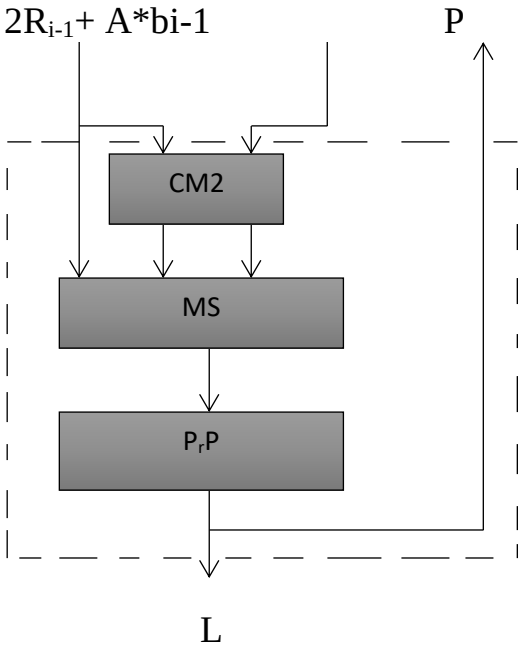
Бұл жұмыста полиномдарды келтірілмейтін полиномдарды модульмен көбейту матрцалық құрылымы қаралады, бұл жағдайда екі дірежелі көбейту полиномыжәне оны модульмен келтіру қосылған , барлық есептеулер биттік тор модулі аралығында орындалады.

Функционалды құрылымы 1-суретте келтірілген. Құрылғы құрамына регистр $P_гA$, $P_гB$ и $P_гP$ бұл жерге операция басталмай тұрып екіліп суреті қабылданады , полином тиісінше A(x) және B(x) үздіксіз полиномы P (x) .Полином A(x) және B(x) көбейтіледі а модуль P (x) келтірілмейтін полином болады.

Регистрден басқа көбейткіш құрамына блок құрылымы кіреді,модуль қосындылары және жартылай жинақтауыш модульмен P (H4OmodP) $СММ_1$-СММ2n-2 , құрылымы N_0/N_5 және или1, сызық кешіктіргіші Л3.1 және Л3.2, Т триггер тактты қ импульс таратқышы РТИ арна санымен n-1, бұл жерде $T1/T_{n-1}$ тактты қ сигнал әзірленеді.

Р модулімен калдықтарды жинақтауыш үлгісі 2-суретте көосетілген.

Сурет 5 - Функционалды құрылымы А қосымшасында келтірілген



Сурет 2.2.1

H4OmodP Сол жақ кірісіне , қосынды нәтижесі $2R_{i-1}+ A*b_{i-1}$ беріледі, оң жақ кірісіне келтірілмейтін полином екілік код Р беріледі,(0 улкен разрядты саны болады $2R_{i-1}+ A*b_{i-1}$), мультиплексор MS шығысында $2R_{i-1}+ b_{i-1}$ өзгеріссіз сан жіберіледі, $2R_{i-1}+ A*b_i$ Р-дан үлкен(1 улкен разрядты саны болады $2R_{i-1}+ A*b_{i-1}$), бұл саннын коды модульмен қосылады екі екілік код Р модулімен , қосынды нәтижесі MS мультиплексор кірісіне беріледі. MS код шығысында P_rP регисторында толтырылады, өтпелі қалдықты $R_i * R_i$ қалыптасады улкен разрядты санға жылжиды азряд он жақтағы үлкен разрядты $CM2_i$ сумматорға беріледі.

b PrP операциясы біткеннен кейін жауабы қалыптасады. N'_0 блок құрылымындағы импульсі шығысындағы T_0 РТИ тактық импульс беріледі бит мәні b_{n-1} реестрден P_rB, взвод мәліметіне екілік код полиномы беріледі A(x)-дан P_rA-ға. A(x) екілік код полиномынан N_1'/ N'_{n-1} кіріс блок шығысына беріледі.

Шығыс $T1/T_{n-1}$ РТИ ТИ ұқсас тиісінше шығыс N_1'/ N'_{n-1} блок құрылымына беріледі.

T_0 сигнал $b_{n-1}=1$ мәнінде код А регистр P_rA шығысында құрылымы N'_0 және или1 H4OmodP шығысында, R_0 аралық қалдық қалыптасады. T_1 сигналы кезіндегі $b_{n-2}=1$ екілік код полиномы А N'_1 блок құрылымы арқылы модульмен қосу сумматоры CM^2_1 сол кірісіне жіберіледі,ал екінші кірісіне екі еселенген разряд R_0 анығырақайтатын болсақ $2R_0$.

$СМ^2_1$ шығысында екілік модуль саны коды қалыптасады нақтырақ айтсақ $2R_0+A*b_{n-2}$. $СМ^2_1$ бұл код шығысында или1 құрылымы арқылы беріледі. Н4OmodP шығысында аралық қалдық R_1 =$(2R_0+A*b_{n-1}$ қалыптасады.

$R_2 \ldots R_{n-1}$ ұқсас аралық қалдық қалыптасады. R_{n-1} сонғы мәні (A(x)*B(x))modP есептеу мәні болады.

Құрылыс жұмысы бір мәнді “Пуск” сигналынан басталады , шығыс мәніне N_0 , N_2 ,N_3 ,N_4 беріледі.

Екінші құрылым шығысына N_0-ға тактық импульс екілік код санына беріледі., k=logn модулі арқылы анықталады,бұл жағдайда n- разрядты көбейткіш.Код тактық импульс есептеуіш шығысына беріледі , РТИ құрамына кіреді. К код мәні $T1/T_{n-1}$ тактық импульс шығарады.

“Пуск” сигналы N_2 ,N_3 ,N_4құрылымдарымен екілік код полномы A(x),B(x) и P(x) қолданылады соған орай PrA ,PrB и PrP регисторларында “Пуск” сигналында Л3.1 сызық кешіктіргішінде кешіктіріледі, содан кейн “Пуск” сигналынан кейін бір мәнді кіріс Т тригерна беріледі және оны 1 қалыпына келтіреді,бір мәнінде болған жағдайында Т триггері N_1 шығыс құрылымына тактық сигналға өтуге рұқсат етеді. N_1 құрылым шығысынан тактық импульс РТИ құрылымына беріліп содан кейін әр-қайсы ТИ шығыс каналынан $T1/T_{n-1}$ сигналы өндіріледі.Сонғы ТИ n-1 шығысында T_{n-1} сигнал өндейді R_{n-1}=R Т триггер ноль мәнді жағдайына қондырылады.Тағы бір ТИ көбейту құрылымна өтуге жол төтейді. T_{n-1} сигналынын тоқтатылуына Л32 N_5 құрылым кірісіне шығу жауабына R шығу құрылымына рұқсат етеді. Поллиномдарды модульмен көбейту келтірілмейтін полиномды матрицалық құрылымына мысал келтірілген .

Мысал:

$A(x)= x^4+x+1;$

$B(x)=x^4+x^2+1;$

$P(x)=x^5+x^2+1;$ болсын

Полиномнын екілік көрінісі:

$A=1\ 0\ 0\ 1\ 1_2;$

$B= 1\ 0\ 1\ 0\ 1_2;$

$P= 1\ 0\ 0\ 1\ 0\ 1_2;$

Алдымен R=A(x)*B(x) есептейміз:

$(x^4+x+1)*(x^4+x^2+1)=x^8+x^5+\cancel{x^4}+x^6+x^3+x^2+\cancel{x^4}+x+1=$

$=x^8+x^6+x^5+x^3+x^2+x+1;$

Содан есептейміз A(x)*B(x)modP

$$\frac{x^8+x^6+x^5+x^3+x^2+x+1}{x^8+x^5+x^3} \left\{ \frac{x^5+x^2+1}{x^3+x} \right.$$

x^5+x^2+x+1

x^5+x^3+x | x^3+x^2+1

$R=x^3+x^2+1$

Екілік көрінісі $x^3+x^2+1= 0\ 1\ 1\ 0\ 1_2$

Есептеу реті A(x)*B(x)modP.

Матрицалық көбейту құрылымы n=5 кестеде келтірілген .

1кестеден көрсе болады , $R= 0\ 1\ 1\ 0\ 1_2$ екенін

	T	T1	T2	T3	T4
PrB=010101	b_4	$B_3=0$	$B_2=1$	0	$B_4=1$
M	010011	0	010011	0	010011
M	-	$2R_0+0=$ 100110	-	-	-
M	-	-	$2R_1+A=$ 00110 10011 ——— 010101	-	-
M	-	-	-	$2R_2+0=$ 101010	-

жалғасы

M	-	-	-	-	$2R_3+A=$ 011110 010011

					001101
H40modP	R_0=AmodP 010011 100101 010010	R_1=(2R)modP 100110 100101 000011	R_2=(2R_1+A)modP 010101 100101 010101	R_3=(2R_2)modP 101010 100101 001111	R=(2R_3+A)modP 001101 100101 001101

3 Экономикалық бөлім

3.1 Техникалық-экономикалық негіздеме

Дипломдық жобаның мақсаты тез және де сенімдішифрлеу құрылғысын әзірлеу .Алда жана заманмен сай болу мақсатында құрылғыны әзірлеу жүзеге асырылды. Осы есептеу барысында біз нақты есептеулерін шығарамыз.

ҚБ-ны дамытудың күрделілігін анықтау үшін ең алдымен барлық негізгі кезеңдер мен жұмыс түрлерінің тізбесі. Сонымен қатар, жекелеген жұмыс түрлерінің жүйелілігін логикалық тұрғыдан реттеуге және оларды параллель орындау мүмкіндігін анықтауға ерекше назар аудару қажет, бұл ҚБ дамуының жалпы ұзақтығын едәуір қысқартуға мүмкіндік береді.

Бағдарламашылар жұмысының креативті элементтері іс жүзінде стандартталмаған, олар тәжірибелі бағдарламашылардың сараптамалық бағалауы немесе бағдарлама атқаратын қызметінің орындалу қиындығына байланысты анықталуы мүмкін.

ҚБ-ны дамытуға жұмсалған шығыстарды анықтау материалдық шығындар, еңбекке ақы төлеу, әлеуметтік салық, негізгі құралдардың құнсыздануы, басқа да шығыстарды қамтитын тиісті бағалауды жасау арқылы жасалады.

3.2 ҚБ әзірлеу қарқындылығы

ҚБ әзірлеудің күрделілігін анықтау үшін біз негізгі жұмыс түрлерінің тізімін құрастырамыз, бұл жұмыстарды логикалық тәсілмен реттеуге және оларды дамытудың жалпы ұзақтығын қысқартуға мүмкіндік беру керек. Жұмыстарды орындаудың еңбегін көрсете отырып, жұмыстарды кезеңге бөлу формасы 4.1-кестеде көрсетілген.

Кесте 4.1 - Жұмыстарды кезеңдер мен түрлері бойынша бөлу және олардың еңбек қарқындылығын бағалау.

БҚ даму кезеңдері	Осы сатыдағы жұмыс түрі	БҚ дамыту еңбек қарқындылығы	
		адм.Х сағ	сағ х күн
Жоспарлау	Жоспарлау, ҚБ тұтастығын дайындау	2 х 16	8 х 2
Талаптарды талдау	Нұсқаулықпен және арнайы құжаттамамен танысу	2 х 24	8 х 3
Техникалық жоба	Жабдықтар мен бағдарламалық жасақтама құжаттамасымен таныстыру. Жабдықтар мен компоненттерді бағалау және таңдау.	2 х 40	8 х 5
Орнату және жабдықтарды монтаждау	Жабдықты орнату, бағдарламалық жасақтаманы орнату және конфигурациялау, басқа компоненттер	2 х 48	8 х 6
Тестілеу және жүйені реттеу	Жүйеде тестілеу және қосу	2 х 40	8 х 5
Дипломдық жұмысты аяқтау үшін қажетті уақыттың жалпы саны		2 х 168	х21

3.2 ҚБ-сын дамыту шығындарын есептеу

ҚБ дамуының өзіндік құнын анықтау үшін келесі элементтерді қамтитын бағалау тізімін құрастыру керек:

- материалдық шығындар;
- еңбекке ақы төлеу;
- әлеуметтік салық;
- негізгі құралдардың амортизациясы;
- басқа шығындар.

3.3 Материалдық шығындар

Негізгі және қосалқы материалдар мен электр энергиясының шығындары материалдық шығындармен байланысты. Материалдық ресурстарға жұмсалған шығындарды есептеу 4.2-кестеде көрсетілген нысан бойынша жүзеге асырылады. Бағдарламалық жасақтаманың құны 4.3-кестеде келтірілген.

4.2-кесте - Материалдық ресурстарға арналған шығыстар

Аттары	Сипаттама	Бағасы
Ноутбук	Asus X705U (X705UV-GC019T)	326990
Виртуальды жеке желі	EDR-810-VPN-2GSFP Industrial Secure Router Switch with	387340
Плата суытқышы	Thermaltake Bigwater 760 Pro 2011-1366-1150-1155-1156-775-AM3+-FM1-FM2+-FM2-AM3-AM2+-AM2	55400
Плата	Arduino Tian	37950
Үздіксіз қоректендіру көзі	APC SUA3000XLI SMART-UPS 3000VA XLI	394400
Модем	Asus RT-AC88U, 8*LAN 1 Гбит/с, 2*USB, 1000/2167Mbps (RT-AC88U)	128990
Желдеткіш	Samsung AR24MSFPAWQ	284990

Кесте 4.3 - Бағдарламалық қамтамасыз ету шығындары

Аттары	Өнімнің атауы	Бағасы

Операциялық жүйе	Win Pro 10 32-bit/64-bit All Lng PK Lic Online DwnLd NR (ESD)	96990
Антивирус	Kaspersky Total Security Multi-Device Box Edition 2ПК 1 жылға	13990
Бағдарламалау тілі	Clarion Enterprise Edition 6.1 Windows арналған	225000

Материалдық ресурстардың жалпы құны (Зм) формула бойынша анықталады (1).

$$З_М = \sum_{i=1}^{n} P_i * T_i \,, \tag{2.11}$$

Зм=326990*2+387340*1+55400*1+37950*1+394400*1+128990*1+284990 *1+96 990*1+13990*1+225000*1 = 1625685 (тг)

3.4 Электрэнергиясына жұмсалатын шығын.

Электрэнергиясына кететін шығынды кесте 4.4 толтыру арқылы табылады. Жалпы құны (2) формула бойынша есептеледі.

$$З_э = \sum_{i=1}^{n} M_i * K_i * T_i * Ц \,, \tag{2.12}$$

Заңды тұлғалар үшін электр тарифі 18,38 тг / кВт * сағ, ҚҚС есебімен.

Кесте 4.4 - Электр шығыны

Жабдықтың атауы	Паспорттық қуаты, кВт	Энергияны пайдалану коэффициенті	БҚ дамуға арналған жабдықтың жұмыс ісету уақыты, h	Электр қуаты тг / кВт * сағ	Бағасы тг
Ноутбук	0,8	0,9	168	18,38	2223,24
Виртуальды жеке желі	0,2	0,7	168	18,38	432,29
Плата суытқышы	0,4	0,7	168	18,38	864,59
Плата	0,6	0,9	168	18,38	1667,43
Үздіксіз қоректендіру көзі жеткізу	0,9	0,9	168	18,38	2501,15
Модем	0,3	0,7	168	18,38	648,44
Желдеткіш	0,9	0,9	168	18,38	2501,15
Жарықтандыру	0,4	0,7	168	18,38	864,59
Электр энергиясының жалпы шығындары					11702,88

3.5 Еңбек ақы төлеу

Еңбекке ақы төлеу $З_{жа}$ шығындарының жалпы құны (3) формула бойынша есептеледі.

$$З_{жа} = \sum_{i=1}^{n} Ч_i * C_i * T_i \qquad (2,13)$$

Формула бойынша анықталған қызметкердің сағаттық бағасы 1190,47 (теңге / сағ)

ҚБ-ны дамытуға қатысатын қызметкерлердің ай сайынғы жалақысы:

- Инженер 1 – 200 000 теңге;
- Инженер 2 – 200 000 теңге.

3.6 Әлеуметтік салық

Әлеуметтік салық - барлық қызметкерлердің еңбек шығындарының 10% -ы және зейнетақы жарналары ($З_{тр}$-дан 11%) әлеуметтік салыққа жатпайды.

ОПВ = 200,000 * 11% = 22,000 (теңге)

СО = (200,000 – 22,000) * 5% = 8900 (теңге)

СН = (200,000 – 22,000) * 11% - 8900= 10680 (теңге)

Екі жұмысшы үшін 2*10680=21360теңге

3.7 Негізгі құралдардың тозуы

Амортизациялық аударылымдар амортизацияның тағайынды шамаларымен орындалады, пайыздармен жабдықтың баланстық құнына және мына формуламен есептеледі:

$$A = \frac{\text{С}_{\text{бас}} * \text{А}_{\text{ш}} * N}{100 * 12 * \text{t}}, \tag{3.1}$$

мұндағы $A_ш$ – амортизация шамалары;

$C_{бас}$– жабдықтың бастапқы бағасы;

N -жұмыс орындалуына кеткен күннің саны;

t – есептеу техникасының қолдануға кеткен жалпы уақыты.

Амортизация шамалары ($А_Ш$), мына формуламен есептеледі:

$$H_A = \frac{\text{С}_{\text{бас}} - K_{\text{тар}}}{\text{Т}_{\text{норм}} * \text{Б}_{\text{бас}}} * 100\%, \tag{3.2}$$

мұндағы $К_{тар}$ – таратылым құны, жабдықтың құнынан 5% құрайды;

$Т_{норм}$ – жабдықтың нормативтік қызмет ету мерзімі (есептеу техникалары үшін – 4 жыл).

Шегерімдерді амортизациялау 4.5-кестеге сәйкес анықталады. Амортизация сомасы (4) формула бойынша есептеледі.

$$З_{АМ} = \sum_{i=1}^{n} \frac{F_i * H_{ai} * T_{Hi}}{100 * T_{эф}}, \quad (2,17)$$

ҚҚ-ның құны сондай-ақ бағдарламалық қамтамасыз етуді және жабдықты жеткізу, орнату және орнату шығындарын қамтиды. Жылдық амортизация нормасы пайдалы қызмет мерзімінің негізінде анықталады және (5) формула бойынша есептеледі:

$$H_{ai} = \frac{100}{T_{Hi}} \quad (2,18)$$

Үздіксіз қуат көздерінен басқа жабдықтар компоненттерін пайдалану 7 жылға жоспарланған. Бағдарламалық жасақтама - 3 жыл. Формуланы (5) қолдану, негізгі қорлардың амортизациясын көрсету үшін 5-кестені толтырылады.

$Н_{А1}$ = 100/4 = 25
$Н_{А2}$ = 100/10 = 10
$Н_{А3}$ = 100/5 = 20

4.5-кесте - Негізгі құралдардың тозуы

Жабдықтардың атауы және БҚ	Жабдықтар мен БҚ құны, тг	Жылдық амортизациялық %	Жабдықтың жұмыс істеу уақытының тиімді қоры және БҚ, сағ	ҚБ-ны дамытуға арналған жабдықтар мен БҚ жұмыс уақыты, сағ	Бағаы, тг
Ноутбук	326990	10	1976	168	2780,1
Виртуальды жеке желі	387340	20	1976	168	6586,3
Плата суытқышы	55400	25	1976	168	1568,9
Плата	37950	10	1976	168	1177,5
Үздіксіз қоректендіру көзі жеткізу	394400	10	1976	168	3353,2
Модем	128990	25	1976	168	3054,4
Желдеткіш	284990	20	1976	168	4845,1
Операциялық жүйе	96990	25	1976	168	2061,5

жалғасы

Антивирус	13990	25	1976	168	2975,5
Бағдарламалау тілі	225000	20	1976	168	3826,1
Негізгі құралдардың жалпы сомасының амортизациясы					3222,8

3.8 Басқа шығыстар

«Өзге шығыстар» коммуналдық шығындарды, лицензиялау және сертификаттауға арналған шығындарды, жарнамалық және басқа да іскерлік және ұйымдастыру шығындарын білдіреді.

Өзге шығынды дамыту үшін айына 19900 теңге көлемінде Интернет шығындары ғана пайдаланылды.

3.9 ҚБ-ны дамытуға жұмсалатын шығындар сметасы

2.3-2.7-тармақтарда келтірілген есептеулер негізінде жалпы шығынды есептеп, оны 4.6-кестеде келтірдік.

Кесте 4.6 - ҚБ-ны дамытуға арналған шығын сметасы

Шығарылатын өнім	Бағасы, тг
Жабдық	1625685
Бағдарламалық жасақтама	
Еңбек ақы төлеу	400000
Әлеуметтік салық	21360
Электр энергиясы	11702,88
Негізгі құралдардың амортизациясы	3222,8
Басқа шығындар	19990
Бағалау бойынша бары	2081960

3.10 БҚ операциялық шығындарын есептеу

БҚ жұмыс істеуі үшін жыл сайынғы операциялық шығыстар (6) формула бойынша есептеледі.

$$З_{ЭКСП} = З_{ЖА} + З_{ЭН} + З_{А} + З_{МАТ} + З_{Ж} \qquad (2,18)$$

- БҚ жұмыс істеу жағдайында әлеуметтік салық бойынша шегерімдермен сарапшылар жалақысына жылдық шығындар;

- Зэн - БҚ тұтынатын электр энергиясының жылдық құны;

- $З_а$ - жылдық амортизация сомасы;

- $З_{мат}$ – БҚ жұмыс істеуі үшін қажетті материалдардың жылдық құны (КТС құнынан 2%);

- $З_ж$ - Жабдықтарды жөндеудің жылдық құны (КТС құнының 7%).

- Жыл бойынша электр энергиясының құны мынадай формула бойынша есептеледі

$$З_{эн} = W * Т_{эф} * Ц \qquad (2,19).$$

Мұнда W - белгіленген КГС қуаты, кВт;

Тэф - КТС-ның тиімді қоры сағаты;

Ц - сағатына 1 кВт электр энергиясының бағасы.

Кесте 4.7 - Жабдық туралы ақпарат

Жабдықтың атауы	Паспорттық қуаты, кВт	Тиімді уақыт қоры, сағ
Ноутбук	0,8	1976
Виртуальды жеке желі	0,2	1976
Плата суытқышы	0,4	1976
Плата	0,6	1976
Үздіксіз қоректендіру көзі жеткізу	0,9	1976
Модем	0,3	8592
Желдеткіш	0,9	1976
Жарықтандыру	0,4	1976

$З_{эн}$=0,3*8592*22+(0,8+0,2+0,4+0,6+0,9+0,9+0,4)*1976*22=56707,2+43564,4=100271,6

Формулаға (8) сәйкес, жыл үшін амортизациялық аударымдар бағасы анықталады.

Мұнда $Н_а$ - амортизация нормасы, % (ҚҚК-нің пайдалы қызмет мерзіміне байланысты);

$К^А$ – күрделі шығындар шамасы және (9) формула бойынша есептеледі.

К = 2081960+(1625685*10%) + 0 = 2244528,5 тг.

З(а) = (2244528,5 * 20) / 100 = 448 905 тг.

$З_{ЭКСП}$ = (400,000+21360) * 12 + 100271,6 + 448 905 + 1625685 * 0,02 + 1625685 * 0,07 = 5 751 808 тг

3.11 КБ-ның ықтимал (келісілген) бағасын анықтау

КБ -ның ықтимал (келісімшарттық) бағасының құны оның орындалуының тиімділігі, сапасы мен мерзімдері негізінде тапсырыс берушінің (тапсырыс берушінің) және орындаушының экономикалық мүдделеріне сәйкес келетін деңгейде белгіленеді.

мұндағы Р - КБ-ның орташа табыстылық деңгейі. % (экономикалық кеңесшімен келісім бойынша 20-30% мөлшерінде қабылданады).

Ц(д) = 2 081 960* (1+0,2) = 2 498 352 (тенге)

Содан кейін, сату бағасы қосылған құн салығын (ҚҚС) есепке ала отырып анықталады, тариф (ҚҚС) заңмен белгіленеді. Қазақстан Республикасының Салық кодексі. 2017 жылға ҚҚС ставкасы 12% деңгейінде белгіленеді.

Өткізу бағасы, ҚҚС есебімен, келесі формула бойынша есептеледі

$$Цр = Цд + Цд* ҚҚС \qquad (2,21)$$

Цр = 2 081 960 + 2 081 960 * 0,12 = 2 331 795(тенге).

3.1 Инвестицияның өтелу мерзімін РР есептеу

Бұл әдіс бастапқы инвестициялардың сомасын өтеуге қажет уақытты анықтауға негізделген

Екі әдіс бар: CF жылдар бойынша тең болғанда және CF жылдар бойынша әртүрлі сомамен жүргенде:

- Егер I_0= = 5 751 808 , ал CF 2 331 795-ден, онда РР= 5000:2300= 2,2 жыл.

Бастапқы инвестициялардың сомасын өтеуге 2 жыл 2 ай кетед кетеді.

Қорытынды

Осы тарауда жасырын әкімшілік етуді, оның ішінде еңбек шығындарын есептеуді жүзеге асыру үшін, ауытқуды анықтауға арналған бағдарламаны әзірлеу үшін қажетті жабдықтар мен бағдарламалық қамтамасыз етуді сатып

алудың экономикалық шығындары есептедім. Жабдықтарды сатып алу шығындарын толығымен есептелді, яғни бағдарламалық өнімді әзірлеудің күрделілігін есептеу; Операциялық шығындарды есептеу: әлеуметтік салық пен зейнетақы жарналары, электр энергиясына жұмсалатын шығындар және амортизациялық аударымдар.

Тұтынушылар үшін экономикалық нәтиже: жабдықты пайдалану шығындарын азайту, негізгі даму құралдарын пайдаланудың экономикалық тиімділігін арттыру. Тұтынушыға арналған сапалы әсер - бұл бағдарламалық жасақтама персоналды бақылауды жақсартуға, жұмыс орнында ақпараттық қауіпсіздік пен өнімділікті қамтамасыз етуге мүмкіндік береді. Сондай-ақ, бағдарламалық қамтамасыз етудің ықтимал келісімшарттық бағасын есептеу жүргізілді, ол 2 331 795 теңгені құрады, ол экономикалық тиімділік тұрғысынан ұтымды шығындар болып табылады.

4 Өміртіршілік қауіпсіздігі

4.1 Еңбек шарттарын талдау

Дипломдық жобада «Шифрлеу құралы - Клиент» үщін криптоалгоритм процесін өңдеу жүргізіледі. Бұл мекеменің 1 қызметкердің көмегімен жүзеге асырылады, ол арнайы орында орналасқан бағдарламаист.

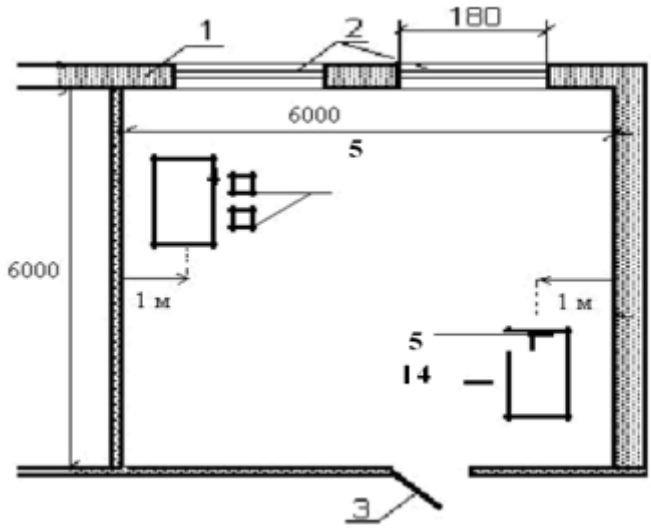
Жобалауға тікбұрышты бөлме таңдалды, мынадай көлеммен: ұзындығы – 6 метр, ені – 6 метр, биіктігі – 2,85 метр, төбесі ақ, қабырғасы ақталған және терезелерімен. Бөлме 3 отыратын жұмыс орнына есептелінген, еңбек құралдары ретінде қолданылады: жабдықтарды бақылау үшін 2 компьютер қажет.

Бөлменің ауданы: $S= 6 \times 6 = 36$ м^2

Биіктігі: $V= 36 \times 2,85$ м^3

Яғни бір адамға тиесілі аудан $36/3 = 12$ м^2 және көлемі $102,6/3 = 34,2$ м^3

Бұл нормаларға сәйкестендірілген бір жұмысшыға арналған ең аз көлемнен көбірек аудан мен көлем (көлем - 15 м^3 аз емес, ауданы - 4,5м^2 аз болмау керек). бөлменің жоспары көрсетілген.



Сурет 6 – Бөлменің жоспары.

Болменің жоспары:

- 1-қабырға;
- 2- терезе ;
- 3- есік;
- 4- үстел;
- 5- орындық.

Бөлме жергілікті салқындату жүйесімен жабдықталған. Бөлмеде тұрақты шу немесе діріл көзі жоқ. Жоба бөлмесі сыртқы шу көздерінен қорғалуы мүмкін пластикалық терезелермен қорғалған.

Бөлмеде электромагниттік сәулелену көздері жоқ. Экран жұмыс істеу үшін сұйық кристалды қолданатын радиоактивті емес жүйені пайдаланады.

Санитарлық нормаға сәйкес бөлмедегі офистік құрал-жабдықтардың ток өткізгіш бөліктеріне адамдардың жақындауына болмайды. Барлық байланыстыратын сымдар мен сызықтар ток өткізбейтін сапалы қаптамамен қапталған.

Жабдыққа ток көзін беру үшін еуророзетка қолданылады, бұл жалпы жерге қосудан қорғаумен байланыстырылған клемманы жерге қосу. Жалпы жерге қосу жүйесі пішінді болып табылады, сонымен қатар, жерге қосылатындар жерге қосылған жабдықтың айналасына, бір-бірінен өте алыс емес етіп орналастырады, қорғалатын жабдықтың барлық таралу ортасын қорғау үшін.

Бөлмеде қалыпты жұмыс шартымен қамтамсыз ету үшін жасанды жарықтандырумен қамтамасыз ету керек.

5.2 Бөлмедегі жылыту жүйелерін талдау, есеп жүргізу

Қондырғы орнатылатын жайда жылдың жылу кезіндегі, келесі жылу бөлу көздерін ескеретін: операторладың, күн радиациясының, жасанды жарықтандырудың, коммутация қондырғыларының бөлетін айқын жылу мөлшерін анықтаймыз. Күннен бөлінетін жылу әйнектің түріне байланысты 90%-ға дейін

бөлмеортасымен жұтылады, қалған бөлігі шағылысады. Жылулық жүктеме шағылысудың максималды деңгейінде максималды мәнге жетеді.

5.1-кесте. Күннен қорғайтын құрылғылардың жылу өткізу коэффициенті

Күннен қорғағыш құрылғы	$\beta_{.҃К}$
Сыртқы:	
- жұқа перделер	0,15
-қалың перделер	0,2
-жалюзи	0,15
ІшкІ:	
-жұқа перделер	0,4
-қалың перделер	0,8

4.1–кестеде көрсетілгендей күннен қорғағыш құрылғылары сыртқы және ішкіден құралады. Терезенің артық көлеңкелеуші заттарның болмағаны кезіндегі күн сәулелерінің терезеден өтетін периоды үшін

$F_0 = F_0$; $F_0 = 0$.

$Q_р = q^1 * F_0 * \beta_{.҃К} = (q_{тік.} + q_{жайыл}) \cdot K_1 \cdot {}^cK_2 \cdot \beta_{К.} \cdot n \cdot H$ о

$B_0 = (352+94) \cdot 0,75 \cdot 0,9 \cdot 0,15 \cdot 3 \cdot 4 \cdot 8 = 4335,12$ Вт

Күн сәулесі терезеден өтпейтін период үшін

$F_0 = F_0$; $F_0 = 0$.

$Q_р = q11_* F0_* \beta_{*҃К} = q_{жайыл} * K_1 * K_2 * \beta_{*.҃К} * n * H_0 * B_{0 =}$

$= 94 \cdot 1,75 \cdot 0,9 \cdot 0,15 \cdot 3 \cdot 4 \cdot 8 = 2131,92$ Вт

Мұндағы, $q_{тік}$, $q_{жайыл}$ – тікелей және жайылған радияциялардың жылулық ағындары, Вт/ м ^{2};

$F_0 = n \cdot H_o \cdot Bo$ – жарық жерінің ауданы, м ^{2} (n – терезелер саны, биіктік Но жәнеені B^o);

- K_1 – көлеңкеленген терезелердің коэффициенті;
- K_2 – кірленген терезелердің коэффициенті;
- Шамдардан түсетін жылу формуламен анықталады:

$Q_{осв} = \eta * N_{осв} = 0,6 * 100 = 60$ Вт

- Мұндағы, η- электр энергиясының жылуғаайналу коэффициенті;
- $N_{осв}$ шамдардың берілген қуаты;
- Қыздыру шамын пайдаланғанда η=0,42- 0,97;

Люминисцентік шамдар η=0,5-0,6. Жарық жүктемесі берілген болуы қажет. Жақсы жарықталған бөлмелер үшін алдын алаесептеулер алуға болады Nосв=50-100 Вт.

Ауаалмасуды есептеу барысында бөлме және өндірістік зиянды заттардың түрлерін қарастырамыз:

- бөлмеде жылу бөлу – артық жылу шығару;
- бөлмеде жылу және ылғалды бөлу- артық жылу және ылғалдар;
- бөлмеде газды және шаңды бөлу- зиянды заттар саны және шаңдар;

Артық жылудың бар болуы кезіндеауаның мөлшері, яғни кеңседен жою қажеттілігін 4.1 формуласымен анықталады.

Мұндағыы, $C_В$-құрғақ ауаның жылусыйымдылығы, (0,24 ккал/кг);
Δ t= t шығ- tкір- бөлмеден шығатын және келіп түсетін ауданың айырымы,С;

- γb=1,20 кг/м3 – ауданың меншікті массасы;
- Qи – кеңседегі артық жылулар , ккал/сағ,
- $Qи=Q_{об}+Q_{осв}+Qл+Qр-Q_{отд}$,
- Мұндағы, Qоб өндірістік құрылғымен бөлінетін жылу, ккал/сағ;
- Qосв - бөлменің жасанды жарықтылық жүйесінен бөлінетін жылу, ккал/сағ;
- Qл – кеңседе қызмет ететін адамдардан бөлінетін жылу, ккал/мағ;
- Qр – кеңсеге күн арқылы түсетін жылу, ккал/сағ;
- Qотд - жасанды жылу таратқышпен жылу беру, ккал/сағ;

Qоб - өндірістік құрылғыдан бөлінетін жылуды мына формуладан көруге болады (5.3)формулада:

$$Qоб=860*Pоб*n$$

Мұндағы, 860 – 1 кВт/сағ жылулық эквиваленті;

- Роб – құрылғының қолданатын қуаты, кВт/сағ (Роб= 12 кВт/сағ);
- n- бөлмеге өтетін жылу мөлшері, оны n= 0,95 деп аламыз.

$$Qоб=860*12*0,95=9804 ккал/сағ$$

Жарықтандырғыш құрылғылардан бөлінетін жылу (5.4)формулада,

$$Qосв= 860 Pосв* α * β * cosφ$$

Мұндағы, Росв – жарықтандырғыш құрылғының қуаты (Росв= 1,28 кВт);

- α – электрлік энергияның жылулыққаайналуындағы ПӘК (қыздыру шамы үшін 0,1- 0,2);
- β – бөлмедегіаппаратура жұмысының біркелкілігінің ПӘК- і (егер барлық аппаратура жұмысістесе β=1);
- cosφ = 0,7 – 0,8 коэффициент.
- Qосв= 860*1,28*0,2*1*0,8= 176,128 ккал/сағ

Адамдармен бөлініп алынған жылуды анықтайық:

$$Qл = Кл \times (q - qисп) \quad (4.1)$$

Мұндағы, Кл – жұмысшылардың саны;

- (q - qисп) – айқын жылу, ккал/с;

- q – жұмыс категориясының мәліметтері кезіндегі бір адамға шығатын жылубөлгіш, ккал/с.

- Qл = 3×(125 - 50)=225 ккал/с;

Күн радияциясымен еңгізілетін жылуды анықтайық:

$$Qр = m \times F \times qост \times К \quad (4.2)$$

Мұндағы, m – кеңседегі терезенің саны;

- F – бір терезенің ауданы, м 2 ;

- qост – күн радиациясы, яғни шыныланған бет арқылы ауданы 1 м 2 , ккал/с болатын жылу мөлшері;

К – шынымен екіесе қапталған, терезенің түзету коэффи циенті. К=0.6

- Qр= 3×2,75×128×0,6=634 ккал/с

Қысқы мезгіл үшін Qр =0 деп аламыз.

$$Qух = \lambda * S * (tвн – tн) / \delta \quad (4.3)$$

Мұндағы, λ=1 Вт/м *С 0 - қабырғаның жылу өткізгіштігі;

- S= 8*10=80 м 2 – бөлменің ауданы;

- tвн – бөлменің ішкі температурасы : жазда 26 С 0 , қыста 20 С 0 ;

- tн – ауадан тыс температура: жазда 21 С 0 , қыста – 15 С 0 ;

- δ = 0,8 м – қабырғаның қалыңдығы.

Қысқы және жазғы кезеңдегі температураны пайдалана отырып Qух формуласын анықтаймыз.

Жазғы кезең үшін: Qух = 0.

Қысқы кезең үшін:

Qух = 1 * 80 * (20 – (– 15)) / 0,8 = 3500 Вт. Qизб формуласына сәйкес :

Жазғы кезең үшін: Qизб = Qоб + Qосв + Qл + Qр. Qизб = 9804+176,128+225+634 = 10839,128 Вт. Қысқы кезең үшін: Qизб = Qоб + Qосв + Qл – Qух. Qизб = 9804+176,128+225-3500 = 6705,128 Вт

Осыдан, бөлмедегі жойылатын қажетті ауасаны:

жазда:

$$L_{\lambda} = \frac{10839\ ,128}{0.24\ *(26\ -\ 21)\ *1.20} = 7527\ ,2\ м^3 / с. \quad (4.4)$$

қыста:

$$L_{\lambda} = \frac{6705,128}{0.24*(20-(-15))*1.20} = 665,2\ м^3/с. \quad (4.5)$$

4.2 Желдеткішті есептеу

Дипломдық жұмысқа байланысты, жұмыс орнында орналасқан МЕСТ 14919-90 қалыңдығы 0,4...0,8 мм болатын жұқа мырыштан жасалынған ауаағарларды дайындап баптауға арналған тартылу желдеткіштерін есептеу қарастырылады .

Жұмыста жүзеге асырылған жабдықтар мен құралдардың ҚР өрт және гигиеналық сертификаттары бар.

Желдеткіш микроклиматтың талаптарымен байланысты көрсеткіштердің мүмкін болатын шамаларын қамтамасыз етеді.

Құйылу желдеткіштері мынандай жағдайларда жүзеге асырылады:

- қысқы мезгілдерде +20 +22 °С дейінгі ауаның жылытуын қамтамасыз етеді;

- ал жазғы мезгілдерде +10 +12 °С дейін ауаның сууын қамтамасыз етеді.

Құйылу желдеткіштеріндегі ауа механикалық қоспалардан тазартылады. Желдеткіштердің өнімділіктері төмендегі формула бойынша есептелінеді:

$$V = V1 \cdot K, м^3/саа$$

Мұндағы,

- V_1 – бөлменің көлемі, $м^3$,

- К – ауаалмастырғыштың мерзімі.

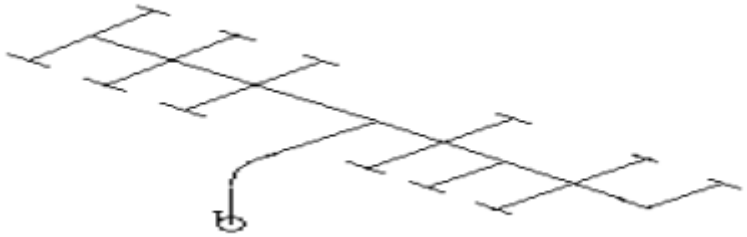
Сығынды желдеткішінің өнімділігін есептеу

Жоғарыдағы көрсетілген бөлменің көлемі бойынша есептейміз. Әр 3 сағат сайын ауа алмасады.

$V_{выт}=(6*6*2,85)*3=308м^3/са$

Құйылу желдеткішінің өнімділігін есептеу

$V_{прит}=(6*6*2.85)*2=205м^3/са$



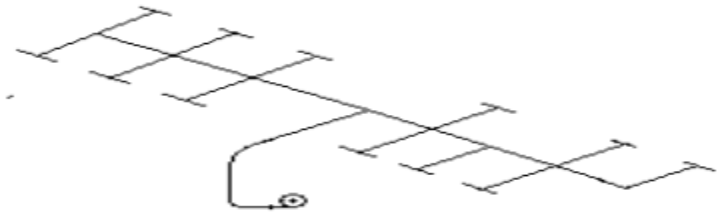
Сурет 4.1 - Тартылу желдеткішінің сұлбасы

Тартылу ауаағарындағы жергілікті кедергілердің коэффициенттерінің жиынтығын, төмендегі формула бойынша есептейміз.

$$\sum I_{выт} = 1,4 * \chi_{возд.выт} + 1,3 + 0,64 \quad (4.6)$$

Мұндағы, $\chi_{возд.выт}$ – тартылу ауаағынындағы торлардың саны

$\sum I_{выт} = 4,1 \cdot 12 + 3,1 + 64,0 = 74,18$



Сурет 4.2 - Құйылу желдеткішінің сұлбасы

Құйылу ауаағарындағы жергілікті кедергілердің коэффициенттерінің жиынтығын төмендегі формула бойынша есептейміз.

$\sum I_{прит} = 1,4 * \chi_{возд.прит} + 1,3 + 2,4$

мұнда χ возд .прит – құйылу ауаағарындағы торлар саны

$\sum I_{прит} = 4,1 \cdot 12 + 3,1 + 4,2 = 5,20$

Ауаөткізгіштердегі қысымның шығынын төмендегі формула арқылы есептейміз.

Мұндағы, l – ауаөткізгіш ұзындығы, м;

- d λ үйкеліс кедергісінің келтірілген коэффициенті;

- 2 2 ν P динамикалық қысым

Құйылу ауаағарларындағы қысымның шығыны төмендегідей есептелінеді:

$$P_{прит} = (70 \cdot 025,0 + 5,20 \cdot 6,21) = 480\ 6\ Па \quad (4.7)$$

Тартылу ауаағарларындағы қысымның шығыны төмендегідей есептелінеді:

$$P_{выт} = (60 \cdot 020{,}0 + 74{,}18 \cdot 4{,}38) = 480\ 6\ Па,$$

Жұмыс орнында құйылу ауаағарына электрқозғалтқыштың қуаты 4,5 кВт, П.Ә.К.=0,4 болатын Ц4-76 маркалы желдеткіштер орнатылған. Ал тартылу ауаағарындағы электрқозғалтқыштың қуаты 3,2 кВт, П.Ә.К.=0,7 болатын Ц4-70 маркалы желдеткіштері орнатылған.

Toshiba N3KVR Daiseikai – бұл жасалған инветордық Тошиба желдеткіші инвертор жетегі бар соңғы буын "және" ең үздік тазартуға, ауаны, кіріктірме желдеткіш, бүгінгі күні.

Аралас инвертор тұрақты ток - жаңа әзірлеу Toshiba қамтамасыз етеді керемет техникалық сипаттамалары, кең мүмкіндіктер орнату қарқындылығы мен ағынының бағытын салқындатылған ауаның жүзеге асыруға мүмкіндік береді, ауаны желдеткіш ең тиімді әлемде жүйесі плазмалық ауаны тазарту Daiseikai бірге фотокаталикалық фильтрлі JAQ қамтамасыз етеді тазалығы ауа желдеткіші тазартады .

Ауаны тазарту, желдеткіш оны қамтамасыз етеді Toshiba Daiseikai келеді жапон стандартына ауа тазартқышты - білдіреді, бұл желдеткіш тазартуды жүзеге асырады ауаны, сол сияқты тиімді және мамандандырылған ауа тазалағыш. Кірістірілген плазмалық сүзгі құтқарады сізге ауа бактериялар,шан, вирустар мен аллергендерден тазартады.

Үздік ауаны тазарту, кірістірілген жайлағыш.

Плазмалық сүзгі Toshiba DaisaikaiБасты ерекшелігі желдеткіш Toshiba Daiseikai жасалады бірегей тазартқыш , ауа, стандартқа сай ауа тазартқышы JEM1467. Арқасында екі сатылы плазмалық сүзгісі ауа ағыны тазартылады ретінде ластанудан (кідіртіледі барлық бөлшектер дейін 0,01 микрон), иіссіз (ұстайды молекуласының диаметрі 0,001-ге дейін). Осылайша, ауа тазарту мүмкін емес тек қана шаң-тозаң, бактериялар мен вирустар, дау зеңнен тазартады!

Белсенді плазмалық сүзгі өз міндеттерін орындауда дейін 10 есе жылдам қарағанда, стандартты пассивті сүзгілер. Ол оңай тазаланады және ауыстыруды талап етеді. Плазмалық сүзгі көпке шыдайды.

Бірінші саты: теріс зарядталған электрондар арналған тұндыру, кесекше, пластина тартады ірі оң зарядталған бөлшектер ластану;

Екінші саты**:** қалған бөлшектер тұнады екінші, неғұрлым тығыз секция теріс зарядталған тұндыру пластина.

Қуатты реттеу инверторы электр энергиясын 40% - ға дейін үнемдейді! Инверторлық компрессорға жиі қосылуы/өшірілуі реттелгенінебайланысты. сондықтан оны шу байқалмайды, ал қызмет ету мерзімі ұзақ кәдімгі болды.

Арасында жаңа әзірлемелер – аралас инвертор тұрақты ток. Енгізу кезінде желдеткіш технологиясы қолданылады, амплитудалы-импульсті модуляция (РАМ). Компрессор жұмыс істейді ең жоғары өнімділігі және

берілген температура қол жеткізіледі 25-30% - ға жоғарылады. Кезде қажетті температурасы қол жеткізілді қосылады кен-импульстік модуляция (PWM). Желдеткіш тоқтайды, ал жұмыс төмен айналымдар істейді және жайлы температурасын сақтайды аз мөлшерде электр энергиясын қлданады.

Өз-өзің тазалау.

Өз-өзің тазалау , жылу алмастырғышта сплит-жүйесі. Қашан желдеткіш режимінде жұмыс істейді салқындату, жылу алмастырғышта ішкі блоктың ылғал қоршаған ауаның теипературасымен тен болады.

Өз-өзің тазалау арқасында ішкі блогында ешқашан құрылада ылғал болмайды, зең, жағымсыз иісі болмайды. Кейін өшіргеннен кейін желдеткіш тағы 20 минут жұмыс істейдіт, содан кейін автоматты түрде өшеді.

Қосымша тазалау сүзгіші ауа Toshiba IAQ

Фотокатикалық сүзгі өте терең тазалау мүмкіндік жасайды ауа көріністері арқылы плазмалық сүзгі және жиынтығында онымен қамтамасыз етуге мүмкіндік береді үздік нәтижесі.

4.3 Өрт қауіпсіздігі негіздері мен өртке қарсы шаралар

Өрт қауіпсіздігін қамтамасыз етуадамдардың өмірі мен денсаулығын, меншікті, ұлттық байлық пен қоршаған ортаны қорғау жөніндегі мемлекеттік қызметтің ажырамас бөлігі болып табылады. Өрттің қай жерде және қашан шығуын болжау мүмкін емес. Ол кез келген уақытта қауіпсіздік және техникалық ережелердісақтамаған кезде болып тұратын жайт. Оны болжау да, дәл айту да мүмкін емес. Өрт - адамдардыңөмірі мен денсаулығына, қоғам мен мемлекеттің мүдделеріне зиян, материалдық залал келтіретін бақылаусыз жану; ерікті өрт сөндіруші - өрттің алдын алу және (немесе) сөндіру жөніндегі қызметкеерікті негізде (еңбек шартын жасаспай) тікелей қатысатын азамат; өртке қарсы ерікті құралымдар - азаматтардың елді мекендерде және ұйымдарда өрттің алдын алу мен оны сөндіруді ұйымдастыруға қатысу нысаны;өрт қауіпсіздігі - адамдардың, мүліктің, меншіктің, қоғам мен мемлекеттіңөрттен қорғалу жай-күйі; өрт қауіпсіздігінің талаптары - өрт қауіпсіздігін қамтамасыз ету мақсатында Қазақстан Республикасының заңнамасымен белгіленген әлеуметтік және техникалық сипаттағы арнаулы шарттар; өрт қауіпсіздігінің талаптарын бұзу Қазақстан Республикасының заңнамасынасәйкес белгіленген өрт қауіпсіздігін қамтамасыз ету жөніндегі нормаларды, ережелер мен нұсқауларды орындамау немесе тиісіншеорындамау; өрт қауіпсіздігі шаралары - өрт қауіпсіздігі талаптарын орындау жөніндегі іс-әрекет;

Өрт салдары зақымдау факторларының әрекеттеріне байланысты болады. Оларға жататындар:

- жанғыш заттың отқа тікелей әсері;

- сәулелер есебінен жоғары температуралы заттар мен объектілерге қашықтықтық әсері;

- жану зонасында иісті газбен улану;

- жану кезіндегітоксинді өнімдерден улану;

Құрылыстардың конструктивті бөліктерінің бұзылып құлауынан адамдардың жарақат алуы немесе қаза болуы. Өрт қауіпсіздігі – бұл өрт болу мүмкіндігін болдырмау жәнеоның пайда болған кезіндеадамдарға, құрылыс және материалдық құндылықтарға өрттің қауіпті факторларының жағымсыз әсерлерін жою үшін қажетті шараларды қолдану болып саналады. Өрт қауіпсіздігі өрттің алдын алу шаралары мен және белсенді өрт қорғанысымен қамтамасыз етіледі. Өрттің алдын алу болып өртті болдырмау немесеоның салдарын азайтуға бағытталған іс-шаралардың кешенісаналады. Белсенді өрт қорғанысы – бұл өрт немесе жарылысқа қауіпті жағдайларымен белсенді күресуді қамтамасыз ету шаралары. Өрттің алдын алу шаралары: - құрылыстық-жобалау; - техникалық;, - ұйымдастырушылық. Құрылыстық-жобалау шаралары - ғимараттар мен құрылыстардың отқа төзімділігімен анықталады (конструкция материалдары жанғыш, қиын жанатын, жанбайтын болып бөлінеді). Отқа төзімділік шегі дегеніміз – бұл оттың әсерінен құрылыс конструкцияларының біріншісызат пайда болғанға дейінгі шыдайтын уақыт интервалы. Барлық құрылыс конструкциялары отқа төзімділік шегі бойынша 8 деңгейге бөлінеді. Ғимараттардың отқа төзімділік деңгейіне байланысты өрт кезінде эвакуациялау үшін шығатын жерлерге дейінгі қашықтықтар белгіленеді. Техникалық шаралары: - өмірге қажетті жүйелерді (жылу, жарықтандыру, вентиляция т.б.) орнатқан кездерде өрт қауіпсіздігі нормаларын сақтау; - құрал-жабдықтар жұмысының тәртібі мен технологиялық процестер парамертлерін сақтау; - әртүрлі қорғану жүйелерін пайдалану. Ұйымдастырушылық шаралар - құрамына өрт қауіпсіздігі бойынша оқу өткізу, өрт қауіпсіздігі шараларының сақталуын тексеру кіреді.

Қорытынды

Қорытындылай келе, жұмыскерлерге жұмысқа қолайлы жағдайын жасау үшүн дипломдық жобама байланысты есептеулер жасалынды.Жұмыс кезіндегі қолайлыжағдайын жасау барысында жарық және жасанды жарық есептелінді .Техникалық қолайлылықты жұмыстын үзілмеушілігін жасау кезіндегі және де жұмыскерледін ауа қолайлығын есеп жүргізілді.Осы есептеулер жүргізу барысында жұмыс қолайлығы жағынан есептеулер жүргізілді.

Қорытынды

Дипломдық жобада шифрлеу құралы туралы және де оның дәлелдер ретінде жазылып көрсетілген құпиясыз мемлекет болуы мүмкін емес. Құпиялар ғылымның, техниканың және саясаттың негізін құрайды. Бірнеше ғасыр бұрын ойлап табылған жазудың жалпы қол жеткізерлік қасиеті бар. Хабар алушыға байланысты бұл қасиетті пайдалы немесе зиянды деп қарауға болады. Жазумен қатар құпия хат (грек тілінде криптография) дамиды. Құпия хат хабардың мағынасын адамдардан жасыруға және оны тек белгілі бір ғана тұлғалар қол жеткізе аларлықтай істеуге арналған. Кез келген қоғам ақпарат өндірмей, жинақтамай және айырбастамай дами алмайды. Нақтылы ақпарат арналған адамдар шеңберіне шек қою қажеттілігі әрқашанда болған. Сондықтан, ақпарат арналмаған адамдардан хабарды жасыру тәсілдері туралы ғылым, яғни криптография пайда болған.

Соған орай шифрлеу құралы үлкен мүмкіндіктер береді тез ары тұрақты, үлкен мөлшерде өңдеу операциаларын жүргізе алад. Құрылғы жұмыс өңімділігінің өте жақсы крипто тұрақтылығы мықты, шифрлеу жылдамдығы көбейді, көп мөлшерде ақпаратты өңдеу мүмкіндігі пайда болды. Құрылғы сенімді болса болады. Осы сапаларына қарап құрылғы үлкен мүмкіндіктерге ие екендігін көрдік.

Пайдаланылған әдебиеттер тізімі

1. Мүсрәлиева Ш.Ж. Қолданбалы криптография. Оқу құралы. Алматы, 2004.

2. Байсалов Е.Р. Криптографияның математикалық негіздері. Алматы, 2003

3. Шнайер Б. Прикладная криптография. Издательство Триумф. Москва, 2002

4. Абдикаликов К.А., Задираки В.К., Мельников С.С. Быстрые алгоритмы вычисления арифметических операций над многоразрядными числами в асимметричных криптоалгоритмах. Доклады НАН РК №2. 2002. Алматы

5. Качко Е.Г. Распараллеливание алгоритмов умножения многократной точности. Вестник УГАТУ «Математическое и программное обеспечение. Т.15. N5 (45). с. 142-147. Уфа. 2011.

6. Тынымбаев С.Т., Мырзабекова К.К. Синтез умножителей с повышенной разрядностью на множительно-суммирующих блоках. Труды международного форума «Инженерное образование и наука в XXI веке: проблемы и перспективы», посвященного 80-летию КазНТУ им. К.И. Сатпаева, Том II, 22-24 октября 2014 г.

7. Петренко В.П., Чипига А.Ф. Комбинированный рекуррентный формирователь остатков. Патент RU №2029435, опубл. 20.05.2009 МПК GO6F 7/72 H03M7/18.

8.Петренко В. И., Кузьминов Ю. В. Умножитель по модулю. Патент РФ RU 2299461, Бюллетень №14, опубликован 20.05.2007.

9. Орлов С. А., Цилькер Б.Я., Организация ЭВМ и систем: Учебник для вузов, 3-изд.-. СПб.: Питер, 2015. -688 с.

10. «Методы дискретной математики в криптологии» - В.М. Фомичев.

11. «Прикладная криптография» - Б. Шнайер.

12. «Основы криптографии» - А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин

13. «Optimal asymmetric encryption» M. Bellare and P. Rogaway

14. «Digital signatures with RSA and other public-key cryptosystems» D. E. Denning