ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасын

Озат Мөлдір

«Ағындық шифрлар негізінде ұялы байланыстағы ақпаратты криптографиялық қорғауды талдау»

ДИПЛОМДЫҚ ЖҰМЫС

5В071900 – Радиотехника, электроника және телекоммуникация мамандығы

Алматы 2022

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
ЭТ ж ҒТ кафедра меңгерушісі
техн.ғыл.кан
Е.Таштай
«20» 05 2022 ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы «Ағындық шифрлар негізінде ұялы байланыстағы ақпаратты криптографиялық қорғауды талдау»

5В071900 – Радиотехника, электроника және телекоммуникация мамандығы

Орындаған

Пікір беруші-
доктор PhD, профессор АУЭС Университетті
Ж.А. Сагындыкова
«20» 05 2022 ж.

Озат Мөлдір

Ғылыми жетекші
PhD докторы
ассистиент профессор
Хабай.А
«20» 05 2022 ж.

Алматы 2022

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Қ.И Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті
Бүркітбаев атындағы Өнеркәсіптікт автоматтандыру және цифрландыру институты
Электроника, телекоммуникация және ғарыш технологиялар кафедрасы
5В071900 – Радиотехника, электроника және телекоммуникациялар

БЕКІТЕМІН
Кафедра меңгерушісі
_____Е.Таштай
«21» ___XII___ 2021ж

Дипломдық жұмыс орындауға
ТАПСЫРМА

Білім алушы *Озат Мөлдір*
Тақырыбы *«Ағындық шифрлар негізінде ұялы байланыстағы ақпаратты криптографиялық қорғауды талдау»*
Университет ректорының *"24"12.2021ж. №1189/ө* бұйрығымен бекітілген
Аяқталған жобаны тапсыру мерізімі «30» 04 2022 ж.
Дипломдық жұмыстың бастапқы берілістері:
1) *Дипломдық жұмыста криптографиялық алгоритмдердің тұрлері мен негізгі әдістеріне және GSM ұялы стандартына криптографиялық алгоритмдерін қысқаша шолу.*
2) Сызықтық кері байланысы бар жылжу регистрі негізінде құрылған криптографиялық алгоритмды ұялы байланыс жүйесінде қолдану технологиясы.
Дипломдық жұмыста қарастырылатын мәселелер тізімі:
а) *GSM ұялы стандартына криптографиялық алгоритмдерін енгізу.*
б) Ұялы байланыс жүйесіне қолданылатын криптологиялық шифрлау технологясы.
в) Сызықтық кері байланысы бар жылжу регистрі құрылымы мен жұмыс принципын талдау.
г) Берілген *ақпаратты қорғаудың жаңа симметриялық кілтін шифрлау алгоритмін құру.*
Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс) :
Сызбалық материалдар 14 слайдпен берлсін.

Ұсынылатын негізгі әдебиет :

1) Bruce Schneier, " Applied Cryptography," John Wiley & Sons Inc.,1996,New York[2] Raj Pandya, "Mobile and Personal Communication Systems and Service"s, 2011 IEEE PRESS, New York.
2) V. K. Garg, "Wireless and Personal Communication System", 12, 2015.
3) Бабаш, А.В. Криптографические методы защиты информ.: Учебное пособие: Т.1 / А.В. Бабаш. - М.: Риор, 2018. - 48 с.р.
4) Васильева, И.Н. Криптографические методы защиты информации: Учебник и практикум для академического бакалавриата / И.Н. Васильева. - Люберцы: Юрайт, 2016. - 349 с.
5) Рябко, Б.Я. Криптографические методы защиты информации: Учебное пособие для вузов / Б.Я. Рябко, А.Н. Фионов. - М.: Горячая линия -Телеком, 2014. - 229 с.
6) Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2015. - 376 с.

Дипломдық жұмысты (жобаны) дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерізімі	Ескерту
Ұябайланыстағы криптографиялық алгоритмдердің тұрлері мен негізгі әдістеріне әдеби шолу	24.01.2022	Әдеби шолу
GSM ұялы стандартының криптографиялық алгоритмдері	15.02.2022	Шолу және талдаулар
Ағынды шифрлау. Сызықтық кері байланысы бар жылжу регистрі (СКБЖР) негізінде шифрау	30.03.2022	Отчет
СКБЖР шифрлауды бағдарламалық іске асыру	27.04.2022	Отчет

Дипломдық жұмыс (жоба) бөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жұмысқа (жоба) қойған

Қолтаңбалары

Бөлімдер	Кеңесшілер, аты, әкесінің аты, тегі (ғылыми дәрежесі, атағы)	Қол қойылған күні	Қолы

	ЭТжҒТ каф. Ассистент-прфессоры, Доктор PhD Хабай Аар		Хабай
Норма бақылаушы	ЭТжҒТ каф. Ассистент Ж.М.Досбаев	23.05.2022	

Ғылыми жетекшісі PhD докторы _____ Хабай Анар
(қолы)

Тапсырманы орындауға алған білім алушы _____ Озат Мөлдір
(қолы)

Күні «20» 05 2022 ж.

АҢДАТПА

Дипломдық жоба ағындық шифрлар негізін қолдана отырып, ұялы байланыстағы ақпаратты криптографиялық қорғау мәселелерін зерттеуге арналған. Сонымен қатар криптографиялық алгоритмдердің түрлері мен негізгі әдістеріне және GSM ұялы стандарт алгоритмдерін қысқаша шолу принциптеріне бағытталған. Ағындық шифрлардың түрлерін, артықшылықтары мен кемшіліктерін, сипаттамаларын атап өтеді. Құпия белгісіз шифрлаудың әрбір құрылған мәнді шифрлау режимінде қайтымды жалған кездейсоқ функция (PRF) ретінде анықтап,2 модульді түрінде есеп шығарылды. RC4 шифрлау режимінің S дайындық кезеңінде инициализациялау кестесі қарастырылды.

Әртүрлі шифрлау алгоритмдерін қолданатын құрылғылар ұсынылған.

Кілт сөздер: Криптография, шифрлау, GSM ұялы стандарты, аутентификация алгоритмдері.

АННОТАЦИЯ

Дипломный проект посвящен изучению проблем криптографической защиты информации в сотовой связи с использованием основы потоковых шифров. Он также фокусируется на типах и основных методах криптографических алгоритмов и принципах краткого обзора криптографических алгоритмов для мобильного стандарта GSM. Перечисляет виды, достоинства и недостатки, характеристики потоковых шифров. В режиме шифрования каждого сгенерированного значения секретного неизвестного шифрования определяли как обратимую псевдослучайную функцию (PRF) и выводили отчет в виде модуля 2. На подготовительном этапе s режима шифрования RC4 была рассмотрена таблица инициализации.

Представлены устройства, использующие различные алгоритмы шифрования.

Ключевые слова: Криптография, шифрование, сотовый стандарт GSM, алгоритмы аутентификации.

ANNOTATION

The diploma project is devoted to the study of the problems of cryptographic protection of information in cellular communications using the basics of stream ciphers. It also focuses on the types and basic methods of cryptographic algorithms and the principles of a brief overview of cryptographic algorithms for the GSM mobile standard. Lists the types, advantages and disadvantages, and characteristics of stream ciphers. In the encryption mode, each generated value of the secret unknown encryption was determined as a reversible pseudorandom function (PRF) and a report was output in the form of module 2. At the preparatory stage s of the RC4 encryption mode, the initialization table was considered.

Devices using various encryption algorithms are presented.

Keywords: Cryptography, encryption, GSM cellular standard, authentication algorithms.

МАЗМҰНЫ

КІРІСПЕ

Адам қоғамында жазудың таралуымен, хаттар мен хабарламалармен алмасу қажеттілігі туындады, яғни жазбаша хабарламалардың мазмұнын бөтен адамдардан жасыру қажеттілігін тудырды. Хабарламаның мазмұнын жасыру әдістерін үш топқа бөлеміз. Бірінші топқа хабарламаны жасыруды жүзеге асыратын жасырушы немесе сызу әдістері кіреді; екінші топ құпия жазудың немесе крипто графиясының әртүрлі әдістерінен тұрады (грек сөздерінен ktyptos-құпия және grapho-жазу); үшінші топтың әдістері арнайы техникалық құрылғыларды құруға бағытталған, ақпаратты құпияландыру болып табылады. Басқа адамдар оқи алмайтындай жеке ақпаратты қайта құру, түрлендіру жолымен қорғау мәселелері адамзатты бұдан бұрында толғандырып келді.

1990 жылдардың басында, коммерциялық интернеттің енді бастау алған шағында, пайдаланушылардың көпшілігі қауіпсіздікті бізге қажет қарапайым қорғаныс құралдарының көмегімен қамтамасыз ететінін түсінді .

Қауіпсіздік пен құпиялылық қауіпсіз аударым мен төлемдерден бастап жеке байланыс пен медициналық ақпаратты қорғауға дейінгі көптеген қосымшаларға әсер етеді. Қауіпсіз байланыстың маңызды аспектілерінің бірі-криптография. Бірақ криптография қауіпсіз байланыс үшін қажет болса да, оның өзі жеткіліксіз екенін ескерген жөн

1 Ұялы байланыстағы криптографиялық алгоритмдер

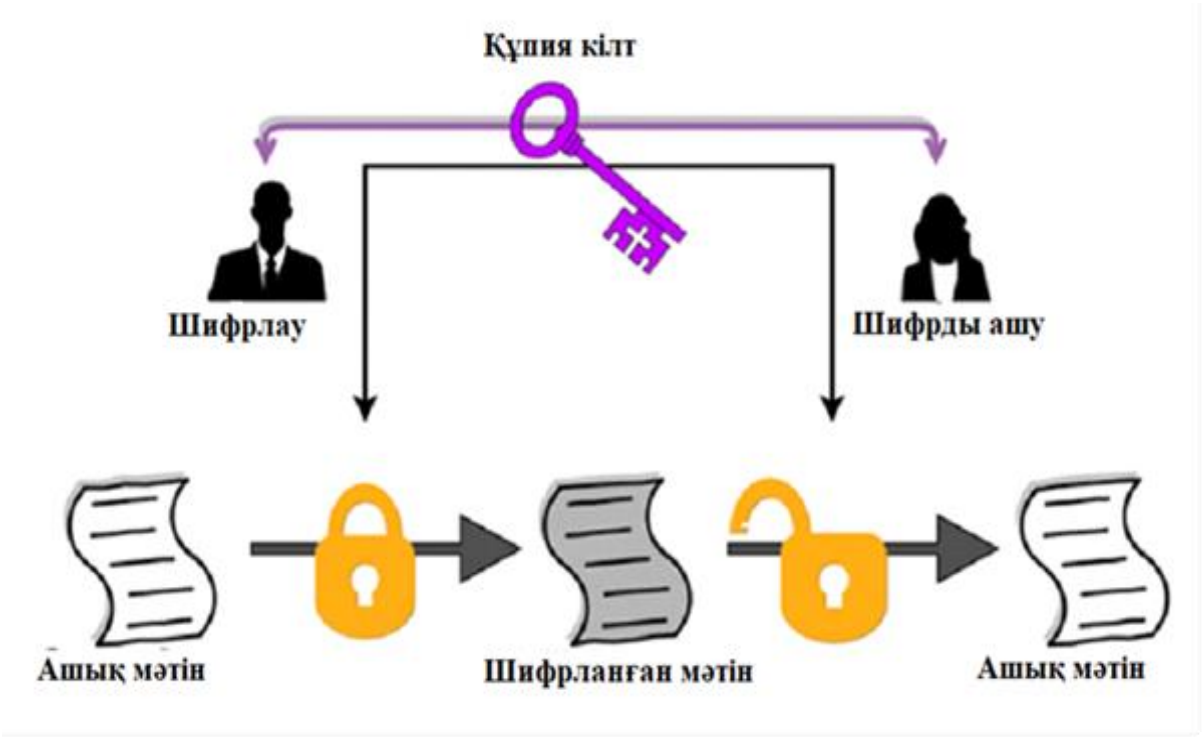
1.1 Криптографияның негізгі ұғымдары мен функциялары

Құпия сөздер біздің өмірімізде маңызды рөл атқарады, сондықтан құпия сөз қайдан пайда болады және ол неге жасалады?

Криптография желілік қауіпсіздік, ақпараттық қауіпсіздік және блокчейн сияқты өнімдердің негізі болып табылады. Кәдімгі асимметриялық шифрлау, симметриялық шифрлау, хэш функциялары және т.б. - мұның бәрі криптография санатына жатады. Криптографияның мыңжылдық тарихы бар. Ауыстырудың бастапқы әдісінен қазіргі асимметриялық шифрлау алгоритміне дейін ол екі кезеңнен өтті: классикалық криптография, заманауи криптография. Криптография-бұл математиктердің даналығы ғана емес, сонымен қатар киберкеңістіктегі заманауи қауіпсіздіктің маңызды негізі. Деректер мен телекоммуникация саласында криптография кез-келген желіні, әсіресе интернетті қамти алатын сенімсіз медиа арқылы байланыс кезінде қажет.

Криптографияның бес негізгі функциясы бар:

1. Құпиялылық немесе қауіпсіздік: болжамды алушыдан басқа ешкім хабарламаны оқи алмайтындығына көз жеткізу;
2. Аутентификация: сіздің жеке басыңызды растау процесі;
3. Тұтастық: алушының алынған хабардың түпнұсқамен салыстырғанда ешқандай жолмен өзгертілмегеніне сендіруі;
4. Сенімділігі: жіберушінің бұл хабарламаны шынымен жібергенін дәлелдеу механизмі;
5. Кілттермен алмасу: криптографиялық кілттерді жіберуші мен алушы бөлісетін әдіс.



1.1 Сурет – Хабарламаны шифрлау

Криптографияда біз ашық мәтін деп аталатын шифрланбаған мәліметтерден бастаймыз. Ашық мәтін шифрланған мәтінге шифрланады, ол өз кезегінде (әдетте) қайтадан пайдалануға болатын ашық мәтінге аударылады. Шифрлау және шифрды шешу қолданылатын криптографиялық схеманың түріне және кілттің белгілі бір түріне негізделген. Формула түрінде бұл процесс былай жазылады:

$$C = E_k(P) \tag{1.1}$$

$$P = D_k(P) \tag{1.2}$$

Мұндағы, P = ашық мәтін, шифрланған деректер жоқ. C = шифрланған мәтін, деректер шифрлау функциясымен өңделеді. E, D = шифрлау әдісі және k = кілт. Ашық мәтінді шифрлау үшін қолданылатын кілт сөз. Симметриялық шифрлау алгоритмінде шифрлау және шифрлау кілттері сәйкес келеді. Кілт алушы мен жіберуші арасында келісіледі, бірақ оны тікелей желі арқылы беру мүмкін емес, әйтпесе кілт ағып кетеді. Әдетте кілт асимметриялық шифрлау алгоритмімен шифрланады, содан кейін екінші тарапқа желі арқылы беріледі немесе тікелей талқыланады. Кілт жоғалмауы керек, әйтпесе шабуылдаушы шифрланған мәтінді қалпына келтіріп, құпия деректерді ұрлайды.

1.2 Криптографиялық алгоритмдердің түрлері

Криптографиялық алгоритмдердің бірнеше классификациясы белгілі. Олардың бірі белгілі бір алгоритмде қолданылатын кілттердің санына байланысты бөлінеді:

- кілтсіз -есептеулерде кілттер қолданылмайды;
- бір кілтті - бір негізгі параметрмен жұмыс істейді (құпия кілт);
- екі кілтті - әр түрлі жұмыс кезеңдерінде олар екі негізгі параметрді қолданады. (құпия және ашық кілт).

Құпия кілт криптографиясы (SKC): шифрлау үшін де, дешифрлау үшін де бір кілтті қолданады; симметриялық шифрлау деп те аталады. Ол негізінен құпиялылық пен сенімділік үшін қолданылады.

Ашық кілт криптографиясы (PKI): шифрлау үшін бір кілтті, ал дешифрлау үшін екіншісін қолданады; асимметриялық шифрлау деп те аталады. Негізінен түпнұсқалықты тексеру, бас тарту және кілттермен алмасу үшін қолданылады.

Хэш функциялары: сандық саусақ ізін беру арқылы ақпаратты қайтымсыз "шифрлау" үшін математикалық түрлендіруді қолданады. Негізінен хабарлардың тұтастығын қамтамасыз ету үшін қолданылады.

1.2 Сурет– Криптографиялық алгоритмдердің жіктелуі

1.3 Криптографиялық әдістерге қойылатын талаптар

Ақпаратты қорғаудың криптографиялық әдістері келесі талаптарға сай болуы керек:

1. Криптоанализге төтеп бере алатын және кілттерді толық сканерлеу арқылы ашуға болатын сенімді шифрға ие болуы қажет. Сондықтан кілтті анықтау ықтималдығы оның ұзындығына байланысты.
2. Қолданатын алгоритмдерді емес, құпия кілттерді сенімді сақтау арқылы криптографиялық жүйенің тұрақтылығын қамтамасыз ету.
3. Бастапқы ақпараттан аспайтын кодталған ақпараттың көлемін жасау.
4. Шифрлау кезінде пайда болатын қателіктерге байланысты ақпараттың бұрмалануы мен жоғалуын болдырмау.
5. Минималды кодтау уақытын қамтамасыз ету.
6. Шифрлау құны мен бастапқы ақпараттың құны арасындағы сәйкестікті қамтамасыз ету.

Ақпаратты қорғаудың криптографиялық әдістері тиімділіктің негізгі көрсеткіші шифрдың тұрақтылығымен сипатталады. Бұл тиімділік кілт болмаған жағдайда кодталғаннан бастапқы хабарламаны алу үшін декодер уақыт пен шығындарға ұшырайды. Егер тез есептелетін шифрлау алгоритмдерінде әлсіз нүктелер болмаса және кілттің жеткілікті сенімді ұзындығы болмаса, бұл шығындар айтарлықтай артады.

Ақпараттық жүйелерде криптографиялық әдісті пайдалану мәселесі қазіргі таңда өзекті мәселе болып отыр.

Біріешіден, компьютерлік желілердің қолданылуы кеңейді, соның ішінде өзге тұлға пайдалануға болмайтын үлкен көлемді әскери, сауда, мемлекеттік, ақпараттардың желілерде таралуы. Екінші жағынан, жаңадан қуатты компьютерлердің, жүйелік және нейрондық есептеу технологияларының пайда болуы, бұған дейін ашылмайды деп жүрген криптографиялық жүйелердің дискредитациясына мүмкіндік берді.

1.4 Неліктен үш шифрлау әдісі қолданылады?

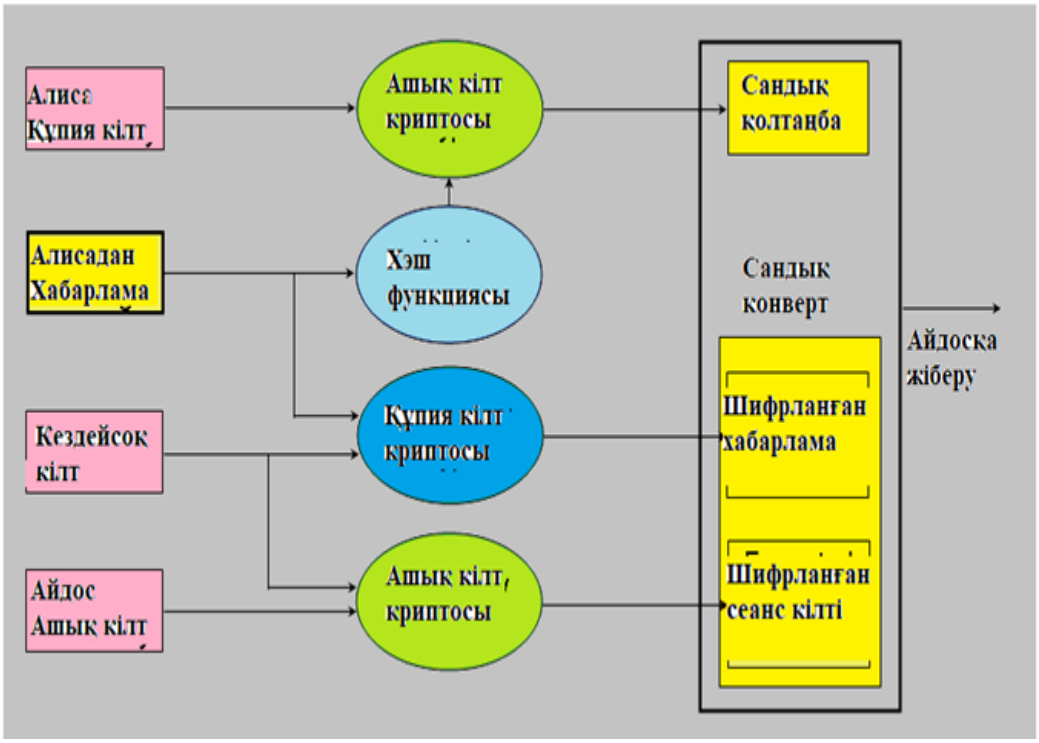
Сонымен, неге криптографиялық схемалардың әртүрлі түрлері бар? Неліктен біз қажет нәрсені тек біреуімен жасай алмаймыз? Жауап: әр схема кейбір нақты криптографиялық қосымшалар үшін оңтайландырылған. Мысалы, хэш функциялары деректердің тұтастығын қамтамасыз ету үшін жақсы жұмыс істейді, өйткені хабарлама мазмұнына енгізілген кез-келген өзгеріс алушының жіберушіге берілгеннен өзгеше хэш мәнін есептеуіне әкеледі. Екі түрлі хабарлама бірдей хэш мәнін беруі екіталай болғандықтан, деректердің тұтастығы жоғары сенімділікпен қамтамасыз етіледі. Екінші жағынан, құпия

кілт криптографиясы хабарламаларды шифрлау үшін өте ыңғайлы, осылайша құпиялылық пен қауіпсіздікті қамтамасыз етеді. Жіберуші хабарламаны шифрлау үшін әр хабарлама үшін сеанс кілтін жасай алады; алушыға хабарламаны шифрлау үшін бірдей сеанс кілті қажет.

Кілттермен алмасу, әрине, ашық кілт криптографиясының негізгі қосымшасы болып табылады. Асимметриялық тізбектерді пайдаланушыларды аутентификациялауға қолдануға болады; егер алушы жіберушінің жеке кілтімен шифрланған сеанс кілтін ала алса, онда тек осы жіберуші хабарлама жібере алады. Ашық кілт криптографиясын хабарламаларды шифрлау үшін теориялық тұрғыдан да қолдануға болады, бірақ бұл сирек жасалады, өйткені құпия кілт криптографиясының алгоритмдері әдетте ашық кілт криптографиясының алгоритмдеріне қарағанда 1000 есе жылдам орындалуы мүмкін.

Ашық және құпия, хэш,сандық қолтаңба мен сандық конвертті қамтитын қауіпсіз берілісті қалыптастыру үшін осы функциялардың барлығын қалай біріктіретіні көрсетілген. Бұл мысалда хабарлама жіберуші-Алиса, ал алушы-Айдос. Сандық конвертте шифрланған хабарлама және шифрланған сеанс кілті бар. Алиса өзінің хабарламасын сеанс кілтімен шифрлау үшін құпия кілт криптографиясын қолданады, ол әр сессияда кездейсоқ пайда болады. Содан кейін Алиса Айдостың ашық кілтін пайдаланып сеанс кілтін шифрлайды. Шифрланған хабарлама мен шифрланған сеанс кілті бірге сандық конвертті құрайды. Хабарламаны алғаннан кейін Айдос сеанстың құпия кілтін өзінің жеке кілтімен қалпына келтіреді, содан кейін шифрланған хабарламаның шифрын шешеді.

Цифрлық қолтаңба екі кезеңде қалыптасады. Біріншіден, Алиса өзінің хабарының хэш мәнін есептейді; содан кейін ол хэш мәнін өзінің жеке кілтімен шифрлайды. Сандық қолтаңбаны алғаннан кейін, Айдос Алисаның ашық кілтімен сандық қолтаңбаны шифрлау арқылы Алиса есептеген хэш мәнін қалпына келтіреді. Айдос хэш функциясын Алисаның бастапқы хабарламасына қолдана алады . Егер алынған хэш мәні Алиса жіберген мәнге сәйкес келмесе, онда Айдос хабарламаның өзгергенін біледі; егер хэш мәндері сәйкес келсе, ол алған хабарламаны Алиса жіберген хабарламамен бірдей деп санауы керек. Бұл диаграмма бізге жалпы түрдегі криптожүйені ұсынады, онда сеанс кілті тек бір сессияда қолданылады. Егер бұл сеанс кілті қандай да бір жолмен бұзылса да, тек сол сеанс бұзылады; келесі сессияға арналған сессия кілті сол сессияның кілтіне негізделмейді, өйткені сол сессияның кілті алдыңғы сессияның кілтіне тәуелді емес. Бұл мінсіз тікелей құпиялылық ретінде белгілі; ымыраға байланысты сіз бір сеанс кілтін жоғалтуыңыз мүмкін, бірақ сіз олардың бәрін жоғалтпайсыз. (Бұл Heartbleed деп аталатын 2014 жылғы OpenSSL жобасында проблема болды.)



1.3 Сурет– Қауіпсіз байланыс үшін үш криптографиялық әдістерін пайдалану.

2 Арнайы бөлім

2.1 GSM стандартындағы абоненттің деректерін шифрлау процедурасы

Ғаламдық ұялы байланыс жүйесі (GSM) - бұл бүкіл әлемде қабылданған сандық ұялы стандарт. GSM-жалпы еуропалық құру үшін 1982 жылы құрылған стандарттау тобының атауы.900 МГц жиілікте жұмыс істейтін жалпы еуропалық Мобильді Ұялы байланыс жүйесінің ерекшеліктерін тұжырымдайтын мобильді телефон стандарты. GSM-де қауіпсіздік үш нысанда жүзеге асырылады: SIM-карта, GSM-телефон және желі. Абонентті сәйкестендіру модулі (SIM) мыналарды қамтиды: - IMSI - TMSI-PIN, -MSISDN-ki аутентификация кілті (64-бит) -A8 алгоритмін құратын шифрлау кілті (Kc) және-A3 аутентификация алгоритмі. SIM-бұл операциялық жүйені (ОЖ), файлдық жүйені және қосымшаларды қамтитын бір чипті компьютер. SIM картасы PIN-кодпен қорғалған және операторға тиесілі. SIM қосымшаларын SIM құралдар жиынтығымен жазуға болады

GSM қауіпсіздігінің кемшілігі-шифрлау. GSM желілері бекітілген қауіпсіз желілерді пайдаланады, сондықтан шифрлау қажет емес. Операторлар екі нүктелі микротолқынды байланыс желілерін, бөлінген сызықты, кейде тіпті интернет өз желілерінің әртүрлі бөліктерін қосуға арналған. Мұның тағы бір

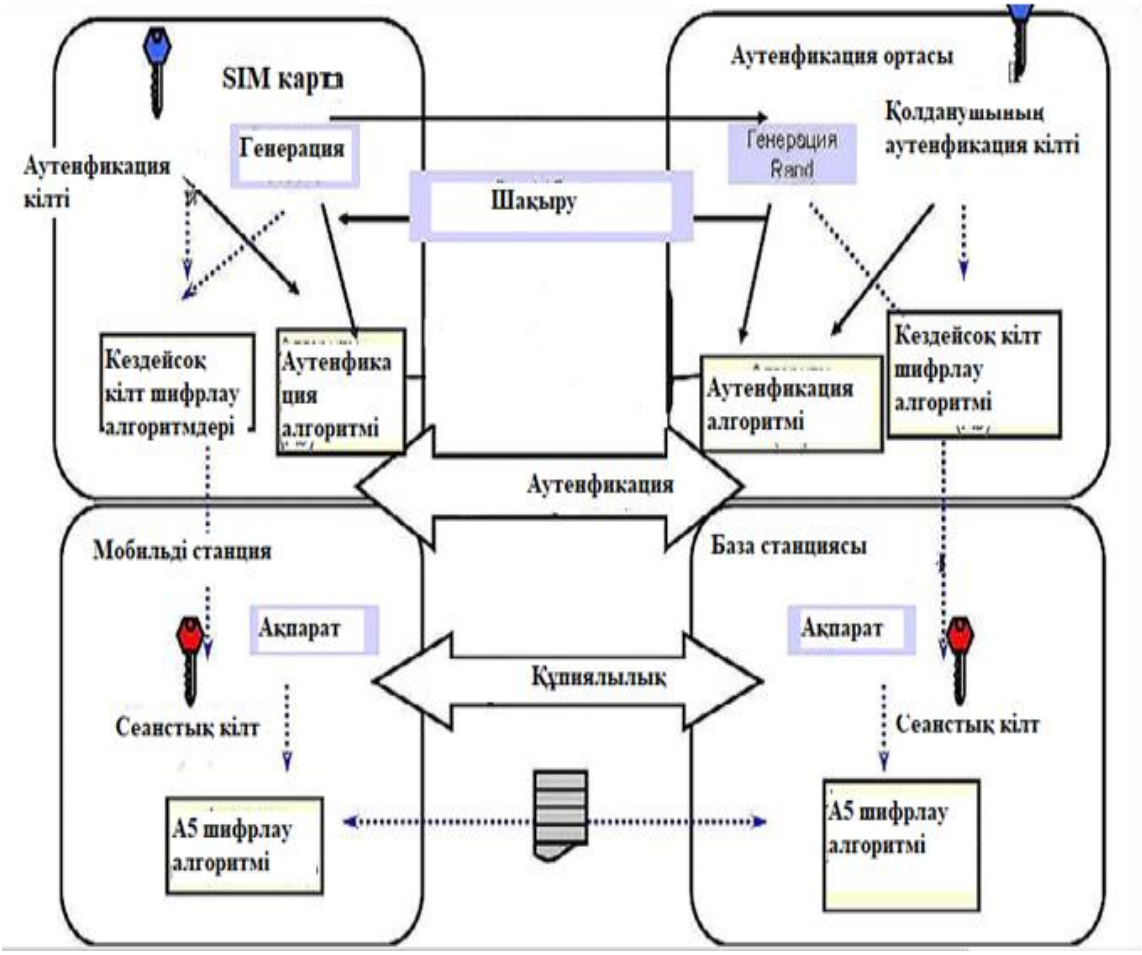
кемшілігі жағдай мынада, операторлардың қызметкерлері абоненттердің деректеріне қол жеткізе алады.

GSM телефонында A5 шифрлау алгоритмі бар.Желі алгоритмдерді қолданады. Аутентификация үшін A3, шифрлау үшін A5:A5-ағынды шифр қолданылады. Мұны аппараттық құралда өте тиімді жүзеге асыруға болады. Оның дизайны ешқашан жария етілмеген. A5-тің бірнеше нұсқалары бар: A5/1 (қазіргі кезде кеңінен қолданылады), A5/2 (A5/1-ге қарағанда әлсіз; кейбір елдерде қолданылады) және A5/3 (Касуми блок шифріне негізделген соңғы нұсқа).

Жалпы деректерді шифрлау үшін A8; ki, IMEI және IMSI аутентификация орталығында сақталады. SIM-картада A3 және A8 алгоритмдері іске асырылған. Оператор қандай алгоритмді қолдану керектігін шеше алады. Алгоритмнің орындалуы жабдық өндірушілері мен желілік операторларға тәуелді емес. SIM картасында 64 биттік шифрлау кілтін (Kc) жасау үшін қолданылатын шифрлау кілтін (A8) құру алгоритмі бар. Бұл кілт аутентификация процесінде қолданылатын кездейсоқ санды (RAND) абоненттің жеке аутентификация кілтімен (ki) шифрлау кілтін (A8) құру алгоритміне қолдану арқылы есептеледі. GSM шифрлау кілтін өзгерту мүмкіндігімен қосымша қауіпсіздік деңгейін қамтамасыз етеді, бұл жүйені тыңдауға төзімді етеді. Шифрлау кілтін қажет болған жағдайда жүйелі түрде өзгертуге болады. Аутентификация процесі сияқты, шифрлау кілтін есептеу (Kc) SIM ішінде жүреді. Сондықтан абонентті аутентификациялаудың жеке кілті (Ki) сияқты құпия ақпарат ешқашан SIM-картамен ашылмайды. Ms және желі арасында шифрланған дауыстық және деректерді беру A5 шифрлау алгоритмін қолдану арқылы жүзеге асырылады. Шифрланған байланыс GSM желісінен шифрлау режимін сұрау командасымен басталады. Бұл пәрменді алған кезде мобильді станция шифрлау алгоритмі (A5) және шифрлау кілті (Kc) арқылы деректерді шифрлауды және шифрлауды бастайды. Абоненттің жеке басының құпиялылығын қамтамасыз ету үшін уақытша мобильді абонент идентификаторы (TMSI) қолданылады. Аутентификация және шифрлау процедураларын орындағаннан кейін tmsi мобильді станцияға жіберіледі. Алғаннан кейін мобильді станция жауап береді. TMSI берілген жерде жарамды. Орналасу аймағынан тыс жерде байланыс орнату үшін TMSI-ге қосымша орналасу аймағын (LAI) анықтау қажет.

Мобильді абоненттің уақытша идентификаторы (TMSI) — бұл көбінесе ұялы телефон мен желі арасында берілетін идентификатор. TMSI кездейсоқ түрде VLR-ді осы аймақтағы әрбір ұялы телефонға, ол қосылған кезде тағайындайды. Нөмір орналасқан жер үшін жергілікті болып табылады, сондықтан ұялы телефон Жаңа географиялық аймаққа ауысқан сайын оны жаңарту қажет. Желі ұялы телефонның TMSI-ді кез келген уақытта өзгерте алады. Ол әдетте абонентті анықтамау және радио интерфейсіндегі тыңдау құрылғыларын бақылау үшін жасайды. Бұл ұялы телефонның қайсысы екенін бақылауды қиындатады, ұялы телефон тек қосылған кезде немесе ұялы телефондағы деректер қандай да бір себептермен жарамсыз болған кезде қысқа уақытты қоспағанда. Осы кезде ғаламдық "халықаралық мобильді абонентті

сәйкестендіру" (IMSI) желіге жіберілуі керек. IMSI оны анықтау мен бақылауды болдырмау үшін мүмкіндігінше аз жіберіледі.



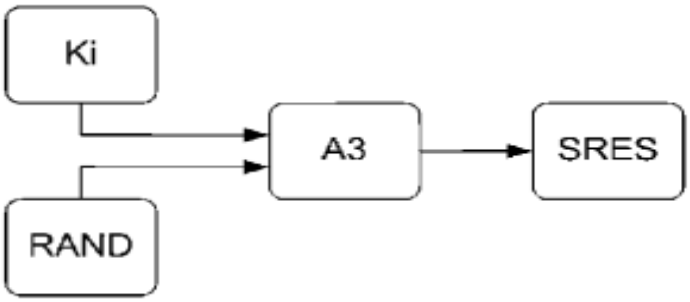
2.1 Сурет– GSM желілерінде қолданылатын шифрлау алгоритмінің сипаттамасы

Бұл суретте келесі қадамдар схемалық түрде көрсетілген:

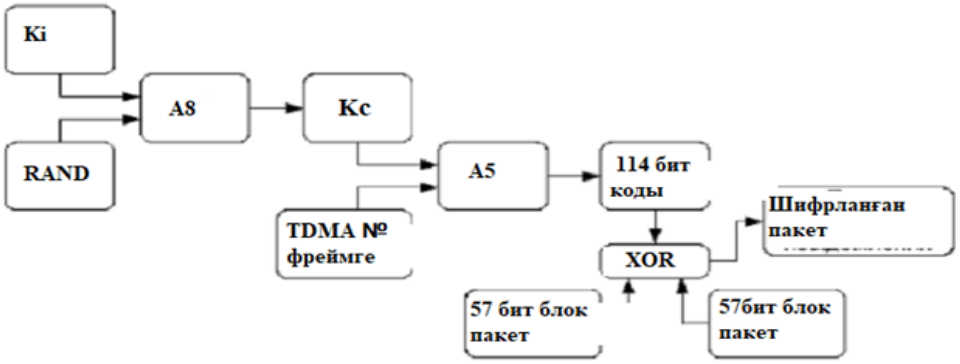
1. Оператордың телефоны желіге қосылады.
2. Оның түпнұсқалығын растау үшін телефон TMSI (Temporary Mobile Subscriber Identity) деп аталатын арнайы сәйкестендіру кодын жібереді.
3. Аутентификация орталығы 128 биттік кездейсоқ Rand санын жасайды және оны мобильді станцияға (МС) жібереді.
4. МС өзінің құпия кілтін және А3 аутентификация алгоритмін қолдана отырып, алынған RAND санын шифрлайды.
5. МС алдыңғы қадамда алынған тізбектен алғашқы 32 битті алады(оларды SRES (signed response) деп атайық) және оларды қайтадан АО-ға жібереді.
6. АО бірдей операцияны жасайды және 32 биттік xres(кеңейтілген жауап) тізбегін алады.
7. Егер екі мән бірдей болса, телефон аутентификацияланған болып саналады.

8. МС және АО сеанстық шифрлау кілтін құпия кілтін және (RAND) кілт алгоритмін қолдана отырып есептейді.

А3 аутентификация алгоритмдері және А8 кілтін қалыптастыру алгоритмі туралы айтатын болсақ, іс жүзінде көптеген ұялы байланыс операторлары осы мақсатта COMP128 деп аталатын бір алгоритмді қолданады(оның COMP128-1, COMP128-2, COMP128-3 көптеген модификациялары бар). COMP128-бұл 128 биттік тізбекті қабылдайтын және шығуда 96 биттік қайтаратын қарапайым хэш функциясы. GSM стандартында ақпараттық қауіпсіздік саясаты абонентті сәйкестендіру және аутентификациялау, сондай-ақ оның сөйлеу сигналын шифрлау тетіктерінен тұрады. Пайдаланушыны анықтауға болатын негізгі элемент-IMSI (International Mobile Subscriber Identity) халықаралық сәйкестендіру нөмірі, ki аутентификациясының бірегей кілті және А3 аутентификация алгоритмі бар SIM картасы. Абонентті тіркеу кезінде үй желісінің авторизациялау орталығы 128 биттік кездейсоқ Rand (Random) санын жасайды және оны пайдаланушының телефонына жібереді. SIM картасында ki кілті мен А3 алгоритмін қолдана отырып, 32 биттік Sres жауаптары (қол қойылған нәтиже) суретте көрсетілген схема бойынша есептеледі.



2.2 Сурет– GSM стандартында авторизация үшін жауап қалыптастыру процедурасы



2.3 Сурет– GSM стандартындағы абоненттің деректерін шифрлау процедурасы

2.2 Ұялы байланыс жүйесіне қолданылатын криптологиялық шабуылдау технологясы

Біз шабуылды "корреляциялық шабуылдар" деп аталатын қарапайым түрде жүзеге асырамыз. Қарастырып отырған шабуылды алғаш рет 2002 жылы екі зерттеуші сипаттаған: Патрик Экдахл және Томас Джонсон.

Инициализация процедурасының анықтамасынан регистрлердің бастапқы күйі k сеансының кілті мен FN кадр нөмірінің сызықтық функциясы деп қорытынды жасауға болады.

Сондай-ақ, генератордың шығу биті XOR шығыс екенін біле отырып, барлық үш регистрді біз келесі теңдіктей жаза аламыз:

$$s_i^1 \oplus s_i^2 \oplus s_i^3 \oplus f_i^1 \oplus f_i^2 \oplus f_i^3 = x \qquad (2.1)$$

Мұндағы, s_i-тек f_i кілт биттерін жүктегеннен кейін регистрлер құратын реттілік, ал f_i тек кадр нөмірінің биттерін жүктегеннен кейін, ал x-регистрдің шығу биті болып табылады.

Инициализация анықтамасынан біз алгоритмнің алғашқы 100 циклі "бос" жұмыс істейтінін білеміз, яғни ешқандай шығыс биттерін шығармайды, ал шығу тізбегінің бірінші биті іс жүзінде 101-ші бит болып табылады. Осылайша, әр қадамда әр регистрдің жылжу ықтималдығы 3/4 екенін ескерсек, 101 қадамнан кейін әр регистр дәл 76 рет ауысады деген болжам жасауға болады. Сондықтан (2.1) формуласы мына түрге айналады:

$$s_{76}^1 \oplus s_{76}^2 \oplus s_{76}^3 = x_1 \oplus f_{76}^1 \oplus f_{76}^2 \oplus f_{76}^3 \qquad (2.2)$$

Оң жақ бөлігі деңгейінің формуласын:

$$s_{76}^1 \oplus s_{76}^2 \oplus s_{76}^3 = O_{(76,76,76,1)}^j \qquad (2.3)$$

Өйткені өрнек оң жақта (2.3) біз білеміз, s негізгі реттілігі туралы 1 бит ақпарат аламыз, атап айтқанда инициализациядан кейін әр регистрдің 76-шы позициясының жағдайы туралы хабар келеді. Осылайша әрекет ете отырып, біз 102 позицияда R1 76 позициясында қалды деп болжай аламыз, ал R2 және R3 регистрлері 77 позициясына көшті, осылайша біз 77-ші регистр позициясы туралы ақпарат аламыз және т.б. бастапқы күйді сәтті қалпына келтіру үшін барлығы 64 битті ашуымыз керек.

Әрине, жағдай (76,76,76) 101 қадамында өте төмен ықтималдылықпен туындайды, егер біз осылай әрекет етуді ұйғарсақ, 101 ауысымнан кейін әр регистр 76 позицияға айналдырылғанға дейін көптеген кадрларды

сұрыптауымыз керек еді. Ekdahl және Johansson кадрларының қажетті санын азайту үшін келесі әдісті ұсынды.

Регистрлер үшін (cl1,cl2,cl3) рет айналатын нақты позицияны болжаудың қажеті жоқ. Ықтималдылықтың үлкен үлесімен әр регистр I=[100,140] сегментінде 76-дан 102-ге дейін өзгеретінін білу жеткілікті.

Осылайша, әр кадр үшін ықтималдылықты есептей аламыз:

$$Pr\{s_1(cl_1)\oplus s_2(cl_2)\oplus s_3(cl_3)=0\}=\sum_{t\in I}P_r\{(cl_1,cl_2,cl_3)\}*\left[O^{j}_{cl1,cl2,cl3,100-t}\right]+\frac{1}{2}*(1-\sum_{t\in I}Pr\{(cl_1,cl_2,cl_3)\}) \quad (2.4)$$

Мұнда,

$$Pr\{cl_1,cl_2,cl_3\}=\frac{\left(\frac{t}{t-cl1}\right)\left(\frac{t-(t-cl1)}{t-cl2}\right)\left(\frac{t-(t-cl1)-(t-cl2)}{t-cl3}\right)}{4^t} \quad (2.5)$$

Бұл t-ші биттің регистрлердің позицияларынан пайда болу ықтималдығын білдіреді (cl1, cl2, cl3).

Әрбір қол жетімді кадр үшін (2.4) есептеу арқылы алынған ықтималдықтар логарифмнің орташасы болады:

$$\Delta_{(cl1,cl2,cl3)}=\sum_{j=1}^{m}ln\frac{Pr^j\{s_1(cl_1)\oplus s_2(cl_2)\oplus s_3(cl_3)=0\}}{1-Pr^j\{s_1(cl_1)\oplus s_2(cl_2)\oplus s_3(cl_3)=0\}} \quad (2.6)$$

Егер (2.6)>0 болса, онда s1(cl1)⊕S2(cl2)⊕S3(cl3)=0, әйтпесе s1(cl1)⊕S2(cl2)⊕S3(cl3)=1.

Шабуылды толығымен алгоритм түрінде сипаттаймыз:

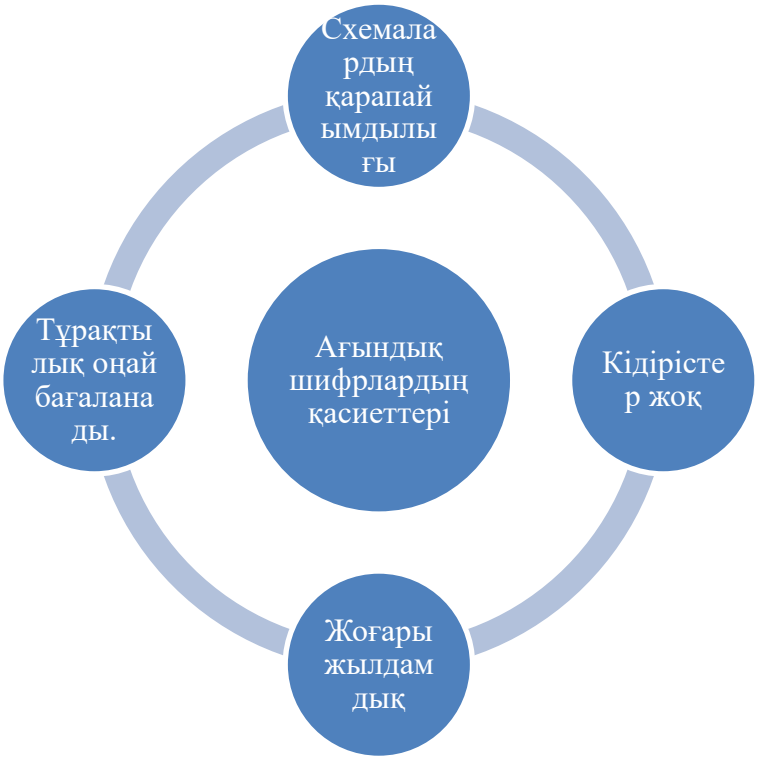
С аралығын таңдаg, мысалы c=[79,86]. Cl1,cl2,cl3 айнымалылары барлық мәндерді c аралығынан шығарсын, әр кадр үшін есептейміз.

Δ мәні негізінде S1(cl1)⊕S2(cl2)⊕S3(cl3)мәнін таңдаймыз.

Бұл алгоритмді орындау нәтижесі 8 белгісізден тұратын S1(79)⊕S2(79)⊕s3(79)=0 түріндегі 512 теңдеу болады. Бұл теңдеулер жүйесін қарапайым санау арқылы шеше отырып, біз әр регистрдің бастапқы мәнінен 8 бит аламыз.

Алгоритмді интервалдар үшін тағы екі рет қайталай отырып [87, 94] және [95, 102] біз әр регистрдің бастапқы күйінің 24 битін аламыз. Бұл бізге жеткілікті. Біз регистрлердің әрқайсысын 101 рет айналдырамыз, біз екінші инициализация қадамынан кейін, яғни регистрлерге негізгі биттерді жүктегеннен кейін регистрлердің күйін аламыз. Енді біз барлық негізгі тізбекті құра аламыз.

2.3 Ағындық шифрлау немесе файлдарды шифрлауды жүзеге асыру

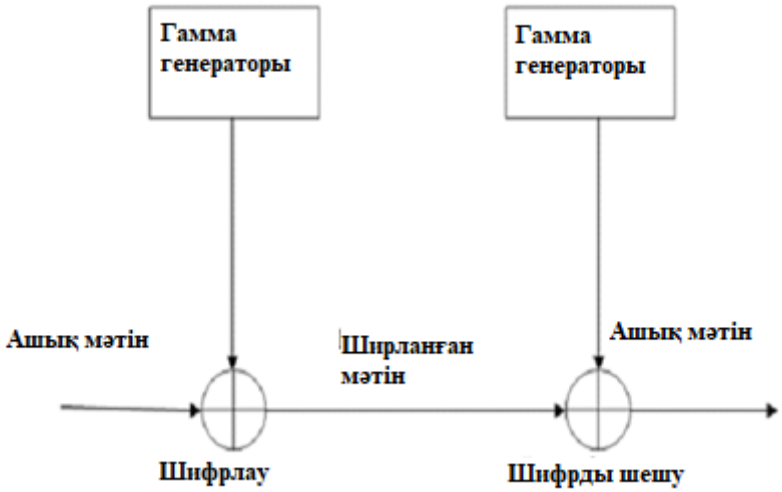


2.1 кесте–Ағындық шифрлардың қасиеттері

Ағындық шифр-қолданылатын кілтке және оның мәтіндік ағындағы позициясына байланысты ашық мәтіннің әрбір элементі шифрланған түрге аударылатын шифрдың симметриялы түрі.

Ағындық шифрдың ерекшелігі-шифрдың блоктық түрімен салыстырғанда шифрлау процесіне басқаша көзқарас. Бұл жоғары деңгейлі API хабарлама тізбегін немесе блоктардың еркін санына бөлінген бір хабарламаны келесі қасиеттері бар құпия кілтпен шифрлайды:Хабарлар мүмкін емес усечены, жойылуы, переупорядочены, дубляж жасалуға немесе өзгертілген жоқ табылған бұл функциялары ашып көрсету. Екі рет шифрланған бірдей реттілік әр түрлі шифрланған мәтіндерді жасайды. Әрбір шифрланған хабарламаға аутентификация тегі қосылады: ағынның зақымдануы ертерек анықталады, ағынды соңына дейін оқымай-ақ. Аутентификация тегін есептеу кезінде әр хабарламада қосымша мәліметтер болуы мүмкін. Хабарламалар әртүрлі мөлшерде болуы мүмкін. Ағынның жалпы ұзындығына немесе жеке хабарламалардың жалпы санына практикалық шектеулер жоқ. Ағынның кез келген нүктесінде алдыңғы хабарламаларды шифрлау үшін пайдаланылатын кілтті "ұмытып", жаңа кілтке ауысуға болады. Бұл API-ді "тең-теңімен" Түйініне реттелген хабарламалар тізбегін қауіпсіз жіберу үшін пайдалануға болады. Ағынның ұзындығы шектеусіз болғандықтан, оны көлеміне қарамастан

файлдарды шифрлау үшін де қолдануға болады. Ол nonces-ті мөлдір түрде жасайды және перне бұрылуын автоматты түрде өңдейді.



2.2 Сурет– биті гаммалау сұлбасы

Ағымдағы шифрларды жобалау кезінде келесі тәсілдердің бірі қолданылады:

- жүйелік-теориялық-криптоаналитик әлі белгісіз және зерттелмеген мәселені құруға негізделген;
- ақпараттық-техникалық-криптоаналитиктен шешімді жасыру әрекетіне негізделген;
- күрделі-теориялық-белгілі, бірақ күрделі проблемаға негізделген тәсіл;
- рандомизацияланған-шешім мүмкін емес болып көрінетін көлемді тапсырма жасалатын тәсіл.

Ағындық шифрлар: түрлері, артықшылықтары мен кемшіліктері, сипаттамалары

Ағын шифрінің сипаттамалары:

- кіріс деректер ағынының жылдамдығымен жүретін Жоғары шифрлау жылдамдығы. Ақпаратты шифрлау онлайн режимінде жүреді, ағынның бит тереңдігіне және түрлендірілетін деректер көлеміне байланысты емес;
- ақаулардың (қателіктердің) көбею әсерінің болмауы. Шифрды шешкеннен кейін қатесіз дәйектілік элементтерінің көлемі шифрлаудан кейін бұрмаланған деректер көлеміне тең болады;
- ағындық кілт құрылымы криптоаналитикке қажетті кілт деректерін шығаруға мүмкіндік беретін осалдықтарға ие;
- ағын шифріне сызықтық алгебраның көмегімен шабуыл жасауға болады. Ағынды шифрларды бұзу талдаудың танымал түрлерінің бірі - ағынды немесе сызықты көмегімен мүмкін болады;

- ағындық шифрларды бұзу әдістері әртүрлі. Блоктық шифрлардан айырмашылығы, мұнда жеке шифрлау алгоритмдеріне назар аударылмайды;

- ағынды шифрларды әзірлеу, әдетте, Еуропаның криптографиялық орталықтарында жүзеге асырылады (мысалы, АҚШ-та блоктық шифрлар жасалады); зерттеу ағымды деректерге шифрларының белсенді өтуде.

2.4 Өзіндік және синхронды шифрлаудың артықшылықтары мен кемшіліктері

Синхронды ағынды шифрлар-бұл шифрлау түрі, онда кілт ағыны шифрмәтін мен ашық мәтінге қарамастан пайда болады. Шифрлау кезінде кілт генераторы шифрлау кезінде қолданылатынға ұқсас бит ағындарын шығарады. Шифрмәтін белгісінің жоғалуы генераторлар арасындағы синхрондаудың бұзылуына және мәтіннің қалған бөлігінің шифрын шешуге байланысты проблемаларға әкеледі.

Синхронды ағынды шифрлардың артықшылықтары:

- ықтимал кірістірулерден қорғау және шифрланған мәтінді жою. Мұндай манипуляциялар синхрондау әкеледі және әрқашан анықталады;

- қатенің таралуымен проблемалардың болмауы. Егер бір бит бұрмаланса, ол дұрыс шешілмейді.

Синхронды шифр ағындарының кемшіліктері:

- шифрмәтіннің белгілі бір биттерін өзгерту мүмкіндігі. Егер қолыңызда ашық мәтін болса, шабуылдаушы биттерді қажетінше реттей алады.

Өздігінен синхрондалатын ағынды шифрлар-бұл асинхронды ағынды шифрлардың бір түрі, онда кілт ағынын құру кілттің өзіне және шифрланған мәтін белгілерінің белгіленген санына жүктеледі. Әр хабарлама кездейсоқ тақырыптан белгілі бір (N) биттен басталады.

Асинхронды ағынды шифрлардың артықшылықтары:

- кодталған ақпараттың статистикасын араластыру. Ашық деректердің статистикалық қасиеттері мәтіннің бүкіл көлеміне қолданылады, өйткені әр белгі келесі Шифр мәтініне әсер етеді;

- ашық деректердің артықтығына негізделген шабуылдарға төзімділік.

Асинхронды ағынды шифрлардың кемшіліктері:

- қайталама берілістің ашылуына сезімталдық;

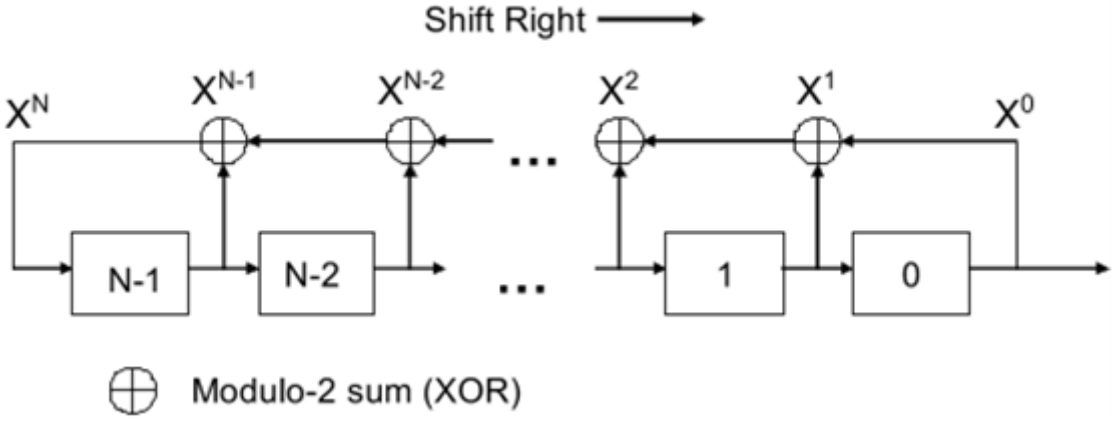
- қателіктердің таралу қаупі. Шифрланған мәтіннің әр дұрыс емес биті үшін N ашық мәтіндік қателер берілген.

2.5 СКБЖР қарапайым көпмүшеге негізделген қасиеттері

СКБЖР шығу тізбегі, қарапайым көпмүшеге негізделген ие қасиеттері:

1. нөлдер саны және бірлік тепе-теңдікте орналасқан(бір артық бірлікке)
2. терезелер-шығу реті барлық мүмкін нұсқаларды қамтиды
3. бір-бір реттен бойынша тіркелімдерді толтыру (нөлдіктен басқа).
4. СКБЖР негізіндегі G генераторының болмауы

Ауыстыру регистрі D триггерлерін біріктірген кезде алынады. Тактілік кірістер бір-біріне қосылады және ығысу регистрінің тактілік кірісі болып табылады. Әр триггердің шығысы ығысу регистрінің шығысы болып табылады және бір уақытта келесі триггердің кірісіне қосылады. Нөлдік триггер кірісі-ығысу регистрінің кірісі. Регистрдің шығуынан оның кірісіне сигнал беру фактісі кері байланыс жасайды.



2.3 Сурет – екі модуль бойынша есептелген регистр

Беріліс қателіктерін жылдам тексеруді қамтамасыз ету үшін қолданылатын циклдік резервті тексеру математикасы LFSR арифметикасымен тығыз байланысты. Жалпы, арифметикасы оларды үйренуге және жүзеге асыруға арналған объект ретінде қызмет етеді. Қарапайым құрылыс блоктарын қолдана отырып, салыстырмалы түрде күрделі логиканы жасауға болады.

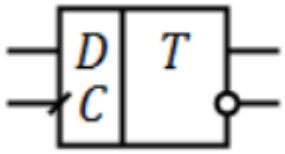
2.6 D-триггер және сызықтық кері байланысы бар жылжу регистрынның оңтайлы ұзындығы

Триггер-бұл екі тұрақты күйдің бірінде ұзақ уақыт болу және оларды сыртқы сигналдардың әсерінен ауыстыру мүмкіндігі бар электрондық құрылғы.

D - триггер-кіріс күйін сақтайтын және шығу жай-күйі бейнеленеді триггер.

Құрылғының электр тізбегінде D-триггер төмендегі суреттегідей көрінеді. Триггердің бұл түрінде міндетті түрде үш Шығыс бар: D (кіріс), C (синхрондау кірісі, сағат кірісі, сағат кірісі, clk, clock) және Q (Шығыс). Олардан бөлек болуы мүмкін тағы: инвертированный шығу, кіру және түсіру қондырғылары

маңызы бар шығу, кіру рұқсаты бар. Дегенмен, жұмыстың мәні үш міндетті қорытындының өзара әрекеттесуінде жатыр, сондықтан біз оларды қарастырамыз.



2.4 Сурет– D-триггердің шартты графикалық белгіленуі

2.2 кесте – Бастапқы және соңғы күйі

Бастапқы күйі		Тактілік импульсін бергеннен кейінгі күйі	
Кіру (D)	Шығу (Q)	Кіру (D)	Шығу (Q)
0	0	0	0
0	1	0	0
1	0	1	1
1	1	1	1

D-триггер жұмыс принципі келесідей: сағат сигналы с кірісіне берілген кезде, шығыс күйі кіріс күйіне тең болады. Яғни, егер белгілі бір уақытта кірісте "нөл" болса, ал шығуда "бірлік" болса, сағат сигналын беру кезінде шығыс кіріс күйін қабылдап, "нөлге"айналады.

2.7 Құпия белгісіз шифр (SUC)

Құпия белгісіз шифр (SUC) - бұл чиптің ішінде кездейсоқ және ішкі түрде жасалған, алдын-ала болжанбайтын шифр. Мұнда пайдаланушы өзі жасаған шифрлау функцияларына әсер ете алмайды. Алынған шифр тұрақты, алынбайтын және рұқсатсыз кіруден қорғалған болып табылады. Тіпті құрылғы өндірушісі де құру процесін бақылай алмауы керек, сонымен қатар алынған шифрды болжамды түрде аша алмауы тиіс.

Шифрларды ендіруге арналған ең жақсы құрылғылар-бұл шифрланбаған және өздігінен конфигурацияланатын чиптік жүйе құрылғылары (SOC).

Әрбір құрылған мәнді шифрлау режимінде қайтымды жалған кездейсоқ функция (PRF) ретінде анықтауға болады:

$$SUC : \{0,1\}^n \to \{0,1\}^m \quad (2.7)$$

$$X \to^{\mathrm{PRF}} \mathrm{Y} \quad (2.8)$$

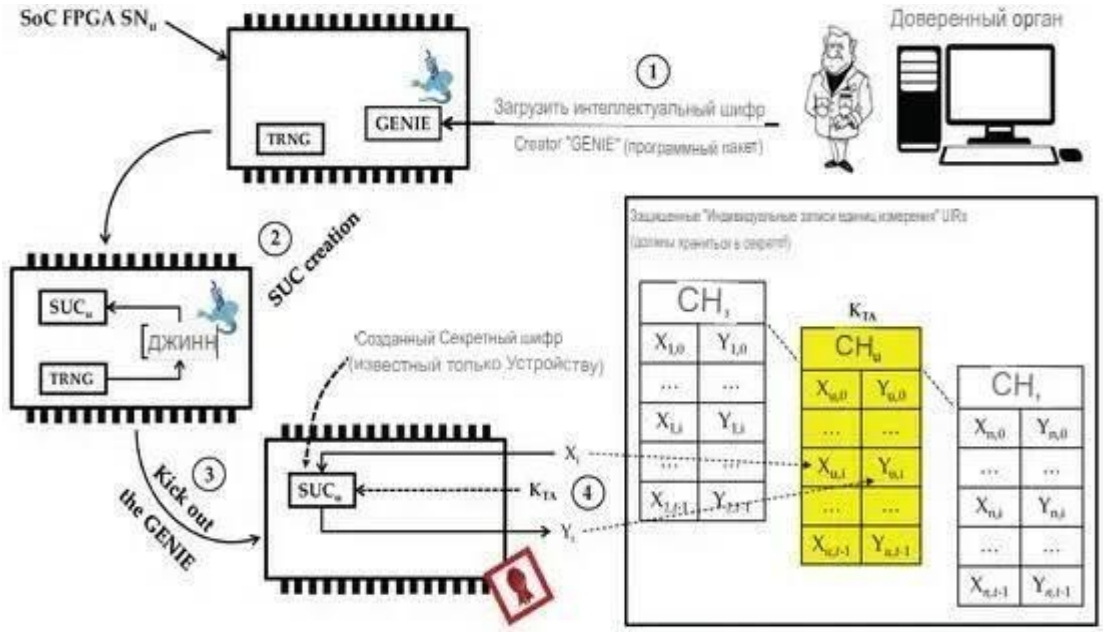
Шифрлау режимінде:

$$SUC^{-1}: \{0,1\}^m \to \{0,1\}^n \quad (2.9)$$

$$X \rightarrow^{PRF^{-1}} Y \quad (3)$$

Егер n = m болса, онда SUC блок шифры ретінде жасалған. Яғни SUC = SUC^{-1}, онда:

2.5-суретте мұндай құрылғыны FPGA-ға енгізудің тұжырымдамалық сценарийі сипатталған-System on Chip (SoC) құрылғысы. Құрылғыны жекелендіру процесі (SoC FPGA) келесідей:



2.5 Сурет– FPGA SoC ортасын құру тұжырымдамасы

Сенімді орта (ТА) бағдарламалық жасақтаманы "GENIE"деп аталатын ақылды шифр жасаушы ретінде жүктейді. "Джиннің тұжырымдамасы" 1001 ғажайыптар түнінен "Аладдиннің шамынан шығып, кез-келген қалауды орындай алатын күшті, адал және мойынсұнғыш тіршілік иесі ретінде алынған". Содан кейін ДЖИНГЕ рандомизацияланған, болжанбайтын және белгісіз нәтижелерге кепілдік беру үшін SoC-де орналасқан кездейсоқ сандар генераторы (TRNG) арқылы болжанбайтын шифр (SUC) жасауға бұйрық беріледі. GENIE құрылған файлды FPGA құрылымында белгісіз жерде /жерлерде үнемі сақтайды және оны деректерді шифрлау мен шифрын шешуге жарамды етеді. Джин шығарылады (яғни, бағдарлама ретінде алынып, құрылғыдан біржола кетуді бұйырады). Ең соңғы нәтиже-ешкім білмейтін қолдануға болатын шифр жасалынады. Жасалған шифрлар әр түрлі болады. Тіркеудің осы кезеңінде ТА әр SUC-ны t-ашық мәтін шаблондарын $\{X\} = X_{u,0} \dots X_{u,t-1}$ теру арқылы сұрайды. Шифрланған мәтіннің тиісті жиынтығын құру үшін $\{Y\} = (Y_{u,0} \dots Y_{u,t-1})$, мұндағы $Y_i = SUC_u(X_i)$. Содан кейін ТА $\frac{X}{Y}$ жұптарын тиісті аймақта құрылғының SN_u сериялық нөмірімен белгіленген жеке жазбалардың (UIR) бірліктерінде сақтайды. $\frac{X_i}{Y_I}$ жұптары кейінірек $\frac{TA}{TA'}$ құрылғыларды анықтау және аутентификациялау үшін қолданылады. Бірнеше

ТА бірдей интерфейсті қолдана отырып, жеке қосымшасы үшін толығымен дербес жұмыс істей алады.

$$SUC : \{0,1\}^n \to \{0,1\}^n \quad (3.1)$$

$$SUC\big(SUC(X)\big) = X \text{ немесе } X \in \{0,1\}^n \quad (3.2)$$

Бұл тұжырымдама Керкхоффа принциптеріне қайшы емес. Екі жағдайды қарастырсақ :

1. Жарияланған GENIE жағдайы: қарсылас шифрды жобалаудың барлық ережелерін біледі. Егер шифр класының мөлшері $|SUC|$ =үлкен болса, онда:

$$|SUC| = N \text{ және } N, \text{яғни } N \longrightarrow \infty , \quad (3.3)$$

Әр шифр кездейсоқ түрде бірдей таңдалады. Егер SUC тең кілт өлшеміне ие болса, онда SUC клондаудың жалпы энтропиясы:

$$CE_{max} = log_2 N + k \quad (3.4)$$

Себебі шифр де, оның кілті де белгісіз. Сонымен қатар, егер шабуылдаушы GENIE дизайнының әлсіздігінен шифр тапса, онда минималды мәні $CE_{min} = k$ тең болады. Егер GENIE дизайнері жақсы заманауи криптограф болса, клондау энтропиясы мына мәнге жақындайды:

$$CE_{max} = log_2 N + k \quad (3.5)$$

2.Жарияланбаған GENIE жағдайы: SUC тұжырымдамасы жұмыс істеуі үшін GENIE-ді жариялаудың қажеті жоқ. Бұл жағдайда минималды CE:

$$CE_{min} = log_2 N_0 + k, \quad (3.6)$$

мұндағы N_0-бұл шифр класының жоғарғы шегі. Ұсынылған негізгі ағын генераторы/ағындық шифрлар тобының кері байланыс қауіпсіздігі шифр дизайны жалпыға белгілі екенін ескере отырып зерттеледі.

Кері байланыс ығысу регистрі жүйеде кері байланыс функциясы пайда болса, циклдерді жасайды, егер :

$$f(x_0, x_1, \dots, x_{N-1}) = x_0 \oplus g(x_1, \dots , x_{N-1}) \quad (3.7)$$

мұндағы g тәуелді емес кез-келген логикалық функция болып есептеледі.

Екілік Брейн тізбегі- бұл 2^N кезеңі бар және әр N-биттік кортеж бір реттілік кезеңі бар тізбек. N де Брюйн реті тізбегінің сызықтық күрделілігі шектеулі 2^{N-1}+N және 2^N-1 де көрсетіледі.

Де Брюйннің модификацияланған реттілігі−бұл 2^N-1 период тізбегі, онда әр N-биттік тізбек тізбектің бір кезеңінде дәл бір рет кездеседі.

N_i−bit бар әрбір NLFSR A_i үшін мұнда $4 \le N_i \le 24$, $2^{Ni}-1$ максималды кезеңін қамтамасыз ететін кері байланыс функциялары жиынтығы ұсынылды. Барлық кері байланыс функциялары теңдеу түрінде болады . Іздеу екі алгебралық дәрежесі бар кері байланыс функциясының үш түрін қамтыды:

$$f_1(x_0, x_1, \dots , x_{N-1}) = x_0 \oplus g_1(x_a, x_b, x_c , x_d) = x_0 \oplus x_a \oplus x_b \oplus x_c x_d \quad (3.8)$$

$$f_2(x_0, x_1, \dots , x_{N-1}) = x_0 \oplus g_2(x_a, x_b, x_c , x_d, x_e) x_0 \oplus x_a \oplus x_b x_c \oplus x_d x_e \quad (3.9)$$

$$f_3(x_0, x_1, \dots , x_{N-1}) x_0 \oplus g_3(x_a, x_b, x_c , x_d, x_e, x_h) x_0 \oplus x_a \oplus x_b \oplus x_c \oplus x_d \oplus x_e x_h \quad (4)$$

мұндағы $a, b, c, d, e, h \in \{1,2,\ldots,\ N-1\}$.

2^N-1 периоды бар N−биттік сызықты емес кері байланысы бар ығысу регистрі (NLFSR) Фибоначчидің кез-келген жиынтығын 4 ішкі жиынға бөлуге болады : негізгі, негізгі кері, негізгі және кері толықтырумен толықтырылады. Тек негізгі формасы бар NLFSR тізімделген. Негізгі форманың кері, қосымша және кері қосымша формалары келесідей сипатталады:

Кері түрі

$$f_r(x_0, x_1, \ldots, x_{N-1}) = x_0 \oplus g(x_{N-1}, \ldots, x_1) \quad (4.1)$$

Толықтауыш түрі

$$f_c(x_0, x_1, \ldots, x_{N-1}) = x_0 \oplus 1 \oplus g(x_1, \ldots, x_{N-1}) \quad (4.2)$$

Кері толықтауыш түрі

$$f_{rc}(x_0, x_1, \ldots, x_{N-1}) = x_0 \oplus 1 \oplus g(x_{N-1}, \ldots, x_1) \quad (4.3)$$

Осылайша, әрбір кері байланыс функциясы үшін кері, қосымша немесе кері толықтырулар тізбегін құратын үш кері байланыс функциясы шығарылуы мүмкін.

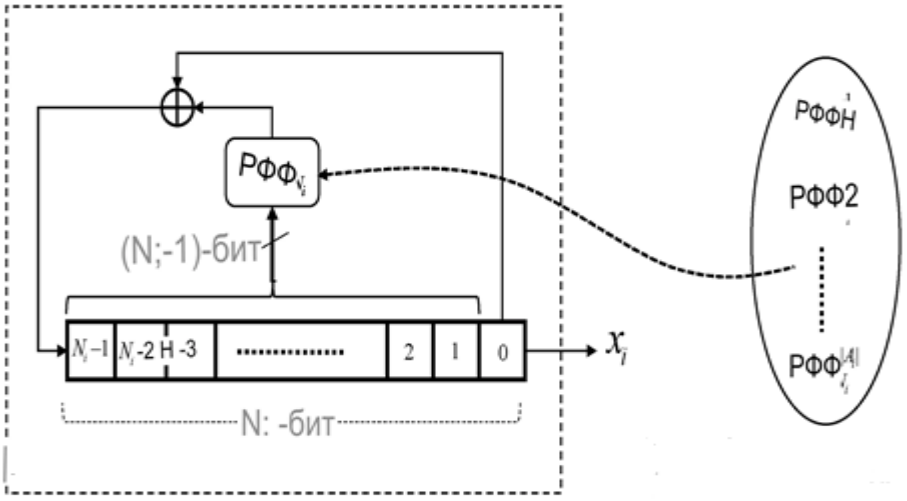
$N_i - bit, S_{N_i}$ тізімделген G логикалық функциялар жиынтығын, олардың кері қондырмасын қамтиды. Бұл функцияларды кездейсоқ кері байланыс (Rffnl) функциялары деп атаймыз.

Әрбір сызықты емес кері байланысы бар ығысу регистрі (NLFSR) Ai ұзындығы Ni үшін кері байланыс функциясы кездейсоқ кері байланыс функциясын (RFFNi) қамтиды. Оның жалпы формасы келесідей анықталады:

$$f(x_0, x_1, \ldots, x_{N-1}) = x_0 \oplus RFF_{N_i}(x_1, \ldots, x_{N-1}) \quad (4.4)$$

мұндағы: әрбір NLFSR үшін N_i ұзындығының A_i қатынасы S_{N_i} кездейсоқ кері байланыс мүмкіндіктерінің жиынтығы таңдалады, осылайша оның әрбір RFF_N^j NLFSR Ai максималды 2^{Ni}−1 кезеңіне жетуге мүмкіндік береді. Мұнда:

$$RFF_{N_i} \in S_{N_i} = \left\{RFF_{N_i}^1, \ldots, RFF_{N_i}^j, \ldots, RFF_{N_i}^{|A_i|}\right\} \quad (4.5)$$



2.6 Сурет– Таңдалған NLFSR жиынтығының жалпы құрылымы

Даралау процесінде кері байланыс функцияларының бірі әр NLFSR AI үшін алдын-ала анықталған жиынтықтан кездейсоқ таңдалуы керек.

4-суреттегі әрбір таңдалған NLFSR A_i 5-суреттегі жалпы құрылым пішініне ие және 2^{Ni}–1 периодтың сызықты емес тізбегін жасайды, Бұл де Брейннің сызықты емес модификацияланған тізбегі болып табылады. L_i NLFSR A_i сызықтық күрделілігі шектеулі кезде:

$$2^{N_{i-1}} + N_i \leq L_i \leq 2^{N_i} - 1 \qquad (4.6)$$

2.8 Ағынды шифрлардың сызықтық күрделілігі және Берлекэмп-Месси алгоритмі

Ұсынылған шифрдегі БМ алгоритмінің күрделілігін талдау үшін шығыс бит ағынының жалпы сызықтық күрделілігінің төменгі шегін есептеу керек. БМ алгоритмінің шабуылының уақыт күрделілігі жалпы сызықтық күрделіліктің квадратына тең. Егер ұзындығы N_1 болса, t-shift регистрлерінің N_1, … ,N_t жұптары салыстырмалы түрде қарапайым, z негізгі ағынының L (ζ) сызықтық күрделілігі белгілі:

$$L(\zeta) \geq F(L_1, \dots, L_t) \qquad (4.7)$$

Егер сызықтық кері байланысы бар жылжу регистрінің ұзындығы салыстырмалы түрде қарапайым болмаса, онда жоғарыда келтірілген бағалау орындалмайды. Бұл жағдайда $F(L_1,...,L_t)$ тек L(ζ) үшін жоғарғы шекараны қамтамасыз етеді.

$\sigma_1,...,\sigma_t$- қарапайым екілік сызықтық кері байланысы бар жылжу регистрі ұзындығының $N_1,...,N_t$ нөлдік емес шығу тізбегі сәйкесінше, L_1 сызықтық күрделілігіне ие. $F(x_1,..., x_t)$ - алгебралық дәреженің логикалық функциясы D ≥ 1. Тізбектің сызықтық күрделілігінің төменгі шегі ζ = F ($\sigma_1,...,\sigma_t$), егер келесі екі шарт орындалса:

1. Алгебралық қалыпты форма (ANF) F(x1,..,xt) құрамында $x_{i1},..,x_{id}$ дәрежесі d, ол үшін n_{i1} ығысу регистрінің тиісті ұзындығы салыстырмалы түрде қарапайым болады.

2.Барлық бірмүшелер үшін D дәрежесі бар,мына шарт орындалады :$x_{i_1} \dots x_{i_{j-1}} x_{i_k} x_{i_{j+1}} \dots x_{i_d}$

Егер екі шарт та дұрыс болса, онда:

$$\mathrm{L}(\zeta) \geq \mathrm{F}(\mathrm{L}_{\mathrm{i}_1}, \mathrm{L}_{\mathrm{i}_2}, \dots, \mathrm{L}_{\mathrm{i}_\mathrm{d}}) \qquad (4.8)$$

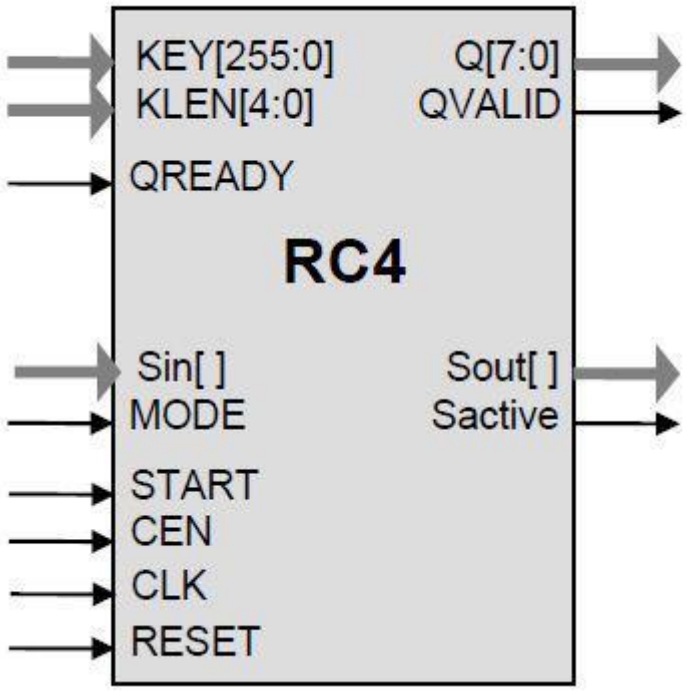
F логикалық біріктіру функциясы 4 алгебралық дәрежеге ие және $d = 4$: $x_{13}x_{14}x_{15}x_{16}$ дәрежесінен тұрады.

$x_{13}x_{14}x_{15}x_{16}$ монохромы алдыңғы 1-шартты қанағаттандырады: d = 4 бар монохромға үлес қосатын тиісті ығысу регистрлерінің ұзындығы $N_{13} = 19$, $N_{14} = 21$, $N_{15} = 22$, $N_{16} = 23$ тең болады.

3 Есептеу бөлімі

3.1 C++ көмегімен RS4 алгоритмін модельдеу

RC4 алгоритмін Ривест арнайы өзгермелі ұзындық кілті бар негізгі ақпарат ағынының генераторы ретінде жасаған. RC4 сияқты алгоритмдермен құрылған жалған кездейсоқ сандар генераторлары блок шифрларына негізделген генераторларға қарағанда әлдеқайда жылдам. RC4 алгоритмі ақпаратты қорғаудың әртүрлі жүйелерінде, компьютерлік желілерде (мысалы, SSL хаттамасында, Windows NT-де парольдерді шифрлау үшін және т.б.) кеңінен қолданылады.



2.7 Сурет– RC4 негізгі ағын генераторының IP ядросының құрылымдық тізбегі

RC4-бұл алгоритмдердің класы, оның блогының немесе сөздің өлшемімен анықталады-параметрі N,әдетте N = 8. Алгоритм талдауын жеңілдету үшін N=4 аламыз. RC4 ішкі күйі 2n сөзден тұратын массивтен және әрқайсысы бір сөзден

тұратын екі санауыштан тұрады. Екі есептегіш, екеуі де n=4 4 биттік, біз I және j деп атаймыз.

Массив s-бокс деп аталатын ауыстыру кестесі ретінде қолданылады, содан кейін S деп белгіленеді, әр уақытта S кестесінде барлық мүмкін n-биттік (біздің жағдайда 4-биттік) сандар аралас түрінде болады. Кестедегі мәндердің нақты өзгеруі кілтпен анықталады. Кестенің әр элементі 0-ден 15-ке дейінгі аралықта мәндерді қабылдайтындықтан, оны екі жолмен түсіндіруге болады: сан ретінде немесе кестедегі басқа элементтің нөмірі ретінде.

RC4 алгоритмі екі кезеңнен тұрады. Бірінші, дайындық кезеңінде s ауыстыру кестесі инициализацияланады, екінші кезеңде жалған кездейсоқ сандар есептеледі.

Алдымен ол 0-ден 15-ке дейінгі сандармен қатар толтырылады. Кілт 4 биттік сөздердің реттілігі түрінде ұсынылады, олар басқа k массивін s өлшемімен толтырады, егер кілт қажет болғаннан қысқа болса, ол бірнеше рет қайталанады. Содан кейін келесі әрекеттер орындалады (алгоритм 1):

1. j = 0; i =0;
2. j = (j + Si + Ki) mod 16;
3. Si и Sj ауыстыру;
4. i = i +1;
5. егер i <16

Осы алгоритмді орындау нәтижесінде s ауыстыру кестесін бастапқы толтыру жүзеге асырылады және бұл бастапқы араластыру құпия кілтке байланысты жүзеге асырылады.

S кестесі дайын болғаннан кейін кездейсоқ N биттік сөздерді құруды бастауға болады. Ол үшін I және j есептегіштеріне 0 бастапқы мәні беріледі. Әрбір жаңа zi мәнін алу үшін келесі әрекеттер орындалады (алгоритм 2):

i = (i + 1) mod 16;
j = (j + Si) mod 16;
Si и Sj ауыстыру;
a = (Si + Sj) mod 16;
zi = Sa.

Алынған 4 биттік zi мәні келесі 4 биттік кіріс ағынының блогын шифрлау кілті ретінде пайдаланылуы мүмкін.

Мысалы, құпия кілт алты 4 биттік мәннен тұрсын (оларды ондық түрінде келтіреміз): 1, 2, 3, 4, 5, 6. RC4 алгоритмі бойынша сандар тізбегін құруға тырысайық.

S кестесін 0-ден 15-ке дейінгі сандармен қатар толтырамыз. Есептеулерді орындау кезінде барлық қосу операциялары 16 модульде орындалатынын есте ұстаған жөн.

2.3 Кесте – S дайындық кезеңінде инициализациялау кестесі

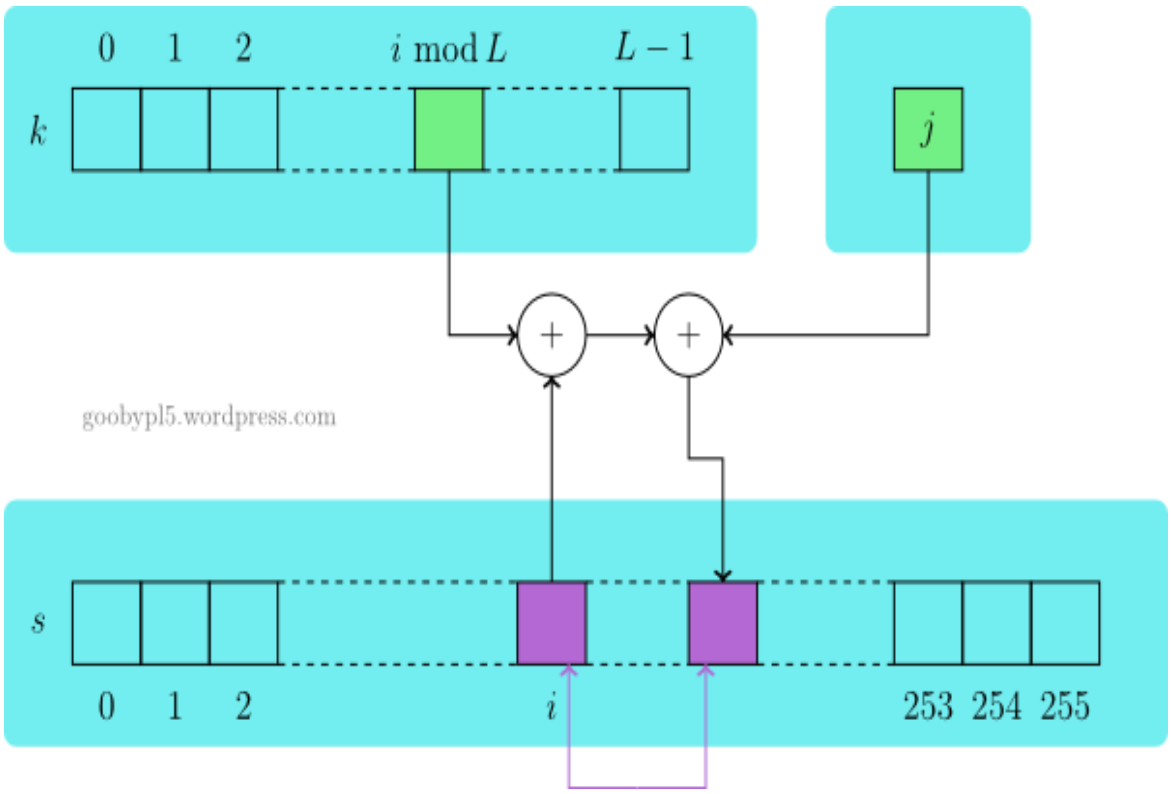
№. алгоритм	Орындалатын әрекет (mod 16 бойынша)	Жаңа мән i	Жаңа мән j

1	j=0, i=0	0	
2	$j=j+S_i+K_i=0+0+1=1$		1
3	Si және Sj, яғни S0 және S1 ауыстыру		
4	I=i+1	1	
5	I<16		
2	J= j+Si+Ki=1+0+2=3		3
3	Si және Sj, яғни S1 және S3 ауыстыру		
4	I=i+1	2	
5	I<16		

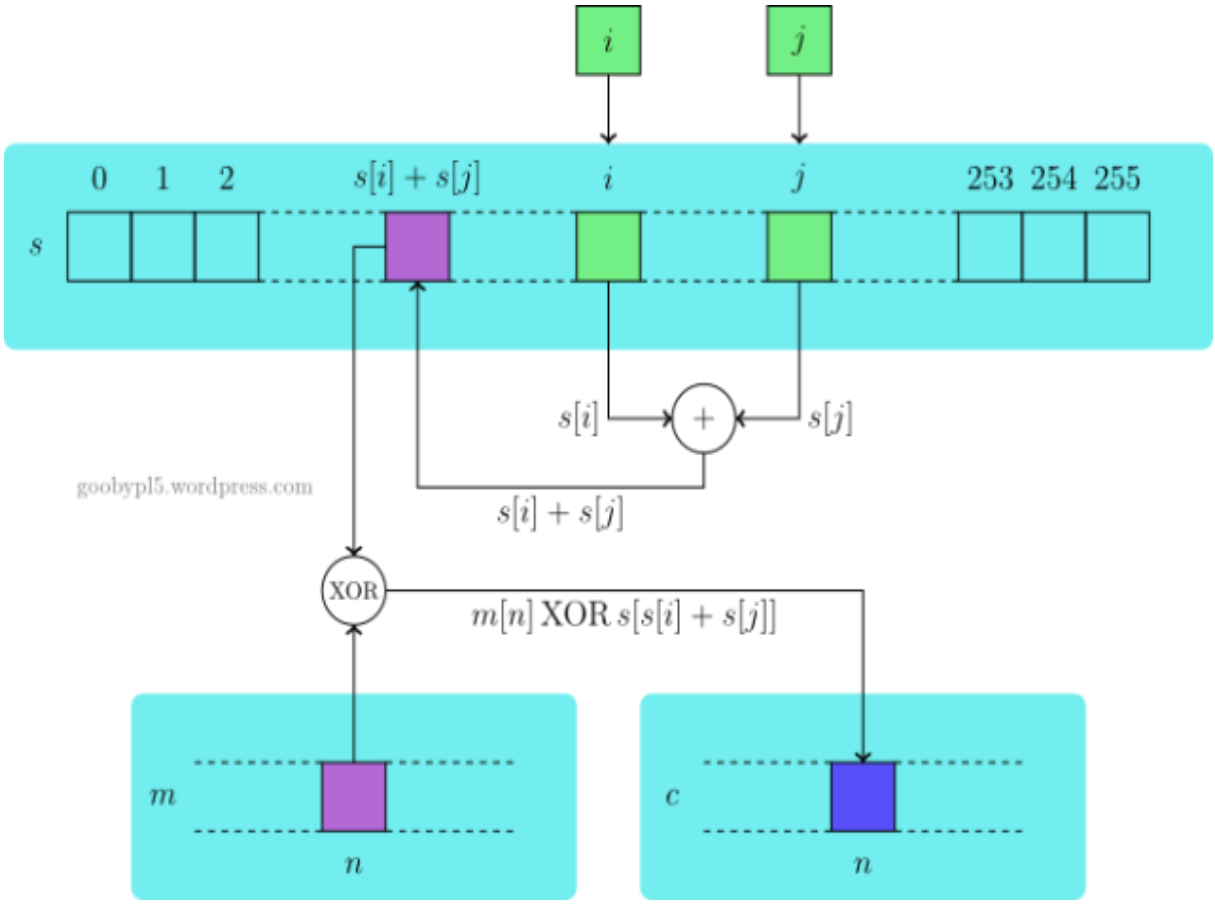
RC4 енді бүгінгі стандарттар бойынша қауіпсіз деп саналмайды. Алғашқы күдіктер 1997 жылы айтылды, 2000 жылға дейін бірнеше теориялық кемшіліктер табылды. 2001/2002 жылдары Флюрер, Мантин және Шамир алғашқы практикалық шабуылдарды ұсынды.

Қазіргі уақытта RC4 классикалық шифр ретінде қарастырылуы керек.. Алайда, қатал шындық, RC4 сымсыз шифрлау (WEP және WPA) және онлайн-банкинг сияқты көптеген кәсіби салаларда қолданылады.

Енді хабарламаны шифрлау үшін басында екі i j айнымалысын жариялап, оларды нөлдермен инициализациялау керек. Шифрлау үшін n-ші символы I-ге (256 модулі бойынша) және s[i+1](сонымен қатар 256 модулі бойынша) артады. Алгоритм сызбасын сызамыз.

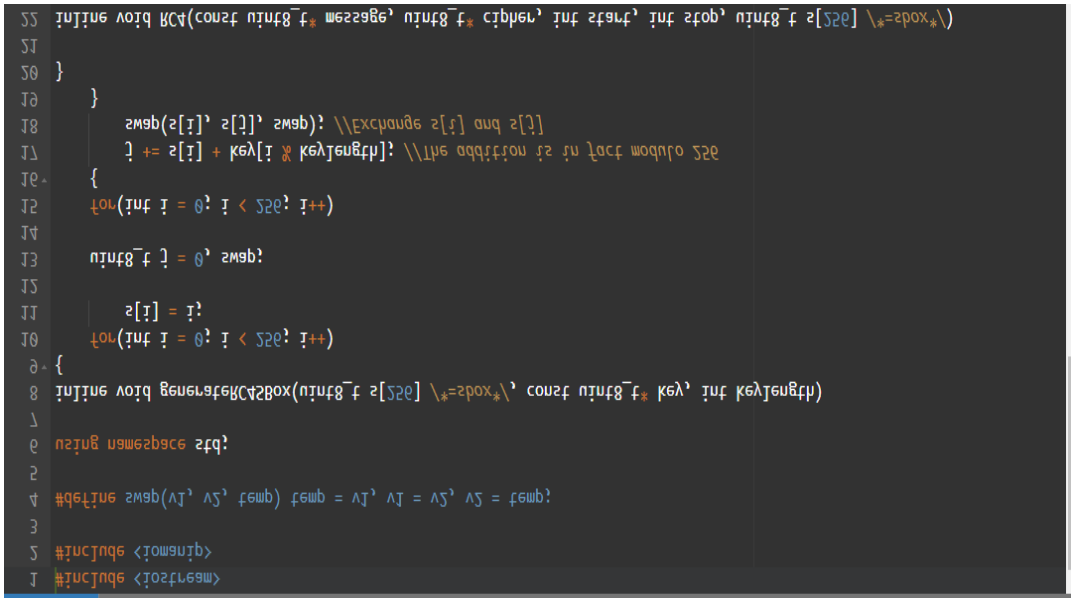


2.8 Сурет– RC4 алгоритм сызбасы

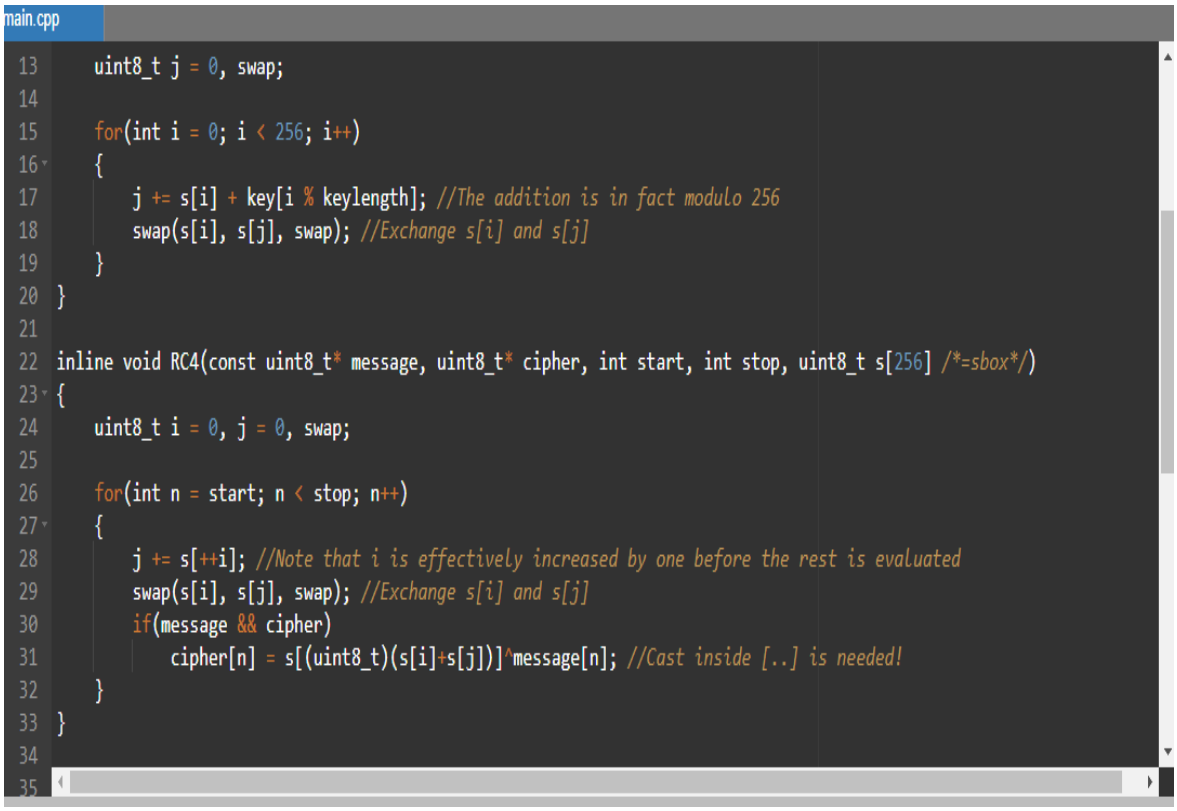


2.9 Сурет– RC4 256 модулі бойынша алгоритм сызбасы

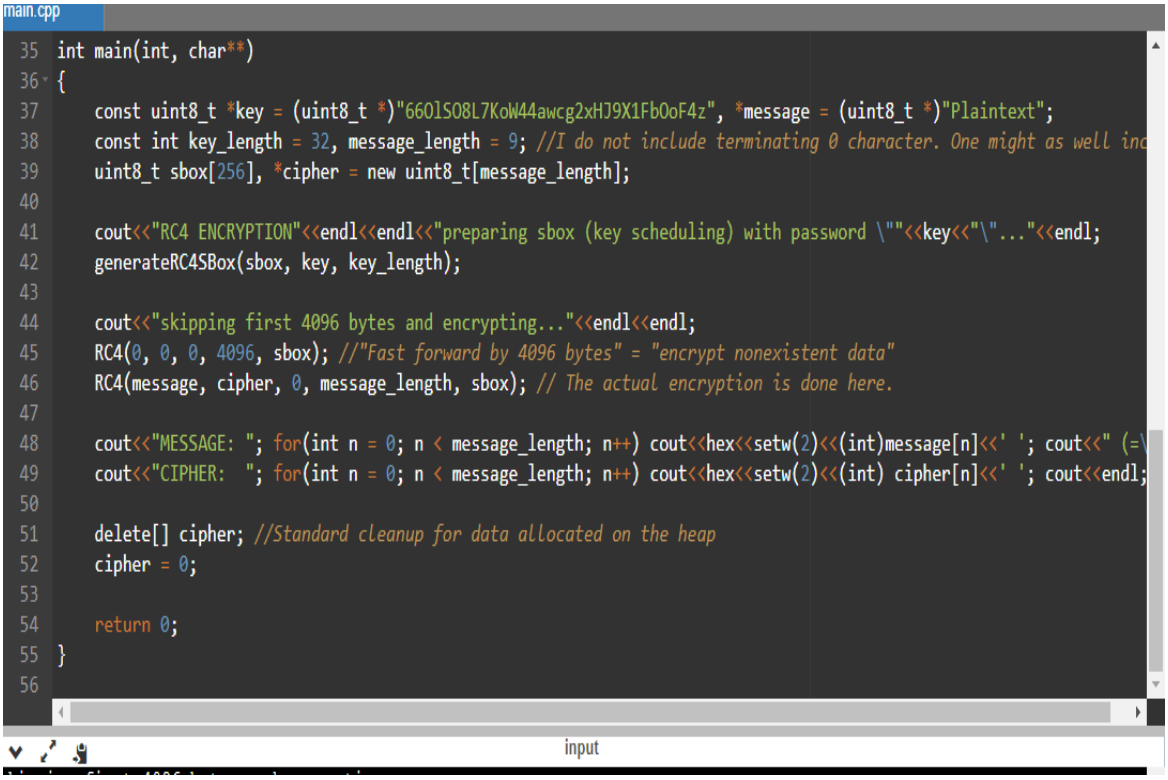
RC4 бағдарламалау салыстырмалы түрде оңай болғандықтан, мен C++ тілінде іске асырамын (код).



3 Сурет– C++ тіліндегі алгоритм құру



3.1 Сурет– C++ тіліндегі алгоритм құру



3.2 Сурет– C++ тіліндегі алгоритм құру

3.3 Сурет– RC4 алгоритмінің соңғы нәтижесі

Сондай-ақ, 45-жолда мен алғашқы 4096 жалған кездейсоқ байттарды консервативті түрде өткізіп жіберемін, бұл RC4-тің кейбір кемшіліктерін

"түзетудің" бір түрі. Кейбір адамдар оны "RC4-drop-4096" немесе сол сияқты деп атайды. Кілт үшін Мен мысал ретінде жиі айтылатын "66olso8l7kow44awcg2xhj9x1fboof4z" қолдандым.

ҚОРЫТЫНДЫ

Қазіргі уақытта ұялы байланыс жүйесі рұқсат етілмеген пайдаланушылардың шабуылдарына осал болып келеді. Бүкіл әлемде көптеген мамандар шабуылдарға қарсы жұмыс істейді, олар әр түрлі жұмыс стандарттары мен жабдықтарды қолданылды. Есептеу қуаты әр екі-үш жыл сайын екі есе артады деген болжам бар. Бүгінгі күнде қауіпсіз алгоритм ойлап тапқаннан күннің өзінде алгоритм 5-6 жылдан кейін қауіпсіз бола алады. Себебі кез-келген алгоритм жасалғаннан кейін, дамудан өтіп, көптеген жылдар бойы жұмыс істелді.

Дипломдық жұмыста жалпы алгоритмдер мен олардың түрлерін қарастырып, жұмыс принциптерін талданды. Құпия белгісіз шифрлаудың әрбір құрылған мәнді шифрлау режимінде қайтымды жалған кездейсоқ функция (PRF) ретінде анықталынды. Оны шифрлау режимінде тексеріп, есептелінді. Жоғарыда айтқанымдай, RC4 шифрлау туралы ең керемет нәрсе - оны жүзеге асырудың қарапайымдылығы. Негізгі логика-27 жол немесе одан да қысқа екенін білдік.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 V. K. Garg, “Wireless and Personal Communication System”, 12, 2015.

3 Бабаш, А.В. Криптографические методы защиты информ.: Учебное пособие: Т.1 / А.В. Бабаш. - М.: Риор, 2018. - 48 с.р.

4 Васильева, И.Н. Криптографические методы защиты информации: Учебник и практикум для академического бакалавриата / И.Н. Васильева. - Люберцы: Юрайт, 2016. - 349 с.

5 Рябко, Б.Я. Криптографические методы защиты информации: Учебное пособие для вузов / Б.Я. Рябко, А.Н. Фионов. - М.: Горячая линия -Телеком, 2014. - 229 с.

6 Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2015. - 376 сГук М. Аппаратные средства локальных сетей/М. Гук - СПб: Издательство

7 Courtois, N.T. Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. In Proceedings of the CRYPTO 2003: Advances in Cryptology, Santa Barbara, CA, USA, 17–21 August 2003; Volume 2729, pp. 176–194. [Google Scholar]

8 Gammel, B.; Göttfert, R.; Kniffler, O. Achterbahn-128/80: Design and analysis. In Proceedings of the ECRYPT Workshop SASC 2007—The State of the Art of Stream Ciphers, Bochum, Germany, 31 January–1 February 2007.

9 Gierlichs, B.; Batina, L.; Clavier, C.; Eisenbarth, T.; Gouget, A.; Handschuh, H.; Kasper, T.; Lemke-Rust, K.; Mangard, S In Proceedings of the ECRYPT Workshop SASC 2008–The State of the Art of Stream Ciphers, Lausanne, Switzerland, 13 February 2008.

10 Lano, J.; Mentens, N.; Preneel, B.; Verbauwhede, I. Power analysis of synchronous stream ciphers with resynchronization mechanism. In Proceedings of the ECRYPT Workshop SASC 2004–The State of the Art of Stream Ciphers, Brugge, Belgium, 14–15 October 2004;

11 Hell, M.; Johansson, T.; Meier, W. Grain-A Stream Cipher for Constrained Environments. Int. J. Wirel. Mob. Comput. 2007, 2, 86–93.

12 Babbage, S. The stream cipher MICKEY 2.0. In New Stream Cipher Designs; Springer: Berlin, Germany, 2006.

13 De Cannìere, C.; Preneel, B. TRIVIUM Specifications. eSTREAM: the ECRYPT Stream Cipher Project. 2006.April 2019).

14 Good, T.; Benaissa, M. Hardware performance of eStream phase-III stream 2008; pp. 163–173.

15 Ваэль, А.; Айюб, М. Физическая и мехатронная безопасность, технологии и будущие тенденции для автомобильной среды. В материалах VDI-Fachtagung Automotive Security, VDI Berichte, Нюртинген, Германия, 27 сентября 2017 г.; Том 2310, стр. 73-95.

16 Маес Р.; Вербаувхеде И. Физически Неклонируемые функции: исследование современного состояния и будущих направлений исследований.

На пути к аппаратной внутренней безопасности; Springer: Берлин, Германия, 2010; стр. 3-37

17 Садеги, А.-Р.; Висконти, И.; Вахсманн, С. Повышение безопасности и конфиденциальности RFID за счет физически не закрываемых функций. В направлении аппаратной внутренней безопасности; Springer: Берлин/Гейдельберг, Германия, 2010.

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Озат Мөлдір

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Ағындық шифрлар негізінде ұялы байланыстағы ақпаратты криптографиялық қорғауды талдау

Научный руководитель: Ерлан Таштай

Коэффициент Подобия 1: 8

Коэффициент Подобия 2: 1.7

Микропробелы: 7

Знаки из здругих алфавитов: 9

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☑ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

30-01-2022
Дата

Заведующий кафедрой

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Озат Мөлдір

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Ағындық шифрлар негізінде ұялы байланыстағы ақпаратты криптографиялық қорғауды талдау

Научный руководитель: Ерлан Таштай

Коэффициент Подобия 1: 8

Коэффициент Подобия 2: 1.7

Микропробелы: 7

Знаки из здругих алфавитов: 9

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☑ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

30.05.2021
Дата

проверяющий эксперт