O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

TERMIZ DAVLAT UNIVERSITETI

MAGISTRATURA BO’LIMI

Qo’lyozma huquqi asosida

UDK_____

ABDIMALIKOV DILMUROD AXAD O’G’LI

MILLIY KRIPTOGRAFIK ALGORITMLARNI QO’LLASH UCHUN KRIPTOGRAFIK KUTUBX ONA ISHLAB CHIQARISH

Mutaxassislik: 70610201 – Kompyuter tizimlari va ularning dasturiy ta’minoti (tarmoqlar va sohalar bo’yicha)

Magistr akademik darajasini olish uchun yozilgan

DISSERTATSIYA

Ilmiy rahbar: _____ t.f.f.d., (PhD)dots. O.M.Allanov

TERMIZ – 2024

Magistrlik dissertatsiyasi mavzusi Termiz davlat universiteti rektorining 2024-yil 19-yanvardagi №5-T/M sonli buyrug'i asosida tasdiqlangan.

Magistrlik dissertatsiyasi Termiz davlat universiteti kafedrasida bajarilgan

Magistrlik dissertatsiyasi elektron nusxasi Termiz davlat universitetining rasmiy web sahifasiga joylashtirilgan.

Dissertatsiya manzilining QR-kodi:

Magistrlik dissertatsiyasi bilan Termiz davlat universitetining axborot-resurs markazida tanishish mumkin (_____ raqam bilan ro'yxatga olingan. Manzil: Termiz shahri, Barkamol avlod ko'chasi 43-uy.)

Ilmiy rahbar: _____t.f.f.d.,(PhD)dots. O.M.Allanov

Kafedra mudiri: _____ i.f.d., prof. O.Q.Xatamov

Magistratura bo'limi boshlig'i: _____ __k.f.f.d.(PhD) D.X. Abduraximov

MUNDARIJA

“Milliy kriptografik algoritmlarni qo‘llash uchun kriptografik kutibxona ishlab chiqish” mavzusidagi magistrlik dissertatsiyasi

ANNOTATSIYASI

Tayanch so’zlar: Kitiptografiya, algoritimlar, kutubxon, konfidensiallik, dasturiy ta’minot, autentifikatsiya, simmetrik, ochiq kalitlin shifrlash, dasturlash, elektron raqamli imzo.

Tadqiqot ob’yekti: Tadqiqot ob’ekti sifatida kriptografik dasturiy vositalarni yaratish jarayoni xizmat qiladi.

Ishning maqsadi: Milliy kriptografik algoritmlarni amalga oshirish imkoniyatini beruvchi kutubxonani ishlab chiqishdan iborat.

Tadqiqot metodlari: Ushbu tadqiqot ishida sonlar nazariyasi, ehtimollar nazariyasi, modellash, qiyosiy tahlil va ob’ektga yo‘naltirilgan dasturlashdan foydalanildi.

Olingan natijalar va ularning yangiligi:

. Ishlab chiqilgan milliy standartlarga asoslangan kriptografik kutubxona arxitekturasi va uni amalga oshirish uchun zarur bo‘lgan tavsiyalar tadqiqot ishining yanligi hisoblanadi.

Tadqiqot natijalarining nazariy va amaliy ahamiyati: Kriptografik kutubxonalarni tahlillashdan olingan natijalar, milliy standartlarni dasturiy amalga oshirishda zarur bo‘lgan bilimlar va milliy standartlar asosida kriptografik kutubxonani ishlab chiqishga tegishli ma’lumotlardan o‘quv jarayonida foydalanish magistrlik dissertatsiyasining nazariy ahamiyati sanaladi.

Magistrlik dissertatsiyasining amaliy ahamiyati milliy standartlar asosida ishlab chiqilgan kutubxonadan turli kriptografik dasturiy vositalarni ishlab chiqishda foydalanish bilan belgilanadi.

Qo’llash sohasi: Elektron hujjat almashinuv tizimlarini tatbiq etishda va elektron huqumat tizimini shakllantirishda ma’lumotlar xavfsizligini ta’minlashga qaratilgan keng qamrovli chora-tadbirlar amalga oshirishda qollaniladi.

Магистерская диссертация на тему" Разработка криптографической библиотеки для применения национальных криптографических алгоритмов"

АННОТАЦИЯ

Ключевые слова: криптография, алгоритмы, библиотека, конфиденциальность, программное обеспечение, аутентификация, симметричный, шифрование с открытым ключом, Программирование, цифровая подпись.

Объект исследования: объектом исследования служит процесс создания криптографических программных средств.

Цель работы: разработка библиотеки, позволяющей реализовать национальные криптографические алгоритмы.

Методы исследования: в этой исследовательской работе использовались теория чисел, теория вероятностей, моделирование, сравнительный анализ и объектно-ориентированное программирование.

Полученные результаты и их новизна: Архитектура криптографической библиотеки, основанная на разработанных национальных стандартах и рекомендациях, необходимых для ее реализации, является янтарем исследовательской работы.

Теоретическая и практическая значимость результатов исследования: результаты анализа криптографических библиотек, знания, необходимые для программной реализации национальных стандартов, и использование в учебном процессе информации, относящейся к разработке криптографической библиотеки на основе национальных стандартов, являются теоретической значимостью магистерской диссертации.

Практическая значимость магистерской диссертации определяется использованием библиотеки, разработанной на основе национальных стандартов, при разработке различных криптографических программных средств.

Область применения: применяется при внедрении систем электронного документооборота и при реализации комплексных мер, направленных на обеспечение безопасности информации при формировании системы электронного права.

Master's thesis on the topic ”Development of a cryptographic library for the application of national cryptographic algorithms”

ANNOTATION

Keywords: cryptography, algorithms, library, privacy, software, authentication, symmetric, public key encryption, Programming, digital signature.

The object of research: the object of research is the process of creating cryptographic software tools.

The purpose of the work: to develop a library that allows you to implement national cryptographic algorithms.

Research methods: Number theory, probability theory, modeling, comparative analysis and object-oriented programming were used in this research work.

The results obtained and their novelty: The architecture of the cryptographic library, based on the developed national standards and recommendations necessary for its implementation, is the amber of research work.

Theoretical and practical significance of the research results: the results of the analysis of cryptographic libraries, the knowledge necessary for the programmatic implementation of national standards, and the use of information related to the development of a cryptographic library based on national standards in the educational process are the theoretical significance of the master's thesis.

The practical significance of the master's thesis is determined by the use of a library developed on the basis of national standards in the development of various cryptographic software tools.

Scope of application: it is used in the implementation of electronic document management systems and in the implementation of comprehensive measures aimed at ensuring the security of information in the formation of an electronic law system.

Kirish

Dissertatsiya mavzusining asoslanishi va uning dolzarbligi. Axborotning kriptografik himoyasi usullari uning butunligini, maxfiyligini, autentifikatsiyasini va rad-etishga qarshi ta’minlaydi hamda apparat, apparat-dasturiy va dasturiy ko‘rinishda amalga oshiriladi. Ular orasida dasturiy kriptogarfik himoya vositalari o‘zining ko‘p vazifaligi, arzonligi va yangilash imkoniyatining mavudligi bilan ajralib turadi. Dasturiy ko‘rinishdagi kriptografik vositaning asosini kriptografik algoritmlardan iborat bo‘lgan kutubxona tashkil etib, undagi algoritmlar sonining ko‘pligi va samarali amalga oshirilishi uning bardoshligini ta’minlaydi.

Respublikamizda davlat va xo‘jalik boshqaruv organlarida elektron hujjat almashinuv tizimlarini tatbiq etishda va elektron huqumat tizimini shakllantirishda ma’lumotlar xavfsizligini ta’minlashga qaratilgan keng qamrovli chora-tadbirlar amalga oshirilmoqda. 2017-2021 yillarda O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasida, jumladan «..axborot xavfsizligini ta’minlash va axborotni himoyalash tizimini takomillashtirish, axborot sohasidagi tahdidlarga qarshi o‘z vaqtida va munosib qarshilik ko‘rsatish» vazifalari belgilangan [1]. Bundan tashqari 2018 yil 14 martdagi PF-5379-son «O‘zbekiston Respublikasining davlat xavfsizligi tizimini takomillashtirish chora-tadbirlari to‘g‘risida»gi [2] va 2018 yil 19 fevraldagi PF-5349-son «Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to‘g‘risida»gi [3] Farmonlari, 2007 yil 3 apreldagi PQ-614-son «O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to‘g‘risida»gi Qarorini misol keltirish mumkin.

Mazkur farmon va qarorlar asosida axborotning kriptografik himoyasini tashkil etish bo‘yicha, xususan, turli milliy standartlar ishlab chiqildi va amalda tadbiq etildi. Bunga misol qilib O‘z DSt 1092:2009 “Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va

tekshirish jarayonlari” [5], O‘z DSt 2826:2014 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elliptik egri chiziqlarga asoslangan elektron raqamli imzoni shakllantirish va tekshirish jarayonlari [9], O‘z DSt 1105:2009 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi [12], O‘z DSt 1106:2009 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi [6], O‘z DSt 1109:2013 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta’riflar [16] va O‘z DSt 1204:2009 Axborot texnolgiyasi. Axborotning kriptografik muhofazasi. Kriptografik modullarga xavfsizlik talablari [8] larni keltirish mumkin.

Hozirda kriptografik dasturiy vositalarni yaratish uchun turli kriptografik kutubxonalar mavjud bo‘lib, ular asosan AQSh, Rossiya Federatsiyasi standartlari va turli xalqaro algoritmlarni qamrab olgan. Milliy kriptogarfik standartlarni o‘z ichiga olgan kutubxonalarni mavjud emasligi va ularga asoslangan milliy dasturiy mahsulotlarni ishlab chiqarishni muhimligini hisobga olgan holda mazkur magistrlik dissertatsiya ishi mavzusini dolzarb deb aytish mumkin.

Ilmiy tadqiqot ishining ob’ekti va predmetining belgilanishi. Tadqiqot ob’ekti sifatida kriptografik dasturiy vositalarni yaratish jarayoni xizmat qiladi.

Tadqiqot predmetini esa milliy standartlar asosida kriptografik kutubxonani yaratish usullari tashkil etadi.

Ilmiy tadqiqot ishining maqsadi va vazifalari. Mazkur magistrlik dissertatsiyasi ishining maqsadi – milliy kriptografik algoritmlarni amalga oshirish imkoniyatini beruvchi kutubxonani ishlab chiqishdan iborat.

Tadqiqot maqsadini amalga oshirish uchun quyidagi vazifalar belgilab olindi:

- kriptografik dasturiy himoya vositalarini va ularni yaratish usullarini tahlil qilish;
- mavjud kriptografik kutubxonalarni algoritm tarkibi, foydalanilgan dasturlash tili va imkoniyati nuqtai nazaridan tahlil qilish;

- milliy kriptografik standartlarni dasturiy amalga oshirish maqsadida tahlil qilish;
- milliy algoritmlarga asoslangan kriptografik kutubxonaning arxitekturasi ishlab chiqish;
- milliy algoritmlarning kriptografik kutubxonasini ishlab chiqish.

Ilmiy tadqiqotning asosiy masalalari va farazlari. Milliy kriptografik algoritmlarga asoslangan dasturiy vositalardan axborot xavfsizligini ta’minlash.

Mavzu bo‘yicha qisqacha adabiyotlar analizi. Mazkur ilmiy tadqiqot ishi doirasida ko‘plab ilmiy ishlar, standartlar va o‘quv qo‘llanmalari mavjud. Ularga O‘z DSt 1204:2009 standarti [8], O‘z DSt 1092:2009 standarti [5], O‘z DSt 2826:2014 standarti [9], O‘z DSt 1106:2009 standart [6]larini, D.Ye.Akbarovning “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi” [17], Varlataya va boshqalarning “Аппаратно-программные средства и методы защиты информатсии” [18], Jdanov va boshqalarning “Методы и средства криптографической защиты информатсии”[19] va B. Shneyerning “Applied Cryptography Second Edition Protocols, Algorthms, and Source Code in C” [20] larni kiritish mumkin.

Bundan tashqari turli ilmiy jurnallarda nashr etilgan ilmiy maqola va Internet ma’lumotlaridan foydalanildi.

Ilmiy tadqiqot ishida qo‘llanilgan uslublarning qisqacha tavsifi. Ushbu tadqiqot ishida sonlar nazariyasi, ehtimollar nazariyasi, modellash, qiyosiy tahlil va ob’ektga yo‘naltirilgan dasturlashdan foydalanildi.

Tadqiqot natijalarining nazariy va amaliy ahamiyati. Kriptografik kutubxonalarni tahlillashdan olingan natijalar, milliy standartlarni dasturiy amalga oshirishda zarur bo‘lgan bilimlar va milliy standartlar asosida kriptografik kutubxonani ishlab chiqishga tegishli ma’lumotlardan o‘quv jarayonida foydalanish magistrlik dissertatsiyasining nazariy ahamiyati sanaladi.

Magistrlik dissertatsiyasining amaliy ahamiyati milliy standartlar asosida ishlab chiqilgan kutubxonadan turli kriptografik dasturiy vositalarni ishlab chiqishda foydalanish bilan belgilanadi.

Ilmiy tadqiqot ishining ilmiy yangiligi. Ishlab chiqilgan milliy standartlarga asoslangan kriptografik kutubxona arxitekturasi va uni amalga oshirish uchun zarur bo‘lgan tavsiyalar tadqiqot ishining yanligi hisoblanadi.

Dissertatsiya tarkibining qisqacha tavsifi. Mazkur tadqiqot ishi kirish, 3 ta bob, xulosa, foydalanilgan adabiyotlar ro‘yxatidan iborat. Ushbu tadqiqot ishida 6 ta jadval, 26 ta rasmdan iborat. Ilmiy tadqiqot ishining umumiy hajmi 76 sahifani tashkil etadi.

I bob. Axborotni himoyalashning kriptografik usullari va vositalar

1.1. Axborotni himoyalashning kriptografik usullari

Kriptografiya murakkab matematik amallarni qo‘llash orqali kuchli shifrlashni loyihalashni maqsad qilgan fan sohasi bo‘lib, bu o‘rinda kuchli shifrlashning ma’nosi uchinchi tomon uchun noma’lum bo‘lgan sir bilan ma’lumot yashirish bilan xarakterlanadi. Shuning uchun, kriptografiya fani qabul qiluvchiga ma’lumotni xavfsiz yetib borishini ta’minlovchi yozish san’ati deb ham yuritiladi.

Kriptografiya axborot xavfsizligini ta’minlashda *konfidensiallik, ma’lumot butunligi*, *autentifikatsiya* va *rad etishdan himoyalash* xizmatlarini amalga oshiradi [21].

Konfidensiallik – axborotni ruxsat etilmagan foydalanuvchilar tomonidan “o‘qish”dan himoyalaydi.

Ma’lumot butunligi – ma’lumot o‘zgarishini aniqlash bilan shug‘ullanuvchi xavfsizlik xizmati bo‘lib, ma’lumot ruxsat etilmagan foydalanuvchilar tomonidan bilmasdan yoki qasddan o‘zgartirilishi mumkin bo‘lgan hollarda qo‘llaniladi.

Autentifikatsiya – qabul qiluvchi tomonida yuboruvchi shaxsini aniqlash orqali ma’lumotni kafolatlashga qaratilgan xavfsizlik xizmati bo‘lib, ma’lumot yuboruvchisi o‘zini tasdiqlashda foydalanadi.

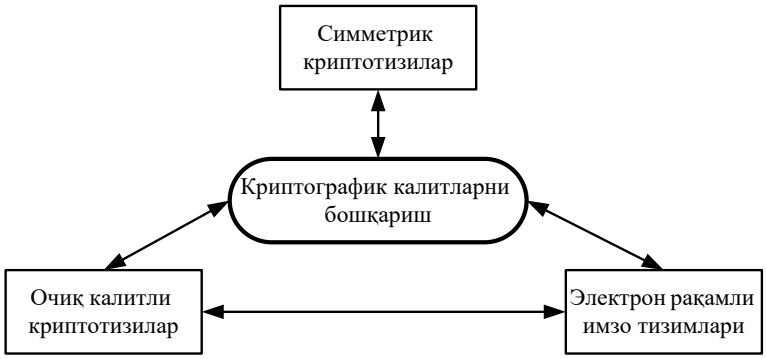
Rad etishdan himoyalash – tomonlarni biror bir harakatni amalga oshirgani uchun egalik yoki javobgarlikni rad etaolmasligini ta’minlovchi xavfsizlik xizmati sanaladi. Masalan, navbat elektron ravishda olingan bo‘lsa va bunda rad etishdan himoyalash xizmati mavjud bo‘lsa, u holda foydalanuvchi navbatni olmadim deb ayta olmaydi.

Hozirgi zamon kriptografiyasi quyidagi bo‘limlarga bo‘linib, ular yuqorida keltirilgan xizmatlarni birini yoki bir nechtasini bajaradi yoki ularga ko‘makchi vazifasini o‘taydi:

- simmetrik shifrlash usullari – *konfidensiallikni* ta’minlashga xizmat qiladi;

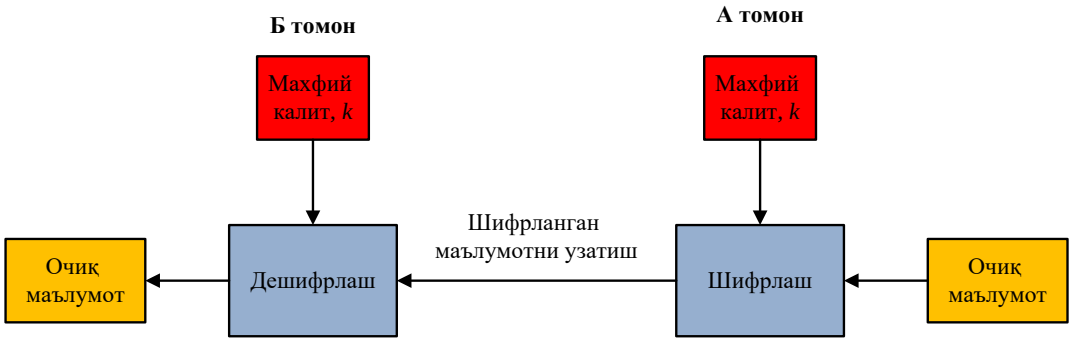
– ochiq kalitli shifrlash usullari – *konfidensiallikni* ta’minlashga xizmat qiladi;
– elektron raqamli imzo algoritmlari – *autentifikatsiya* va *rad etishdan himoyalash*ni amalga oshiradi;
– kriptografik kalitlarni boshqarish – yuqoridagi bo‘limlar o‘z vazifasini bajarishda ko‘makchi vazifasini bajaradi.

Zamonaviy kriptografiya bo‘limlari orasidagi funksional bog‘liq mavjud bo‘lib, bir bo‘lim qolgari xizmatiga asoslanadi yoki uning asosida quriladi. Umumiy holda ushbu bog‘liqni quyidagi 1.1-rasmda ko‘rish mumkin [21].



1.1.1– rasm. Zamonaviy kriptografiya bo‘limlari orasidagi funksional bog‘liqlik

Simmetrik shifrlash usullari qadimdan foydalanib kelingan kriptografik usul sanalib, ma’lumotni shifrlash va deshifrlashda aynan bir maxfiy kattalikdan foydalanadi (1.2-rasm).



1.1.2– rasm. Simmetrik shifrlash usuli

Simmetrik shifrlash usullari foydalanilgan zamonga bog‘liq holda *klassik* va *zamonaviy* simmetrik shifrlash usullariga ajratiladi [22]. Klassik shifrlash usullari o‘zining soddaligi bilan ajralib tursada, o‘sha vaqt nafasi bilan

xarakterlanadi. Zamonaviy simmetrik shifrlash usullari esa yuqori hisob kitobni talab etishi sababli hisoblash qurilmalarida amalga oshiriladi.

Simmetrik zamonaviy shifrlash usullari foydalanilayotgan muhitga ko‘ra *blokli* va *oqimli* shifrlarga ajaratiladi. Simmetrik blokli shifrlash usullari hozirda keng qo‘llanilayotgan kriptografik usul sanalib, o‘zining tezkorligi va bardoshligi bilan ajralib turadi. Oqimli shifrlash usullari real vaqt tizimlarida foydalanishga mo‘ljallangan bo‘lib, kichik hisoblash muhitida ham amalga oshirish imkonini beradi.

Simmetrik shifrlash usullari quyidagi akslantirishlarga asoslanadi [22]:

- simmetrik o‘rin almashtirish;
- simmetrik o‘rniga qo‘yish.

O‘rniga qo‘yish akslantirishi hozirgi kunda simmetrik blokli shifrlarning bardoshligini ta’minlovchi chiziqsiz akslantirishi hisoblanadi (S-jadval). O‘rin almashtirish akslantirishlari ham blokli va oqimli shifrlarning asosi sanaladi (IP yoki P-jadval).

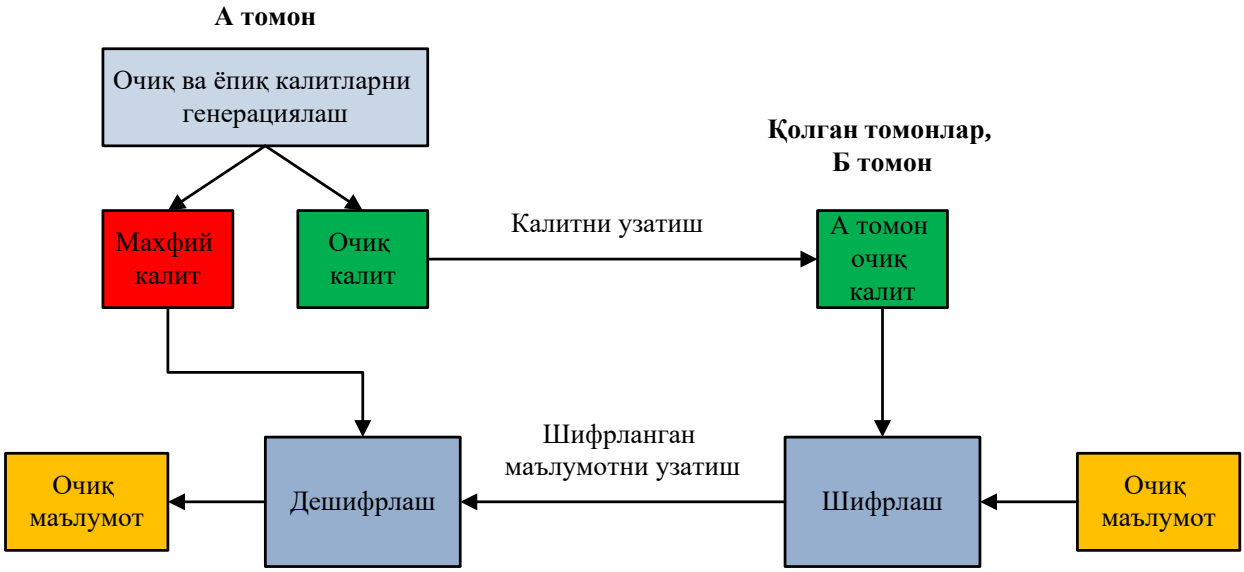
Simmetrik blokli shifrlash algoritmlari sohasida har bir rivojlangan va rivojlanayotgan davlatlar o‘z standartlariga ega. Masalan, AQSh davlatida AES (Advanced Encryption Standard) [23], Rossiya davlatida GOST R 34.12-2015 [24] va Respublikamizda O‘z DSt 1105:2009 [12].

Simmetrik blokli shifrlardan farqli ravishda oqimli shifrlash usullari asosan xalqaro standartlar sifatida ishlab chiqilgan bo‘lib, ularga keng qo‘llanilayotgan RC4, ISAAC+, A5/1, ChaCha20 algoritmlarini keltirish mumkin.

Simmetrik blokli shifrlash usullari odatda turli shifrlash *rejimlari*da (modes) foydalaniladi. Har bir shifrlash rejimi o‘ziga xos bo‘lgan xususiyatga ega. Masalan, ECB (Electronic Code Book) rejimi shifrlash va deshifrlash jarayonlari uchun hisoblashni parallel amalga oshirish imkoniyatini bersada, bir xil ochiq matn blokini bir xil shifrmatn blokiga aylantirib berishi natijasida xavfsizlik muammosi mavjud. Bundan tashqari hozirda CBC (Cipher Block Chaining), CFB (Cipher Feed Back), OFB (Output feed Back) va CTR (Counter) kabi shifrlash rejimlaridan amalga keng qo‘llanilib kelinmoqda [22].

Simmetrik kriptografik tizimlar ma’lumotni shifrlash va deshifrlashda bardoshli va tezkor sanalsada, ularda maxfiy kalitlarni almashinish muammosi mavjud. Shu sababli odatda simmetrik shifrlash kalitlarini almashinish uchun ochiq kalitli shifrlash usullaridan foydalaniladi.

Ochiq kalitlin shifrlash usuli simmetrik usullardan farqli ravishda ma’lumotni shifrlashda va deshifrlashda turli kalitlardan foydalanadi. Masalan, ma’lumotni shifrlashda qabul qiluvchining ochiq kalitidan foydalaniladi. Deshifrlash uchun esa qabul qiluvchi o‘zining maxfiy kalitidan foydalanadi. Ushbu shifrlash usulining umumiy ko‘rinishi quyidagi 1.3-rasmda aks ettirilgan.



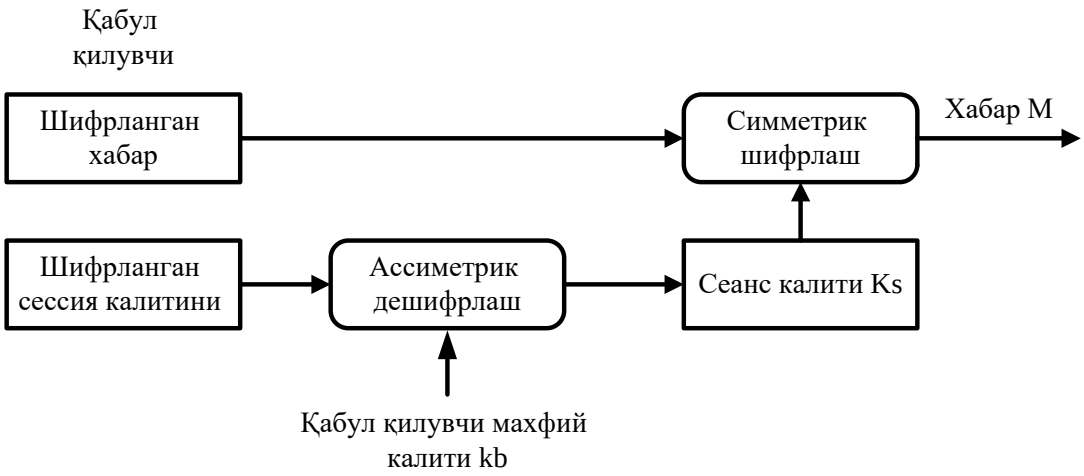
1.1.3-rasm. Ochiq kalitli shifrlash usuli

Simmetrik kriptotizimlardan farqli ravishda har bir foydalanuvchiga ikkita kalit mavjud bo‘lib, ulardan biri maxfiy va ikkinchisi ochiq kalit deb ataladi. Maxfiy kalit faqat kalit egasiga ma’lum bo‘lib, ma’lumotni deshifrlash uchun qo‘llaniladi. Ochiq kalit barchaga ochiq bo‘lib, ma’lumotni shifrlash uchun qo‘llaniladi. Ochiq kalit odatda maxfiy kalitdan bir tomonlama hisoblash usuli asosida hisoblab topiladi.

Ochiq kalitli kriptogarfik tizimlarning bardoshligi foydalanilgan bir tomonlama funksiyaga asoslangan bo‘lib, quyida ularning ayrimlari keltirilgan [21]:

- *faktorlash muammosi*: $n = p \times q$ tenglikdan n berilgan taqdirda uni teng bo‘lgan ikki tub ko‘paytuvchilar p va q larga ajratish qiyinchiligi bilan xarakterlanadi;
- *diskret logarifmlash muammosi*: $y = g^x mod p$ tenglikdan y, g, p lar berilgan taqdirda x ni topish muammosi bilan xarakteralanadi;
- *chekli maydonda elliptik egri chiziqlar muammosi*: $Q = n * P$ tenglikdan Q, P berilgan taqdirda n ni topish qiyinchiligi bilan xarakterlanadi;
- *chekli maydonda daraja parametri muammosi*: $y = g^{\backslash x} mod p$ tenglikdan y, g, p lar berilgan taqdirda parametr R va x ni topish qiyinchiligi bilan xarakterlanadi.

Ochiq kalitli kriptografik tizimlar amalda simmetrik kriptografik algoritmlar kalitini shifrlash va xavfsiz taqsimlash, elektron raqamli imzo algoritmlarida va autentifikatsiyalash maqsadida foydalaniladi. Quyidagi 1.1.4-rasmda ochiq kalitli shifrlash usullaridan simmetrik kalitlarni shifrlashda foydalanish tartibi keltirilgan.



1.1.4 – rasm. Gibrid shifrlash usuli

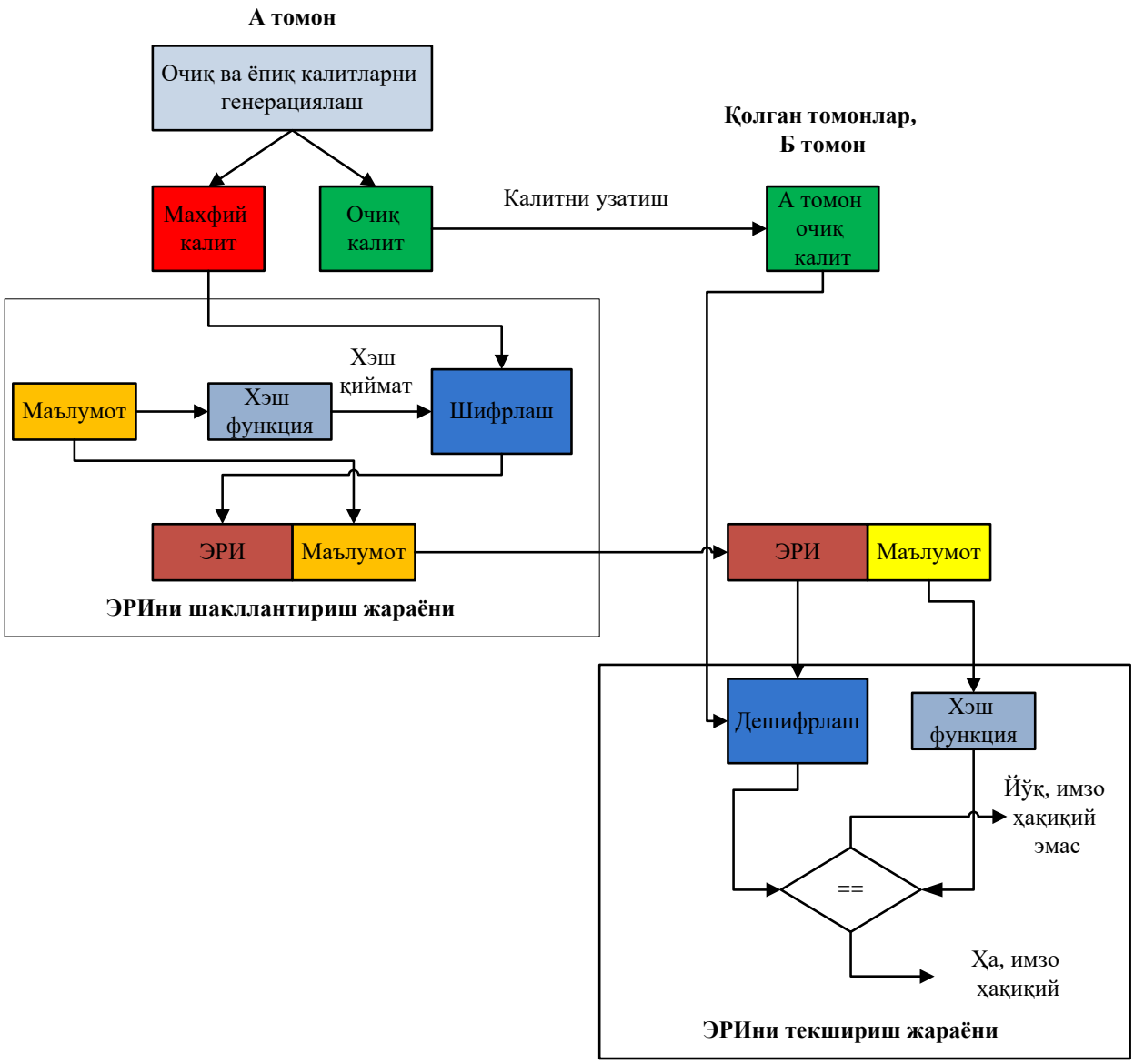
Bundan tashqari, ochiq kalitli kriptogarfik tizimlardan amalda elektron raqamli imzo algoritmlarini hosil qilishda keng qo‘llaniladi. Elektron raqamli imzo tarmoqda uzatilayotgan axborotni *butunligini, autentifikatsiyasini* va yuboruvchini *rad-etish*dan himoyalaydi.

Elektron raqamli imzo tizimlari ochiq kalitli kriptografik tizimlar va xesh – funksiyalar asosida yaratiladi (1.5-rasm). Xesh-funksiya ma’lumotni butuniligini ta’minlashda foydalanilsa, ochiq kalitli kriptografik tizimlar esa autentifikatsiya va rad etishdan himoyalash vazifasini bajaradi.

Xesh-funksiya – bir tomonlama akslantirishni amalga oshiruvchi funksiya bo‘lib, kiritilgan ixtiyoriy uzunlikdagi ma’lumotni fikserlangan uzunlikdagi qiymatga aylantirib beradi. Kriptogarfik xesh-funksiyaga quyidagi talablar qo‘yiladi:

- bir tomonlamalik, $y = f(x)$ dan x ni keltirib chiqarishning imkonsizligi;
- kirishda ixtiyoriy uzunlikdagi ma’lumotni qabul qilish;
- amallar bajaralishining tezkorligi yoki funksiyaning tezkor bo‘lishi;
- berilgan $x_1 \neq x_2$ ma’lumotlar uchun $f(x_1) = f(x_2)$ shartni qanoatlantirishi, ya’ni, kolliziyaga bardoshlik.

Elektron raqamli imzo va xesh-funkitsiyalar bo‘yicha aksariyat davlatlarda standartlar ishlab chiqilgan. Masalan, AQSh davlatida SHA3 xesh-funksiyalar oilasi [25], Rossiya Federeratsiyasida GOST R 34.11-2012 [26] va O‘zbekiston respublikasida O‘z DSt 1106:2009 xesh-funksiya standartlari [6] hozirgi kunda amalda foydalanilsa, ushbu davlatlarda mos ravishda ECDSA [27], GOST R 34.10-2012 [26] va O‘z DSt 1092:2009 [5] hamda O‘z DSt 2826:2014 [9] ERI standartlari mavjud.



1.1.5 – rasm. ERIni shakllantirish va tekshirish muolajasi

Kriptografiyaning yuqorida keltirilgan bo‘limlariga tegishli usullar axborotni ta’minlashda aynan bir vazifani bajarsa, kriptografik kalitlarni boshqarish tizimi ushbu usullarga xizmat qiladi. Kriptografik kalitlarni boshqarish tizimlari quyidagi vazifalarni bajarish orqali kriptografik tizimlar ishini to‘liq va xavfsiz bo‘lishini ta’minlaydi [17]:

- bardoshli kalitlarni generatsiyalash;
- kalitlar tomonlar orasida xavfsiz uzatish;
- kalitlarni xavfsiz saqlash.

Kriptografik kalitlar tizim uchun muhim ahamiyatga ega. Kriptografik algoritmlarning bardoshligi faqat kalitni no’malumligiga asoslanishini hisobga olinsa, kalitlarga yuqori talablar qo‘yilishini faraz qilish mumkin.

1.2. Kriptografik dasturiy vositalar va ularni yaratish usullari

Amalda kriptografik usullar axborot xavfsizligini ta’minlashda ma’lum ko‘rinishlarda shakllantiriladi. Kriptografik himoya usullari quyidagi vositalar shaklida amalga oshiriladi [18]:

- apparat kriptografik himoya vositasi;
- apparat-dasturiy kriptogarfik himoya vositasi;
- dastruriy kriptografik himoya vositasi.

Axborotning apparat ko‘rinishdagi kriptografik himoya vositalari o‘zining tezkorligi, xavfsizligi va narxining yuqoriligi bilan xarakterlanadi. Apparat ko‘rinishdagi kriptografik vositalarda barcha amallar qurilmaning resursi va xotirasidan foydalanib amalga oshiriladi. Bundan tashqari apparatning boshqa vositalar, masalan, kompyuter orqali boshqarilish yoki yangilash imkoniyati mavjud emas. Kriptografik apparat ko‘rinshdagi vositalarga maxsus tokenlarni misol keltirish mumkin.

Amalda yangilash va boshqarish imkoniyatiga ega va hisoblanishlarni qurilma xotirasida amalga oshiruvchi kriptografik vositalar – *apparat-dasturiy* kriptogarfik vositalar deb atalib, ular o‘zida apparat vositalarda mavjud barcha yaxshi xususiyatlarni mujassam etgan. Bundan tashqari apparat-dasturiy kriptogarfik vositalarning ham narxi yuqori bo‘lib, ularda asosan simmetrik kriptotizimlar amalda oshirilgan. Hozirgi kunda apparat-dasturiy vositalar ishlab chiqarish sohasida AKKORD, KRIPTON, GRYaDA kabi tashkilotlar etakchilik qilishmoqda.

Amalda keng tarqalgan kriptografik vosita bu – *dasturiy ko‘rinishdagi* himoya vositasi bo‘lib, ko‘p imkoniyatli, arzon va shuning bilan birga yangilanish imkoniyatlariga ega. Dasturiy ko‘rinishdagi kriptografik vositalar barcha amallarni kompyuter xotirasidan foydalangan holda amalga oshiradi. Apparat,

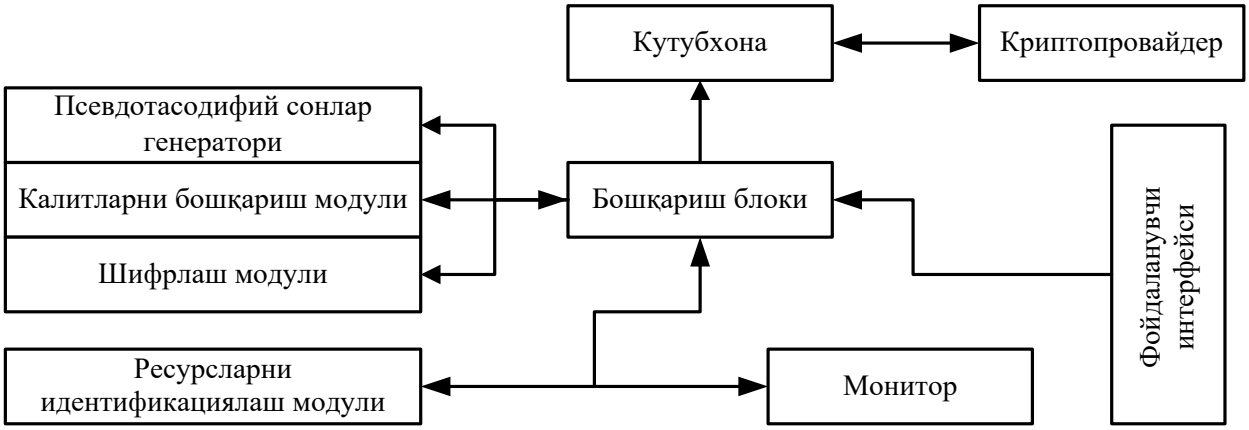
apparat-dasturiy va dasturiy kriptografik himoya vositalarining qiyosiy tahlili quyidagi 1.2.1-jadvalda keltirilgan.

1.2.1-jadval

Kriptogarfik himoya vositalarining qiyosiy tahlili

Vositalar turi/ Omillar	**Dasturiy**	**Apparat**	**Apparat-dasturiy**
Amal bajarish tezligi	sekin	tezkor	tezkor
Qo‘llanish sohasi	ERI va assimetrik shifrlashda	Simmetrik shifrlashda	Simmetrik va assimetrik shifrlashda, ERI
Amallarni bajarilish manbasi	ShK markaziy protsessori	Maxsus mikroprotsessor	Maxsus mikroprotsessor
Vositani yangilash imkoniyati	Mavjud, oson	Mavjud emas	Mavjud, murakkab
Bardoshliligi	Past	Yuqori	Yuqori
Narxi	Past	Yuqori	Yuqori

Kriptografik usullarni dasturiy ko‘rinishi o‘zida barcha usullar va algoritmlarni qamrab olgan bo‘lib, amalga keng qo‘llaniladigan ko‘rinishi hisoblanadi. Keng tarqalgan dasturiy vositalarga ZASTAVA kompleksi, PGP, Secret Disk kabilarni kiritish mumkin. Quyidagi 1.2.1-rasmda dasturiy kriptografik vositalarning umumiy sxemasi aks ettirilgan [18].



1.2.1-rasm. Kriptografik dasturiy vositalarning umumiy sxemasi

Boshqarish bloki barcha qolgan modullarni birlashtiradi va foydalanuvchi interfeysi orqali kiritilgan buyruqlarni amalga oshiradi. Dasturiy kriptogarfik himoya vositasining asosini kriptogarfik kutubxonalar tashkil etib, ular kriptoprovayderlar asosida operatsion tizim bilan mujassamlashtiriladi.

Kriptografik kutubxona dasturiy ta’minotlarning o‘zagi hisoblanib, unda zarur bo‘lgan algoritmlar amalga oshirilgan bo‘ladi. Boshqa modullar aynan ushbu kutubxonaga qiymatlar kiritish orqali natijalarni foydalanuvchiga qayd etadilar.

Amalda kriptografik dasturiy vositalarda barcha turdagi algoritmlar amalga oshiriladi va ular quyidagi vazifalarni bajarishda ko‘llaniladi [19]:

- foydalanuvchilarni identifikatsiya/ autentifikatsiyadan o‘tkazishda;
- operatsion tizim va dasturiy vositalarni kriptografik himoyasini ta’minlashda;
- tasodifiy va psevdotasodifiy kalitlarni generatsiyalashda;
- diskdagi barcha ma’lumotlarni shifrlashda;
- elektron raqamli imzo tizimlarini ishlab chiqishda va h.

Umumiy holda, dasturiy kriptografik himoya vositalari quyidagi xususiyatlarga ega:

- kriptografik dasturiy himoya vositalari boshqa qurilmalarda saqlangan bo‘lishi mumkin;
- blokli shifrlash algoritmlarida blok o‘lchami fayl segmenti o‘lchamini oshirishi mumkin, natijada esa fayl o‘lchami ortishi mumkin;
- dasturiy kriptografik himoya vositalarining shifrlash tezligi apparat vositalar tezligiga qaraganda past bo‘lishi mumkin, chunki barcha hisoblashlar markaziy protsessorda amalga oshiriladi.

Kriptogarafik algoritmlarni har qanday ko‘rinishda amalga oshirganda ham xavfsizlik muammolari mavjud bo‘lib, ular quyidagi hollarda yuzaga kelishi mumkin:

- mos axborotni himoyalash algoritmini tanlashdagi xatolik:

    - axborotni himoyalash algoritmlarini mos klasini tanlashdagi xatolik;
    - kriptografik algoritmlarni loyihalashdagi xatolik;
- kriptografik algoritmlarni amalga oshirishdagi xatolik;
- kriptografik algoritmni noto‘g‘ri usulda foydalanish;
- tashqari muhitning hisobga olinmagan xususiy xususiyatlari.

Birinchi holatdagi xatoliklarga xavfsiz bo‘lmagan MD2, MD4, MD5, HAVAL-128 xesh-funksiyalaridan foydalanishni misol keltirish mumkin. Ya’ni, ushbu xesh-funksiyalarning bardoshligi isbotlamagani yoki ularda kolliziya hodisasi kuzatilgani bois, zaiflik kelib chiqishi mumkin.

Ikkinchi turga tegishli bo‘lgan xatoliklarga quyidagilarni kiritish mumkin:

- dasturlashda mavjud bo‘lgan *bag*lar tufayli kelib chiqadigan xatoliklar;
- mos bo‘lmagan algoritmlardan foydalanish, masalan, kriptografik psevdoatasodfiy sonlar generatori talab etilganda uning o‘rniga dasturlash tilidagi oddiy *rand()* – funksiyasidan foydalanish.

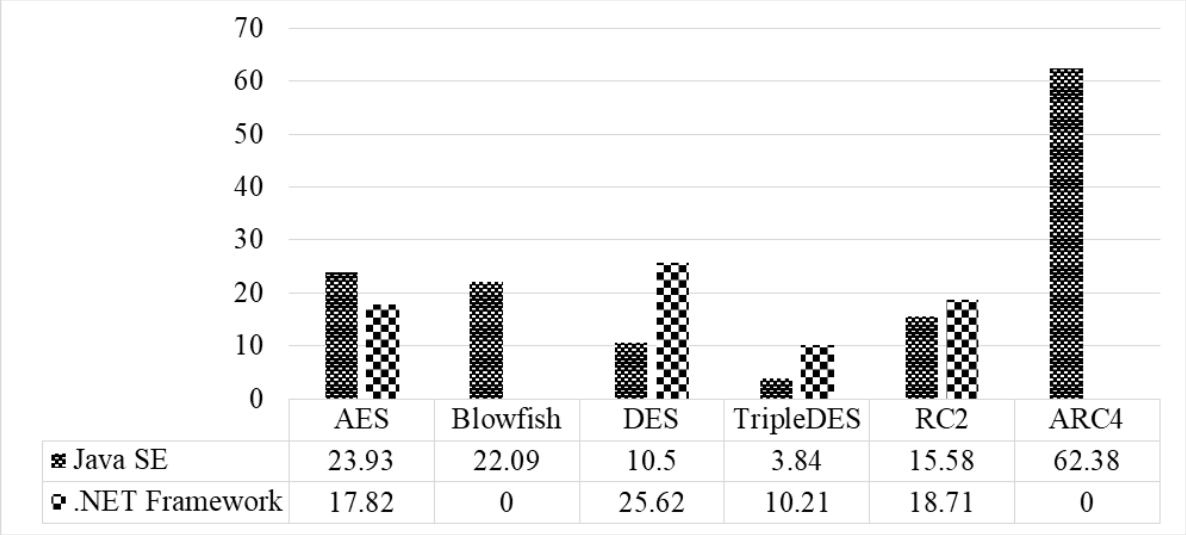
Keyingi turdagi xatolik bu kriptografik algoritmdan noto‘g‘ri tarzda foydalanish orqali kelib chiqadi. Masalan, psesdotasodifiy sonlar generatorini amalga oshirganda, uni vaqti-vaqti bilan ichki holatini yangilash (Reseed) amalga oshirilmasligi natijasida generator tasodifiy bo‘lmagan qiymatlarni hosil qilishi mumkin.

Oxirgi keltirilgan xatolik turiga quyidagi holatni keltirish mumkin. Faraz qilinsin, operatsion tizim dastur xotirasidan maxfiy axborotni (masalan, shifrlash kalitini) vaqtinchalik diskka ko‘chirmoqda. Ma’lumotlar diskka ko‘chirilgan vaqtda agar kompyuter to‘satdan o‘chib qolsa, u holda maxfiy ma’lumot noma’lum muddatda xavfsiz bo‘lmagan muhitda qoladi.

Bundan tashqari kriptografik algoritmlar maxsus *freymvork*lar ko‘rinishida amalga oshiriladi. Amalda keng keng tarqalgan kriptografik algoritmlarni o‘z ichiga olgan freymvorklar bu - *Microsoft .NET Framework* [28] va *Java Platform Standard Edition (Java SE)* [29] lardir. .NET Frameworki ixtiyoriy CLI tillari (C#, .NET uchun Visual Basic, .NET uchun Delphi, C++/CLI va h.)

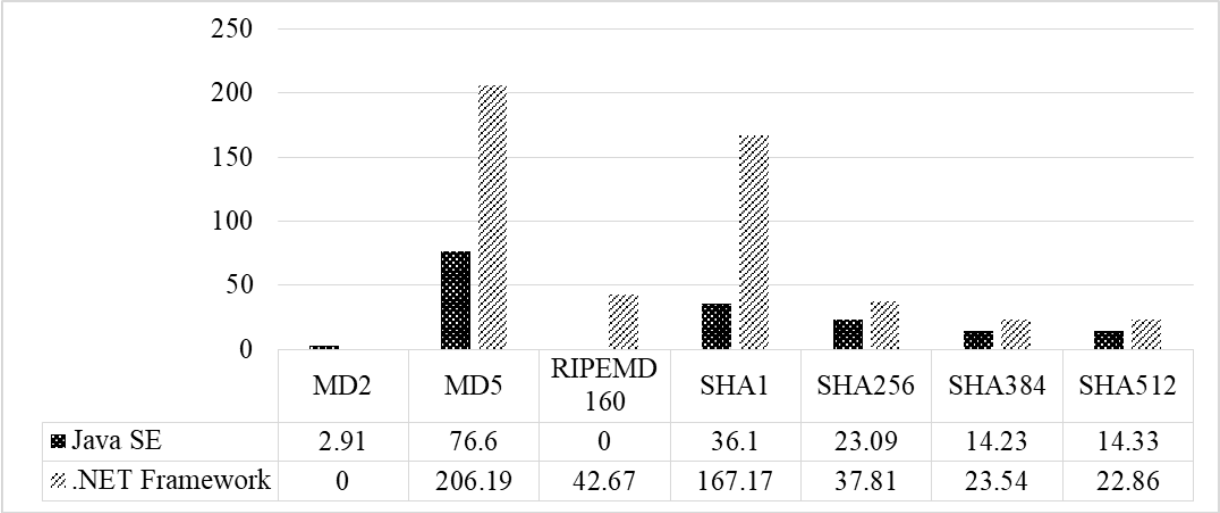
orqali foydalanilsa, Java Sedan esa Java dasturlash tilida yoki boshqa tillar orqali foydalanish mumkin.

Dasturlash tillarining imkoniyatidan kelib chiqib, bir kriptografik algoritm turlicha tezkorlik va boshqa xususiyatlarni taqdim etishi mumkin. Quyidagi 1.7, 1.8 va 1.9 – rasmlarda Java SE 6 va .NET Framework 3.5lard simmetrik blokli shifrlash algoritmlari va xesh-funksiyalarining o‘rtacha tezliklari keltirilgan [33].



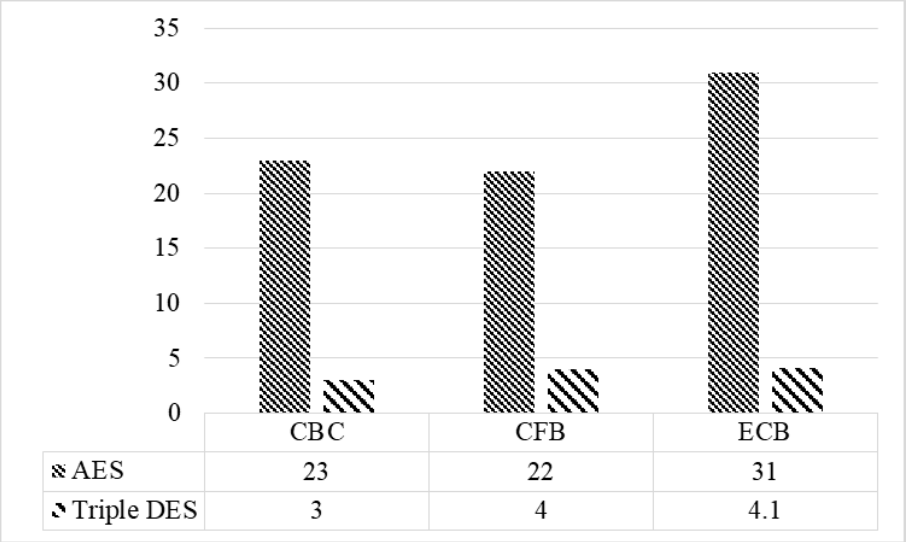
	AES	Blowfish	DES	TripleDES	RC2	ARC4
Java SE	23.93	22.09	10.5	3.84	15.58	62.38
.NET Framework	17.82	0	25.62	10.21	18.71	0

1.2.2-rasm. Turli simmetrik shifrlarning tezlik bo‘yicha tahlili (MB/c)

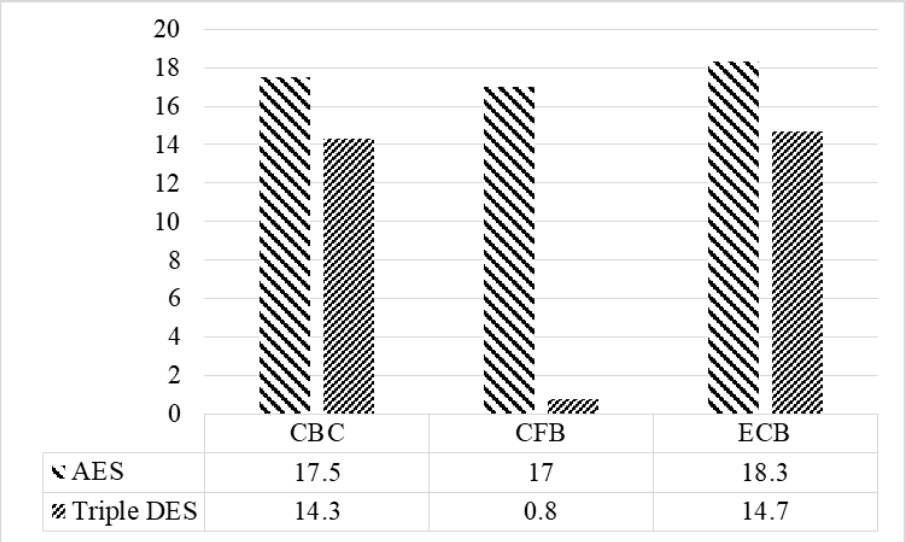


	MD2	MD5	RIPEMD 160	SHA1	SHA256	SHA384	SHA512
Java SE	2.91	76.6	0	36.1	23.09	14.23	14.33
.NET Framework	0	206.19	42.67	167.17	37.81	23.54	22.86

1.2.3-rasm. Turli xesh-funkitsiyalarning tezlik tahlili (MB/s)



a) Java SEda turli simmetrik shifrlash rejimlari tezligi (MB/s)



b) .Net Frameworkda turli simmetrik shifrlash rejimlari tezligi (MB/s)

1.2.4-rasm. Turli blokli shifrlash rejimlarining tezliklari tahlili

1.3. Mavjud kriptografik kutubxonalarning tahlili

Hozirgi kunda kriptografik himoya axborotning ishonchli himoyalash usullardan biri sanalib, ma’lumot ustida turli o‘zgartirishlarni (shifrlash amallari) amalga oshirgan holda uni ruxsat etilmagan foydalanuvchi uchun tushunarsiz ko‘rinishga olib keladi. Ushbu shifrlash amallari maxsus algoritmlar to‘plamidan foydalanilgan holda turli yo‘llar bilan amalga oshiriladi.

Kriptografik kutubxona – kriptografik maqsadda foydalanish uchun zarur bo‘lgan bir qancha algoritmlarning to‘plami bo‘lib, u odatda jamlangan algoritmlarni bajaradigan vazafasiga ko‘ra turkumlangan holda o‘zida saqlaydi.

Hozirda turli dasturlar tillari uchun yaratilgan qator kriptografik kutubxonalar mavjud bo‘lib, ularning algoritm tarkibi va amalga oshirilishi turlicha.

Kriptografik kutubxonalarni yaratishda xavfsizlik birlamchi va muhim talab bo‘lganligi bois, bu jarayon uzoq vaqt, katta xarajat va yuqori malakani talab etadi. Shu bois mavjud kriptografik kutubxonalarni foydalanishdan oldin, ularning xususiyatlari haqida axborotga ega bo‘lish talab etiladi.

Kriptografik kutubxonalardagi algoritmlar odatda quyidagicha turkumlanishi mumkin:

- kriptografik kalitlarni generatsiyalash va taqsimlash algoritmlari;
- blokli shifrlash algoritmlari;
- xesh funksiya algoritmlari;
- oqimli shifrlash algoritmlar;
- xabarlarni autentifikatsiyalash kodlari;
- ochiq kalitli kriptografik tizimlar (asosan elliptik egri chiziq);
- ochiq kalit kriptografiyasi standartlari va h.

Ushbu maqolada quyida keltirilgan keng foydalaniluvchi kriptografik kutubxonalarning yuqoridagi omillar bo‘yicha tahlili keltirilgan (1.2-1.6 - jadvallar) [30, 32]:

- Botan;
- Bouncy Castle;
- cryptlib;
- Crypto++;
- Libgcrypt;
- libsodium;
- libtomcrypt;
- Nettle;
- OpenSSL;
- wolfCrypt.

1.3.1 – jadval

Kriptografik kutubxonalar xususiyatlarining qiyosiy tahlili

№	Algoritm nomi	Ishlab chiqilgan til	Ochiq kodli	Litsenziya	Madadlovchi operatsion tizimlar
1.	Botan	S++	+	Soddalashgan BSD	Linux, FreeBSD, AIX, Windows, macOS, Android, iOS, QNX, IncludeOS
2.	Bouncy Castle	Java, C#	+	MIT litsenziya	J2ME, Java Runtime Environment 1.1+, Android, Android. C# API
3.	cryptlib	C	+	Tijoriy litsenziya	AMX, BeOS, ChorusOS, DOS, eCOS, FreeRTOS/OpenRTOS, uItron, MVS, OS/2, Palm OS, QNX Neutrino, RTEMS, Tandem NonStop, ThreadX, uC/OS II, Unix (AIX, FreeBSD, HP-UX, Linux, macOS, Solaris, etc.), VDK, VM/CMS, VxWorks, Win16, Win32, Win64, WinCE/PocketPC/etc, XMK
4.	Crypto++	C++	+	Ochiq litsenziya	Unix (OpenBSD, Linux, macOS, etc.), Win32, Win64, Android, iOS, ARM
5.	Libgcrypt	C	+	GNU LGPL v2.1+	Barcha UNIX operatsion tizimlari va Win32, Win64, WinCE
6.	libsodium	C	+	ISC litsenziya	macOS, Linux, OpenBSD, NetBSD, FreeBSD, DragonflyBSD, Android, iOS, 32 va 64-bit Windows (Visual Studio, MinGW, C++ Builder), NativeClient, QNX, JavaScript, AIX, MINIX, Solaris
7.	libtomcrypt	C	+	Ochiq	GNU/Linux, FreeBSD, macOS, Windows
8.	Nettle	C	+	GNU GPL v2+	GNU/Linux, FreeBSD, macOS, Windows
9.	OpenSSL	C	+	Apache Licence 1.0	Solaris, Linux, macOS, QNX, BSD, Windows, OpenVMS
10.	wolfCrypt	C	+	GPL v2 yoki tijoriy	Win32/64, Linux, macOS, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded Linux, WinCE, Haiku, OpenWRT, iPhone (iOS), Android, Nintendo Wii va Gamecube through

№	Algoritm nomi	Ishlab chiqilgan til	Ochiq kodli	Litsenziya	Madadlovchi operatsion tizimlar
					DevKitPro, QNX, MontaVista, NonStop, TRON/ITRON/µITRON, Micrium's µC/OS, FreeRTOS, SafeRTOS, Freescale MQX, Nucleus, TinyOS, HP-UX

1.3.2 – jadval

Kriptografik kutubxonalarning qiyosiy tahlili (kalitlarni generatsiyalash, taqsimlash va ochiq kalitli kriptografik tizimlar)

№	Kutubxona nomi	Mavjud algoritmlar	
		Kalitlarni generatsiyalash va taqsimlash	Ochiq kalitli kriptorafik tizimlar
1.	Botan	ECDH, DH, DSA, RSA, ElGamal, DSS	NIST, SECG, ECC Brainpool, ECDSA, Curve25519, EdDSA
2.	Bouncy Castle	ECDH, DH, DSA, RSA, ElGamal, NTRU, DSS	NIST, SECG, ECC Brainpool, ECDSA, Curve25519, GOST R 34.10
3.	cryptlib	ECDH, DH, DSA, RSA, DSS	NIST
4.	Crypto++	ECDH, DH, DSA, RSA	NIST
5.	Libgcrypt	ECDH, DH, DSA, RSA, ElGamal, DSS	NIST, SECG, ECC Brainpool, ECDSA, Curve25519, EdDSA, GOST R 34.10
6.	libsodium	DH, DSA, ElGamal, NTRU, DSS	NIST, Curve25519, EdDSA
7.	libtomcrypt	ECDH, DH, DSA, RSA	
8.	Nettle	DSA, RSA	NIST
9.	OpenSSL	ECDH, DH, DSA, RSA	NIST, SECG, ECC Brainpool, ECDSA, Curve25519
10.	wolfCrypt	ECDH, DH, DSA, RSA, NTRU, DSS	NIST, Curve25519, EdDSA

1.3.3 – jadval

Kriptografik kutubxonalarning qiyosiy tahlili (xesh funksiyalar va xabarlarni autentifikatsiyalash kodlari)

№	Kutubxona nomi	Mavjud algoritmlar	
		Xesh funksiyalar	Xabarlarni autentifikatsiyalash kodlari
1.	Botan	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, GOST, Stribog, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
2.	Bouncy Castle	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, GOST, Stribog, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC

№	Kutubxona nomi	Mavjud algoritmlar	
		Xesh funksiyalar	**Xabarlarni autentifikatsiyalash kodlari**
3.	cryptlib	MD5, SHA1, SHA2, SHA3, Repidm-160, Whirlpool	HMAC-MD5, HMAC-SHA1, HMAC-SHA2
4.	Crypto++	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, GOST, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, BLAKE2-MAC
5.	Libgcrypt	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, GOST, Stribog, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
6.	libsodium	SHA2, Blake2	HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
7.	libtomcrypt	MD5, SHA1, SHA2, SHA3, Repidm-160, Tiger, Whirlpool, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC
8.	Nettle	MD5, SHA1, SHA2, SHA3, Repidm-160, GOST, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES
9.	OpenSSL	MD5, SHA1, SHA2, Repidm-160, Tiger, Whirlpool, GOST, Blake2, MD2, MD4,	Poly1305-AES, HMAC
10.	wolfCrypt	MD5, SHA1, SHA2, SHA3, Repidm-160, Blake2	HMAC-MD5, HMAC-SHA1, HMAC-SHA2, Poly1305-AES, BLAKE2-MAC

1.3.4 – jadval

Kriptografik kutubxonalarning qiyosiy tahlili (blokli shifrlash va shifrlash rejimlari)

№	Kutubxona nomi	Mavjud algoritmlar	
		Blokli shifrlash	**Shifrlar rejimlari**
1.	Botan	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish, Twofish, CAST5, IDEA, GOST 28147-89	CBC, OFB, CFB, CTR, CCM, GCM, OCB, XTS, AES-Wrap, Stream
2.	Bouncy Castle	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish, Twofish, CAST5, IDEA, GOST 28147-89	ECB, CBC, OFB, CFB, CTR, CCM, GCM, OCB, AES-Wrap, Stream
3.	cryptlib	AES-128, AES-192, AES-256, 3DES, Blowfish	ECB, CBC, CTR
4.	Crypto++	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish	ECB, CBC, CTR, CCM, GCM
5.	Libgcrypt	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish, Twofish, CAST5, IDEA, GOST 28147-89	ECB, CBC, OFB, CFB, CTR, CCM, GCM, OCB, XTS, AES-Wrap, Stream
6.	libsodium	AES-256	CTR, GCM
7.	libtomcrypt	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish, Twofish, CAST5	ECB, CBC, OFB, CFB, CTR, CCM, GCM, OCB, XTS, Stream
8.	Nettle	AES-128, AES-192, AES-256, Camellia, 3DES, Blowfish	ECB, CBC, CTR, CCM, GCM

№	Kutubxona nomi	Mavjud algoritmlar	
		Blokli shifrlash	Shifrlar rejimlari
9.	OpenSSL	AES-128, AES-192, AES-256, Camellia, 3DES, CAST5, IDEA	CBC, OFB, CFB, CTR, CCM, GCM, OCB, XTS, AES-Wrap, Stream
10.	wolfCrypt	AES-128, AES-192, AES-256, Camellia, 3DES, IDEA	ECB, CBC, CTR, CCM, GCM

1.3.5 – jadval

Kriptografik kutubxonalarning qiyosiy tahlili (ochiq kalit standartlari va oqimli shifrlash algoritmlari)

№	Kutubxona nomi	Mavjud algoritmlar	
		Ochiq kalit standartlari	Oqimli shifrlash algoritmlari
1.	Botan	PKCS#1, PKCS#5, PKCS#8, IEEE P1363, ASN.1	RC4, Salsa20, ChaCha
2.	Bouncy Castle	PKCS#1, PKCS#5, PKCS#8, PKCS#12, IEEE P1363, ASN.1	RC4, HC-256, Salsa20, ChaCha, Grain, VMPC, ISAAC
3.	cryptlib	PKCS#1, PKCS#5, PKCS#8, PKCS#12, ASN.1	RC4
4.	Crypto++	PKCS#1, PKCS#5, IEEE P1363, ASN.1	RC4, Salsa20, SEAL, Panama, WAKE
5.	Libgcrypt	PKCS#1, PKCS#5, PKCS#8, PKCS#12, IEEE P1363, ASN.1	RC4, Salsa20, ChaCha
6.	libsodium		Salsa20, ChaCha
7.	libtomcrypt	PKCS#1, PKCS#5, PKCS#8, ASN.1	RC4, ChaCha
8.	Nettle	PKCS#1, PKCS#5	RC4, Salsa20, ChaCha
9.	OpenSSL	PKCS#7, PKCS#12, ASN.1	RC4, ChaCha
10.	wolfCrypt	PKCS#1, PKCS#5, PKCS#8, PKCS#12, ASN.1	RC4, HC-256, Rabbit, Salsa20, ChaCha

Olingan tahlil natijalari mos dasturlash tiliga qarab kutubxonani tanlashda, kriptografik algoritmlardan xavfsiz foydalanishda, algoritmlarning tezlik bo‘yicha taqqoslashda katta samara beradi. Ushbu kutubxonalardan foydalanish kod qatorini kamaytirishga, xavfsiz kodni yaratishga va sarflanadigan vaqt hajmini kamayishiga sababchi bo‘ladi.

Yuqorida keltirilgan tahlil natijalaridan shuni bilish mumkinki, aksariyat kutubxonalar xalqaro algoritmlar yoki AQSh standartlari va kamdan – kam holda Rossiya davlat standartlarini o‘z ichiga olgan. Shuni hisobga olgan holda, milliy standartlarni o‘z ichiga olgan kriptografik kutubxonani yaratish dolzarbdir. Shuning uchun ushbu kriptografik kutubxonani yaratish keyingi tadqiqot ishining maqsadi qilib olindi.

Birinchi bob bo‘yicha xulosalar

1. Axborotni maxfiyligini, butunligini, autentifikatsiyasini va rad etishdan himoyalashda kriptografik usullarning o‘rni muhimligi aniqlandi.

2. Kriptografik algoritmlar apparat, apparat-dasturiy va dasturiy ko‘rinishlarda amalga oshirilib, ular ichida keng qamrovligi, yangilashning osonli va narxning kamligi xususiyatlari bo‘yicha dasturiy ko‘rinishdagi kriptografik vositalar afzal deb topildi.

3. Kriptografik dasturiy vositalarni qurishda maxsus kriptografik kutubxonalardan va freymvorklarga asoslanilishi aniqlandi.

4. Mavjud kriptografik kutubxonalar tahlil qilinganda ularda asosan xalqaro kriptografik algoritmlar, AQSh yoki Rossiya davlati standartlarini amalga oshirilganligi, milliy kriptografik algoritmlarni amalga oshirilmaganligi aniqlandi.

II bob. Milliy kriptografik algoritmlar va ularning tahlili

2.1. O‘z DSt 1105:2009 - ma’lumotlarni shifrlash algoritmi

Ushbu bobda milliy kriptografik standartlar bilan tanishilib, ularni kutubxona sifatida shakllantirish masalasi ko‘rib chiqiladi. Hozirda kriptografiya sohasida quyidagi milliy standartlar mavjud:

- O‘z DSt 1105:2009 - ma’lumotlarni shifrlash bo‘yicha standart;
- O‘z DSt 1106:2009 - xesh – funksiya standarti;
- O‘z DSt 1092:2009 va O‘z DSt 2826:2014 - elektron raqamli imzoni shakllantirish va tekshirish standartlari.

Mazkur bo‘limda ma’lumotni shifrlash standarti O‘z DSt 1105:2009 tahlil qilinadi. Ushbu standart «UNICON.UZ» - Fan-texnika va marketing tadqiqotlari markazi davlat unitar korxonasi («UNICON.UZ» DUK) tomonidan ishlab chiqilgan va foydalanishga kiritilgan. Ushbu standartda O‘zbekiston Respublikasining «Elektron raqamli imzo to‘g‘risida»gi va «Elektron hujjat almashuvi to‘g‘risida»gi qonunlarining normalariga amal qilingan. Ushbu standartning dastlab ishlab chiqilgan O‘z DSt 1105:2006 o‘rniga ishlab chiqilgan [12].

«Ma’lumotlarni shifrlash algoritmi» (MShA) standarti elektron ma’lumotlarni muhofaza qilish uchun mo‘ljallangan kriptografik algoritmni ifodalaydi. MShA - simmetrik blokli shifr bo‘lib, axborotni shifrmatnga o‘girish va dastlabki matnga o‘girish uchun foydalaniladi. MShA 256 bit uzunlikdagi ma’lumotlar blokini shifrmatnga o‘girish va shifrmatnni dastlabki matnga o‘girish uchun 256 yoki 512 bit uzunlikdagi kriptografik kalitdan foydalanishi mumkin.

Standart, elektron hisoblash mashinalari (EHM) tarmoqlarida, alohida hisoblash komplekslari va EHMda axborotga ishlov berish tizimlarida axborotni shifrlashning yagona algoritmini o‘rnatib, ma’lumotlarni shifrlash qoidalarini belgilaydi.

Ma’lumotlarni shifrlash algoritmi dasturiy, apparat yoki apparat-dasturiy kriptografik modullarda amalga oshirish uchun mo‘ljallangan. Tashkilotlar,

korxonalar va muassasalar EHM tarmoqlarida, alohida hisoblash komplekslarida yoki EHMda saqlanuvchi va uzatiluvchi ma’lumotlarning kriptografik muhofazasini amalga oshirishda mazkur standartdan foydalanishlari mumkin.

Ushbu standartni ishlab chiqish davomida O‘z DSt 1047 [10], O‘z DSt 1109 [11] bo‘yicha atamalar, hamda quyidagi atamalar mos ta’riflari bilan qo‘llanilgan:

- *initsializatsiyalash vektori:* Kriptografik algoritm doirasida kriptografik jarayonning tayanch nuqtasini aniqlash uchun ishlatiladigan vektor.
- *seans kaliti:* Shifrlash kaliti va funksional kalit asosida shakllanadigan maxfiy kalitlarning ikki o‘lchamli massivi.
- *shifrlash vositalari:* Axborot almashtirishning kriptografik algoritmlarini amalga oshiruvchi va ularni qayta ishlashda, saqlashda va telekommunikatsiya kanallari bo‘ylab uzatishda axborotni ruxsat etilmagan foydalana olishdan muhofaza qilish uchun mo‘ljallangan apparat, dasturiy va apparat-dasturiy vositalar.
- *shifrmatn bloklarini ilaktirish rejimi:* Har bir shifrlangan (dastlabki matnga o‘girilgan) kriptografik blok oldingi shifrlangan (dastlabki matnga o‘girilgan) blokka bog‘liq bo‘lgan shifrlash rejimi. Birinchi blok uchun shifrmatnning oldingi bloki sifatida initsializatsiyalash vektoridan foydalaniladi. Ochiq matnning oxirgi bloki to‘liq bo‘lmagan holatda, u zarur uzunlikkacha to‘ldiriladi.
- *elektron kod kitobi rejimi:* Ochiq matnning barcha bloklari ma’lumotlarini shifrlash algoritmlariga muvofiq bir-biridan mustaqil, bitta kalit bilan shifrlanadigan shifrlash rejimi.

  Ushbu standartda quyidagi belgilanishlardan foydalanilgan:

  M – dastlabki (ochiq) matn;

  S – shifrmatn;

  m – shifrlash rejimi;

sh – dastlabki matnni shifrmatnga o‘girish rejimi indeksi;

dsh – shifrmatnni dastlabki matnga o‘girish rejimi indeksi;

Holat – ikki o‘lchamli holat massivi;

$H_{ch,}$ H_o – ikki o‘lchamli holat massivining chap (yuqori) va o‘ng (quyi) qismi;

k – shifrlash kaliti;

k_f – funksional kalit;

k_{se} – seans-bosqich kaliti;

B_a – elementlarni bayt sathida almashtirish chiziqli massivi;

K_{ss} – shifrlash seans kaliti elementlarining chiziqli massivi;

K_s – shifrlash seans kalitining ikki o‘lchamli massivi;

K_{sch}, K_{so} – shifrlash seans kaliti massivining chap (yuqori) va o‘ng (quyi) qismi (yarmi);

K_e – bosqich kalitining ikki o‘lchamli massivi;

r, (p+1) – modul, $p = 256$;

ye – shifrmatnga o‘girish yoki dastlabki matnga o‘girish protsedurasining bosqichlar soni;

bosqich – shifrmatnga o‘girish yoki dastlabki matnga o‘girish protsedurasining tartib raqami;

R – parametr;

$\oplus$ – *XOR* amalining belgisi (*2* modul bo‘yicha qo‘shish amali);

® – sonlarni *p* modul bo‘yicha *R* parametr bilan ko‘paytirish amalining simvoli;

$®_2$ – *p* modul bo‘yicha diamatritsaviy ko‘paytirish amalining simvoli;

$\backslash^{-1}$ – *p* modul bo‘yicha *R* parametr bilan teskarilash amalining simvoli;

$\backslash^{d}$ – *p* modul bo‘yicha *R* parametr bilan *d*-darajaga oshirish amalining simvoli;

$^{-1}$ – *p* yoki *p+1* modul bo‘yicha teskarilash amalining simvoli;

IV – initsializatsiyalash vektori.

MShAda quyidagi matematik amallardan foydalanilgan:

- modul arifmetikasining diamatritsalar algebrasidan;
- butun sonlarni parametrli ko‘paytirish, teskarilash va darajaga oshirish deb atalgan parametrli algebra amallaridan foydalanilgan.

Shifrmatnga o‘girish va dastlabki matnga o‘girish protseduralarida foydalaniladigan diamatritsalar algebrasining asosiy amali diamatritsani *p* modul bo‘yicha diamatritsaga teskarilash amali hisoblanadi. Bu amallarda ikki o‘lchamli seans kaliti massivining maxsus tuzilmali *4*x*4* tartibli kvadrat diamatritsa bilan aks ettiriluvchi qismlari ishtirok etadi; maxsus tuzilmali diamatritsa uchun barcha diagonal elementlar bir xilligi, *1*-satrdagi nodiagonal elementlar, shuningdek *2*-satrning boshi va oxiridagi elementlar ham bir xilligi xosdir. *4*x*4* tartibli maxsus tuzilmali diamatritsa bayt darajasida o‘nta element asosida shakllanadi. 2.1-jadvalda d_0 , d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9 elementlar asosida shakllangan diamatritsa keltirilgan.

2.1.1-jadval

Maxsus tuzilmali diamatritsa

d_7	d_0	d_1	d_2
d_8	d_7	d_8	d_8
d_9	d_3	d_7	d_9
d_4	d_5	d_6	d_7

*4*x*4* tartibli maxsus tuzilmali diamatritsaning diaaniqlovchisi diagonal elementni uchta yig‘indiga ko‘paytmasi sifatida topiladi, bu yig‘indilardan har biri diagonal element bilan bitta satrda joylashgan o‘ngdan qo‘shni element bilan ustun elementlarining yig‘indisini ifodalaydi.

Ko‘rilayotgan diamatritsa uchun diaaniqlovchi *d* quyidagicha topiladi:

$$d \equiv d_7 \text{ x } (d_7 + d_0 + d_8 + d_3 + d_5) \text{ x } (d_7 + d_1 + d_8 + d_9 + d_6) \text{ x } (d_7 + d_2 + d_8 + + d_9 + d_4) \ (mod\ p).$$

(1)

Maxsus tuzilmali diamatritsani teskarilash shartlarini tekshirish MShA parametrlariga qo‘yiladigan asosiy talab hisoblanadi. U diagonal elementning

qiymatlarini va aytib o‘tilgan ko‘paytmalarni *2* moduli bo‘yicha nol bilan taqqoslashga keltiriladi. Bu har qanday shifrlash kaliti va funksional kalitdan teskari diamatritsani shakllantirishga imkon beradi.

MShAda elementlarni aralashtirish uchun *4*x*4* tartibli diamatritsalar ustida ko‘paytirish amalidan foydalaniladi:

$$H' \equiv H \circledR_2 K \ (mod\ p),$$

bu yerda $\circledR_2$ – *p* modul bo‘yicha diamatritsaviy ko‘paytirish amalining simvoli, *H’*, *H*, *K* – *4*x*4* tartibli diamatritsalar, *H’* – natijaviy diamatritsa, *H*, *K* – berilgan diamatritsalar.

Diamatritsaviy ko‘paytirish amali $\circledR_2$ quyida keltirilgan ifodalar asosida hisoblanadi.

s, *u* $\in \{0,1,2,3\}$ uchun:

$$h'[u,u] \equiv h[u,u] * \Sigma^{3}_{i=0}\, k[i,u] - \Sigma^{3}_{i=0,\ i\neq u} h[i,i] * k[i,u] \ (mod\ p),$$

$$h'[s,u]_{s\neq u} \equiv h[s,u] * \Sigma^{3}_{i=0}\, k[i,u] + k[s,u] * \Sigma^{3}_{i=0}\, h[i,u] - \Sigma^{3}_{i=0;\ i\neq s,u} h[s,i] * k[i,u] \ (mod\ p),$$

bu yerda *h’[u,u]* - natijaviy diamatritsaning diagonal elementi, *h’[s,u]* - natijaviy diamatritsaning nodiagonal elementi, *h[s,u]*, *h[i,u]*, *h[s,i]*, *h [i,i]*, *k[i,u]*, *k[s,u]*,– *H*, *K* ning elementlari.

MShAda shuningdek butun sonlarni parametrli ko‘paytirish, teskarilash va darajaga oshirish deb atalgan parametrli algebra amallaridan foydalaniladi.

X ni *Y* ga *p* modul bo‘yicha *R* parametrli ko‘paytirish amali $X \circledR Y \ (mod\ p)$ ko‘rinishda belgilanadi va quyidagi ko‘rinishda aniqlanadi:

$$X \circledR Y \ (mod\ p) \equiv X + Y\,(1 + R\,X) \ (mod\ p). \qquad (2)$$

Ushbu amal kommutativ va assotsiativ amaldir.

X o‘zgaruvchini *r* modul bo‘yicha *R* parametrli teskarilash amali $X^{\backslash -1} \ (mod\ p)$ shaklida belgilanadi va quyidagi ko‘rinishda aniqlanadi:

$$X^{\backslash -1} \ (mod\ p) \equiv -X\,(1 + R\,X)^{-1} \ (mod\ p), \qquad (3)$$

bu yerda $X^{\backslash -1} \circledR X \equiv 0 \ (mod\ p)$, *0* – parametrli gruppaning birlik elementidir.

Asos *X* ni *p* modul bo‘yicha *R* parametr bilan *d*-darajaga oshirish amali $X^{\backslash d}$ *(mod p)* ko‘rinishida ifodalanadi. Masalan, *d = 37* bo‘lganda *R* parametr bilan $X^{\backslash d}$ quyidagicha hisoblanadi:

$X^{\backslash 37} \Rightarrow X^{\backslash 32+4+1}\ (mod\ p) \equiv ((((X^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2} \circledR\ (X^{\backslash 2})^{\backslash 2} \circledR\ X\ (mod\ p)$,

bu yerda: $X^{\backslash 2}\ (mod\ p) \equiv X\ (2 + X\ R)\ (mod\ p)$.

MShAda foydalaniladigan sonlarni parametrli darajaga oshirish amali bayt bo‘yicha qayta almashtirish talabini hisobga olgan holda amalga oshirilgan.

MShA quyidagi parametr va funksiyalardan foydalanadi:

a) *k – 256* yoki *512* bit uzunlikdagi shifrlash kaliti;

b) k_f *– 256* bit uzunlikdagi funksional kalit;

c) K_e *– 8*x*4 (*yoki *4*x*8)* tartibli ikki o‘lchamli massiv shaklidagi bosqich kaliti;

d) *b – 256* bit li kirish bloklari soni;

e) *ye* – bosqichlar soni, *ye=8*;

f) *r, (r +1)* – modul, *r=256*;

g) *Aralash()* – oddiy shifralmashtirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirish uchun diamatritsaviy qismlar ustida amalga oshiriladi; mazkur shifralmashtirish kirishi *Holat* massivining diamatritsaviy qismlari hamda K_1 va K_2 massivlari bo‘lib, chiqishi *Holat* massividir;

h) *BaytAlmash()* – oddiy shifralmashtirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda *Holat* massivi elementlarini almashtirish massivi elementlari bilan bayt sathida almashtirish uchun foydalaniladi; mazkur shifralmashtirish kirishi bayt sathida *Holat* massivi, almashtirish masivi chiziqli massiv B_{sA} *[256]* yoki B_{sAD} *[256]* bo‘lib, chiqishi bayt sathida *Holat* massividir;

i) *Sur()* – *Holat* massivi elementlarini yanada yaxshiroq aralashtirish uchun, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirishda foydalaniladi; mazkur almashtirish kirishi bayt sathida *Holat* massivi, chiqishi ustun bo‘ylab shifrlashda pastga va satr bo‘ylab o‘ngga yoki shifrni ochishda

ustun bo‘ylab yuqoriga va satr bo‘ylab chapga surilgan bayt sathida *Holat* massividir;

j) *ShaklSeansKalitBayt()* – seans uchun kalit shakllantirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirishda *BaytAlmash()* shifralmashtirishini bajarish uchun foydalaniladi; mazkur shifralmashtirish kirishi shifrlash kaliti *k* va funksional kalit k_f bo‘lib, chiqishi bayt sathida chiziqli massivlar B_{sA} *[256]* va B_{sAD} *[256]*;

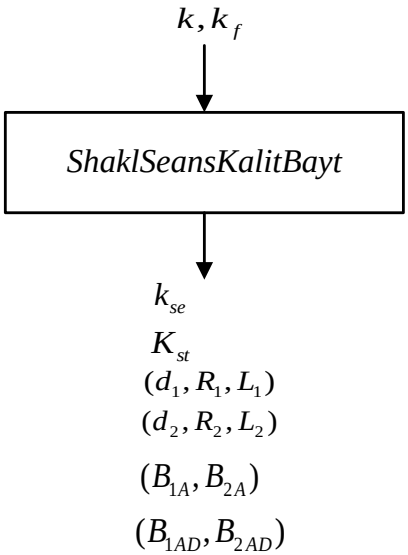
k) *ShaklSeansKalit()* – seans uchun kalit shakllantirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirishda *Aralash()* shifralmashtirishini bajarish uchun foydalaniladi; mazkur shifralmashtirish kirishi baytli elementlardan tarkib topgan chiziqli massiv K_{st}*=[32]* bo‘lib, chiqishi maxsus tuzilmali diamatritsalardan tashkil topgan (K_{1t}, K_2) yoki (K_1, K_{2t}) massivlar juftliklaridir;

l) *ShaklBosqichKalit()* – seans davomida seans-bosqich kalitidan bosqich kalitini shakllantirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirishda *Qo’shBosqichKalit()* almashtirishini bajarish uchun foydalaniladi; mazkur almashtirish kirishi chiziqli seans-bosqich kaliti massivi k_{se}, chiqishi bayt sathida berilgan ikki o‘lchamli K_e*[8,4]* massividir;

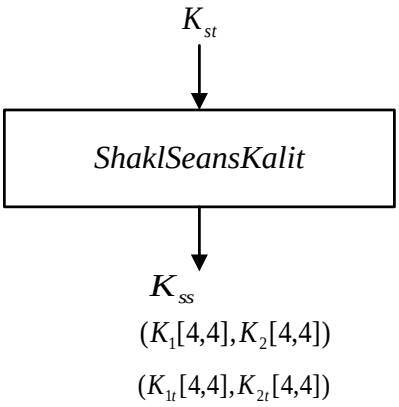
m) *Qo’shBosqichKalit()* – oddiy shifralmashtirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda *Holat* va bosqich kaliti massivi K_e elementlari ustida istisnoli yoki (*2* moduli bo‘yicha bitlab qo‘shish) amalini bajarishdan iborat; mazkur shifralmashtirish kirishi bayt sathida *Holat* massivi, K_e massivi bo‘lib, chiqishi bayt sathida *Holat* massividir;

n) *Qo’shHolat()* – oddiy shifralmashtirish bo‘lib, shifrlash bloklari ustida amalga oshiriladigan elektron kod kitobi rejimidan boshqa rejimlarda dastlabki matnni shifrmatnga va teskari yo‘nalishda *XOR* amali ishtirokida foydalaniladigan almashtirish. MShAda yuqorida keltirilgan akslantirishlarning kirish qiymatlari va ularga mos bo‘lgan chiqish quymatlari quyida keltirilgan (ularni amalga oshirish tartibi standartda keltirib o‘tilgan [12]):

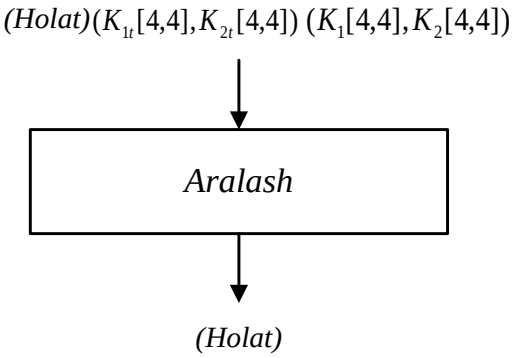
1. *ShaklSeansKalitBayt(k,*k_f*)* almashtirishi



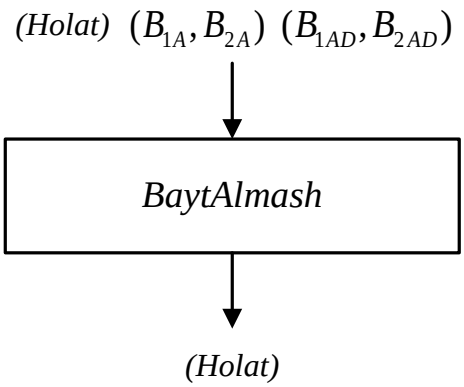
2. *ShaklSeansKalit (K_{st})* almashtirishi



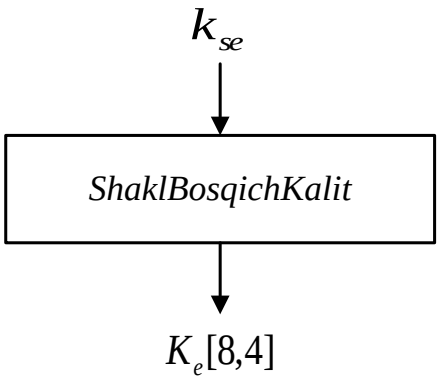
3. *Aralash (Holat, K_s)* almashtirishi



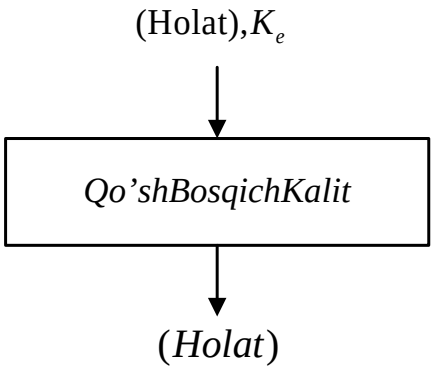
4. *BaytAlmash(Holat, B_a)* almashtirishi



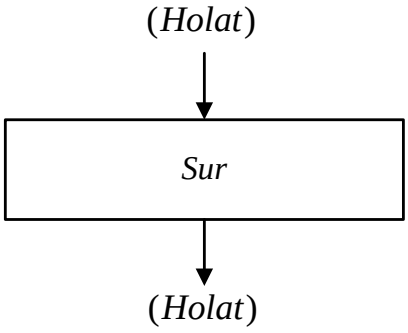
5. *ShaklBosqichKalit (k_{se})* almashtirishi



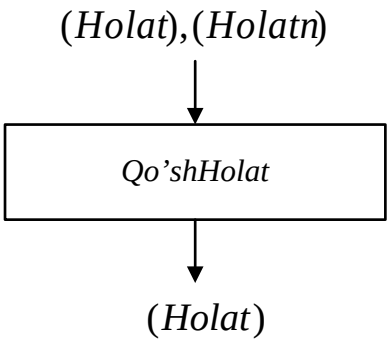
6. *Qo'shBosqichKalit (Holat, K_e)* almashtirishi



7. *Sur (Holat)* almashtirishi



8. *Qo'shHolat(Holatn, Holat)* almashtirishi



MShA belgilab qo‘yilgan ikki xil - *256* va *512* bit uzunlikdagi kalitlar yordamida amalga oshiriladi. Birinchi holatda, shifrlash kriptografik moduliga *256* bitli kalit kiritiladi. Bu kalit to‘laligicha shifrlash kaliti *k* sifatida olinadi, dastlabki seansning k_f funksional kaliti esa, shifrlash kalitining xesh-funksiyasi qiymati sifatida hisoblab topiladi.

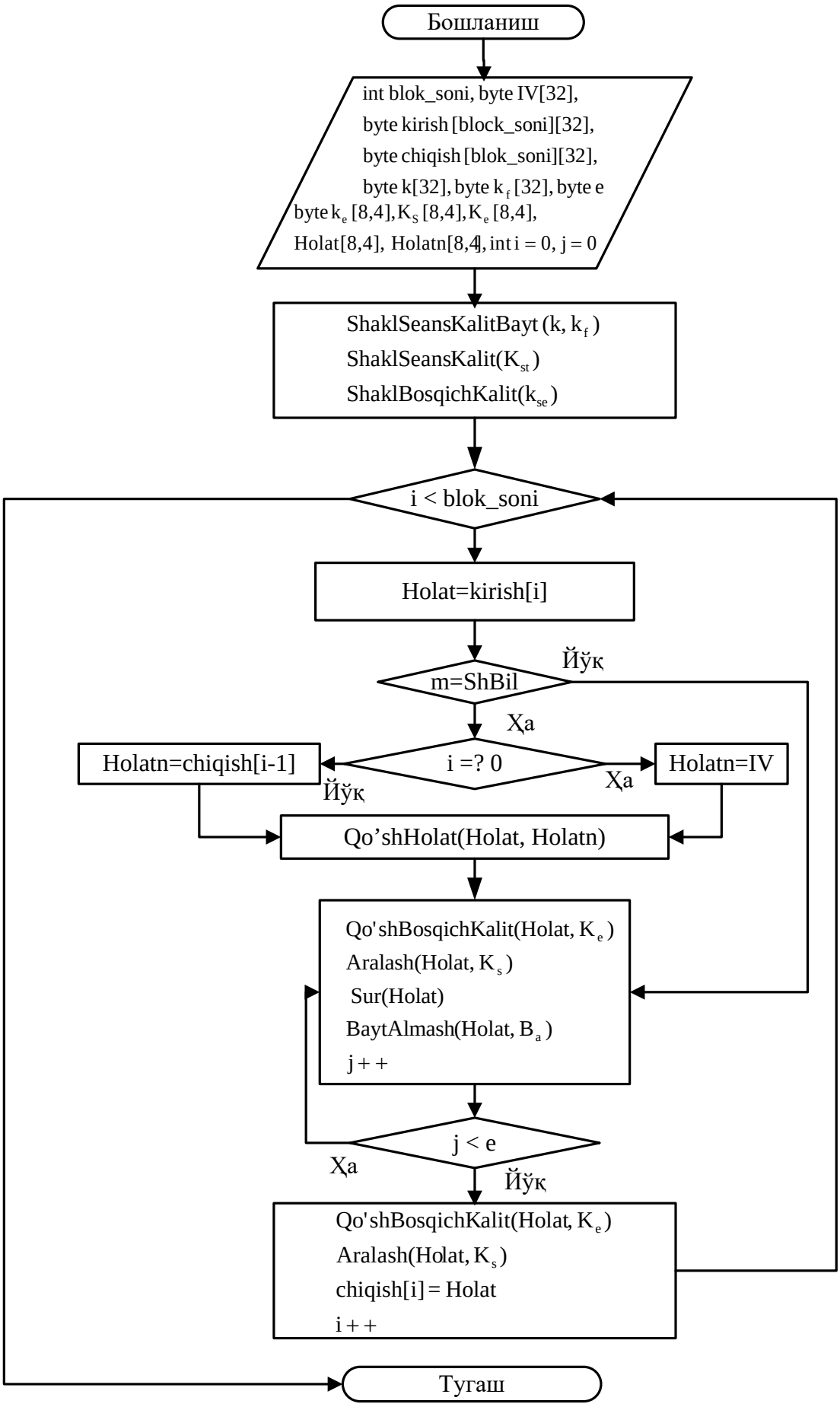
Ikkinchi holatda, shifrlash kriptografik moduliga *512* bitli kalit kiritiladi. Bu kalitning *256* bitli birinchi yarmi, shifrlash kaliti *k* sifatida olinadi, uning *256* bitli ikkinchi yarmi birinchi seansning funksional kaliti k_f sifatida olinadi.

Uchinchi holatda, shifrlash kriptografik moduliga hech qanday yangi kalit kiritilmaydi. Shifrlash kaliti *k* sifatida oldinngi seansda ishlatilgan shifrlash kaliti olinadi, funksional kalit k_f sifatida esa oldingi seansda ishlatilgan funksional kalit k_{f-1} ning shifrlash kaliti *k* dan foydlanib xeshlangan qiymati olinadi.

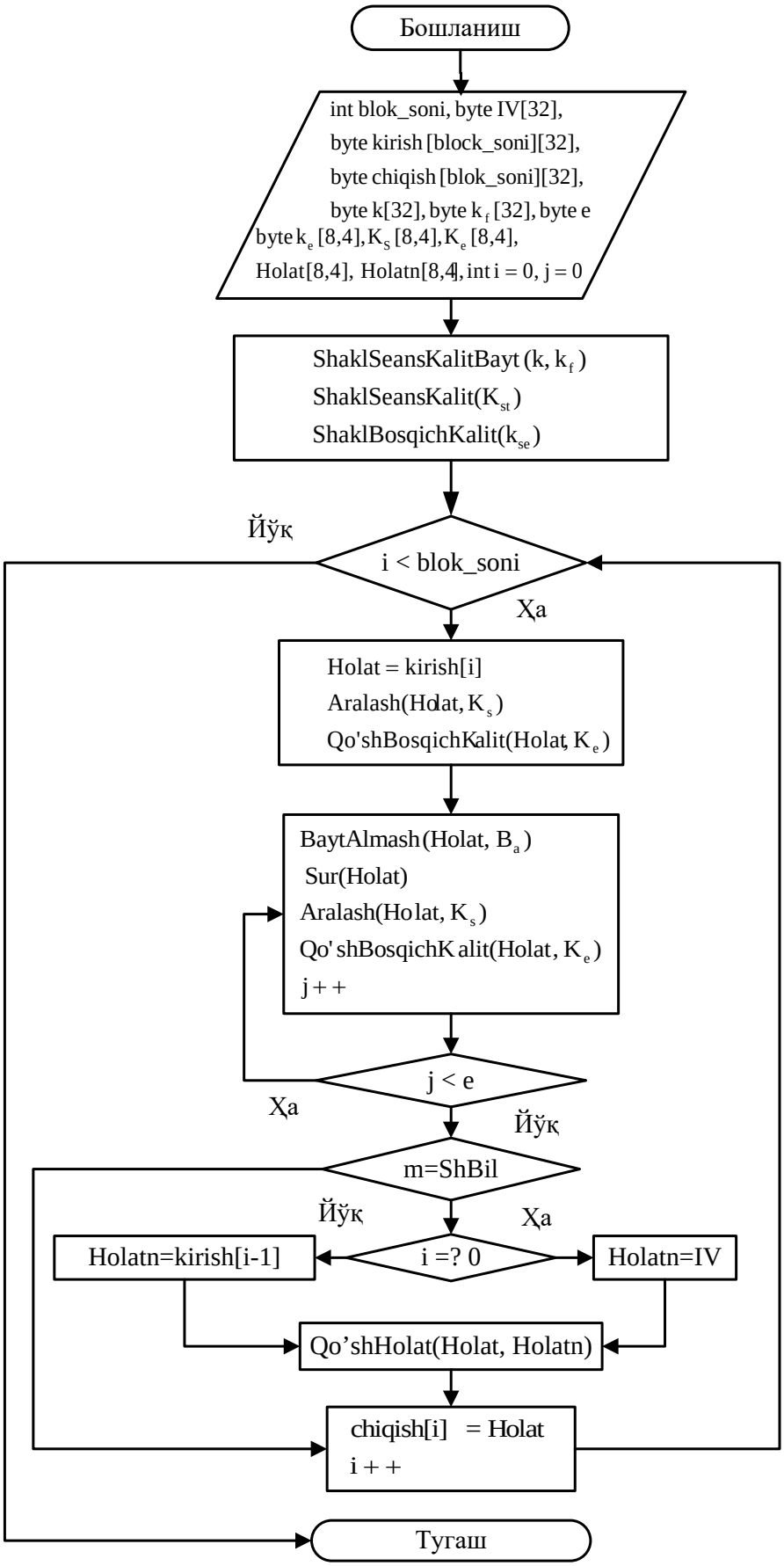
MShA standartidan xalqaro standartlarda qabul qilingan barcha blokli shifr rejimlarida foydalanish mumkin. Quyida MShA uchun ikkita tayanch ish rejimini bayon etish bilan cheklanilgan:

- elektron kod kitobi (*Elektron kod kitobi*);
- shifr bloklarini ilaktirish (*ShifrBloklarni ilaktirish, ShBil*).

Keltirilgan almashtirishlardan foydalangan holda MShAning shifrlash va deshifrlash ketma-ketliklarining blok-sxemalari mos ravishda 2.1 va 2.2 – rasmlarda keltirilgan.



2.1.1-rasm. MShning shifrlash ketma-ketligining blok - sxemasi



2.1.2-rasm. MShning deshifrlash ketma-ketligining blok - sxemasi

2.2. O‘z DSt 1106:2009 - xesh – funksiya

Mazkur standart axborotni qayta ishlash va muhofaza qilishning kriptografik metodlarida, shu jumladan avtomatlashtirilgan tizimlarda axborot uzatish, qayta ishlash va saqlashda elektron raqamli imzo protseduralarini amalga oshirish uchun qo‘llaniladigan ikkilik simvollarining istalgan ketma-ketligi uchun xeshlash funksiyasining (XF) algoritmini va hisoblash protsedurasini belgilaydi [6].

Ushbu standart GOST 28147-89 (Sistemы obrabotki informatsii. Zaщita kriptograficheskaya. Algoritmы kriptograficheskogo preobrazovaniya), O‘z DSt 1047:2003 (Axborot texnologiyalari. Atamalar va ta’riflar) va O‘z DSt 1109:2006 (Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta’riflar) standartlaridan foydalanilgan holda ishlab chiqilgan.

XFda kirish ketma-ketligining uzunligi 128 yoki 256 bitga karralidir, chiqish ketma-ketligi va xeshlash kaliti qayd etilgan 128 yoki 256 bit uzunlikka ega. Ushbu standartda kirish, chiqish va xeshlash kalitining boshqa uzunliklariga yo‘l qo‘yilmaydi.

Ushbu standart o‘zida 2 ta algoritmni mujassamlashtirgan bo‘lib, birinchi algoritm parametrli algebga muammosiga asoslangan bo‘lsa, ikkinchi algoritm GOST 28147-89 blokli shifrlash algoritmiga asoslangan. Ushbu standartda quyidagi belgilanishlar va sozlanmalar mavjud:

O‘z DSt 1106:2009 – birinchi algoritm. Ushbu algoritmning tavsifi quyida keltirilgan. Birinchi algoritm uchun quyidagi belgilanishlar qabul qilingan [6]:

M - dastlabki ma’lumotlar (xabar);

h - xesh-funksiya;

m - xesh-funksiya qiymati, bunda $m = h(M)$;

k - xeshlash kaliti;

k_e - *4x8* tartibli ikki o‘lchamli massiv ko‘rinishidagi bosqich kaliti;

holat - *4x8* tartibli ikki o‘lchamli massiv ko‘rinishidagi xeshlashning oraliq natijasi;

holatn - *4x8* tartibli ikki o‘lchamli massiv ko‘rinishidagi kirish bloki;

r - modul, bunda $p \in \{16, 256\}$;

ye - xeshlash protsedurasining bosqichlar soni;

b - dastlabki ma’lumotlardagi bloklar soni;

⊕ - *XOR* amalining simvoli (2-modul bo‘yicha qo‘shish amallari);

⊗ - diamatritsalarni *r* moduli bo‘yicha ko‘paytirish amalining simvoli;

® - parametr bilan *r* moduli bo‘yicha ko‘paytirish amalining simvoli;

$^{-1}$ - *r* moduli bo‘yicha teskarilash amalining simvoli;

$\backslash^{-1}$ – parametr bilan *r* moduli bo‘yicha teskarilash amalining simvoli;

$\backslash^{x}$ - parametr bilan *r* moduli bo‘yicha *x*-darajaga ko‘tarish amalining simvoli;

XF - xeshlash funksiyasi;

NY - nazorat summasi;

|| - konkatenatsiya simvoli.

XFda quyidagi parametr va funksiyalar foydalaniladi:

a) *k* – yarim bayt (bayt) darajasidagi chiziqli massivi ko‘rinishidagi *128* yoki *256* bit uzunlikdagi xeshlash kaliti;

b) k_e - *4x8* tartibdagi ikki o‘lchamli massiv ko‘rinishidagi bosqich (raund) kaliti;

s) *b* – dastlabki ma’lumotlardagi bloklar soni;

d) *uzunlik* – dastlabki ma’lumotlarning bitlardagi uzunligini o‘z ichiga oluvchi xeshlash funksiyasiga kiruvchi ma’lumotlarning oxirgidan oldingi bloki;

ye) *NY* - o‘nlik sanoq tizimida dastlabki ma’lumotlar qiymatlari summasini o‘z ichiga oluvchi xeshlash funksiyasiga kiruvchi ma’lumotlarning oxirgi bloki;

f) *r* - modul, $r \in \{16,256\}$;

g) ye_0 - *128* va *(256)* bitli kirish bloklari uchun *(b +2)10* ga teng bo‘lgan xeshlash protsedurasi bosqichlarining umumiy soni;

h) *Qo’sh (holat, holatn)* - *holat* massivi va *holatn* massivi joriy qiymatlarining yarim bayt (bayt) darajasidagi elementlari ustida *p* moduli

bo‘yicha *(A, B, R)* parametri bilan darajaga ko‘tarish amali asosida xeshlash protsedurasida foydalaniladigan o‘zgartirish;

i) *BaytZichlash (holat, holatn)* - *holat* massivi va *holatn* massivi joriy qiymatlarining yarim bayt (bayt) darajasidagi elementlari ustida, agar modul *p=16* bo‘lsa, *XOR* amalidan foydalanilgan holda yoki agar modul *p=256* bo‘lsa, bitta massivga zichlash chiziqli massivi asosida xeshlash protsedurasida foydalaniladigan o‘zgartirish;

j) *Aralash(holat, k_e)* – diamatritsalarni ko‘paytirish amali asosida xeshlash protsedurasida foydalaniladigan o‘zgartirish. Bu yerda ko‘paytiriladigan diamatritsalar, mos ravishda, *holat* va k_e bosqich kaliti ikki o‘lchamli massivlarining kvadrat shaklidagi chap va o‘ng yarimlariga o‘zaro mos keladi;

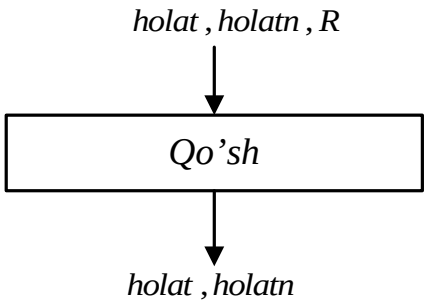
k) *SurHolat(holat)* - *holat* massivi ustida amalga oshiriladigan, xeshlash protsedurasida foydalaniladigan o‘zgartirish, bu *holat* massivining barcha to‘rtta satrini gorizontal va vertikal bo‘yicha surilishlarning turli qiymatlariga davriy surishlardan iborat;

l) *SurKalit(k_e)* - k_e massivi ustida amalga oshiriladigan xeshlash protsedurasida foydalaniladigan o‘zgartirish, bu k_e massivining barcha to‘rtta satrini gorizontal va vertikal bo‘yicha surilishlarning turli qiymatlariga davriy surishlardan iborat;

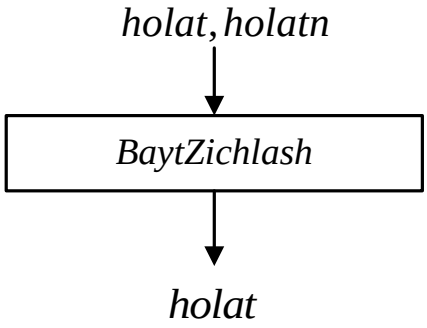
m) *TuzilmaKalit(k_e, k)* - xeshlash protsedurasining har bir bosqichi so‘ngida foydalaniladigan o‘zgartirish, bu uning strukturasini dastlabki xeshlash kaliti *k* strukturasiga keltirish maqsadida k_e massivining har bir yarim bayti (bayti) ustida amalga oshiriladi; ushbu o‘zgartirish natijasi k_e massivining kvadrat qismlaridan har birini teskarilash shartlarini qanoatlantiradi.

Keltirilgan almashtirishlarning umumiy ko‘rinishi quyidagicha bo‘lib, ularning to‘liq tavsifi [6]da keltirilgan:

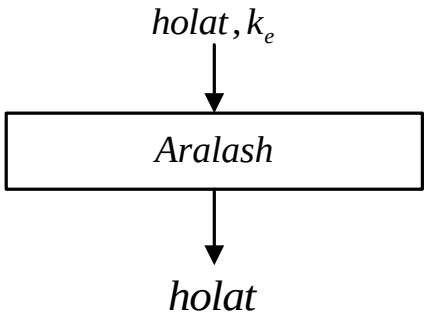
1. Qo’sh(holat, holatn, R) o‘zgartirish



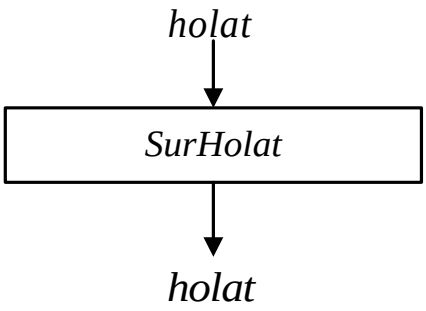
2. *BaytZichlash(holat, holatn)* o‘zgartirishi



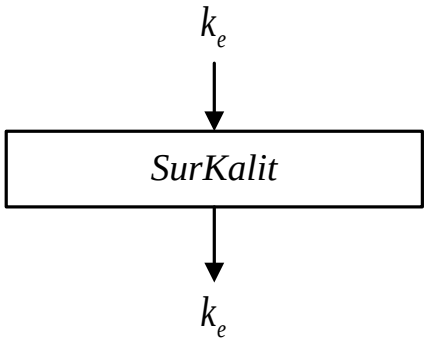
3. *Aralash(holat, k_e) o‘zgartirishi*



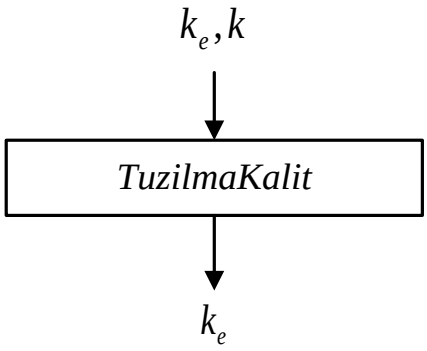
4. *SurHolat(holat) o‘zgartirishi*



5. *SurKalit(k_e) o‘zgartirishi*



6. TuzilmaKalit(k_e,k) o‘zgartirishi



Keltirilgan akslantirishlar asosida O‘z DSt 1106:2009 standartining birinchi algoritmining blok sxemasi 2.3-rasmda keltirilgan.

O‘z DSt 1106:2009 – ikkinchi algoritm. Ushbu algoritmning tavsifi quyida keltirilgan. Ikkinchi algoritm uchun quyidagi belgilanishlar qabul qilingan [6]:

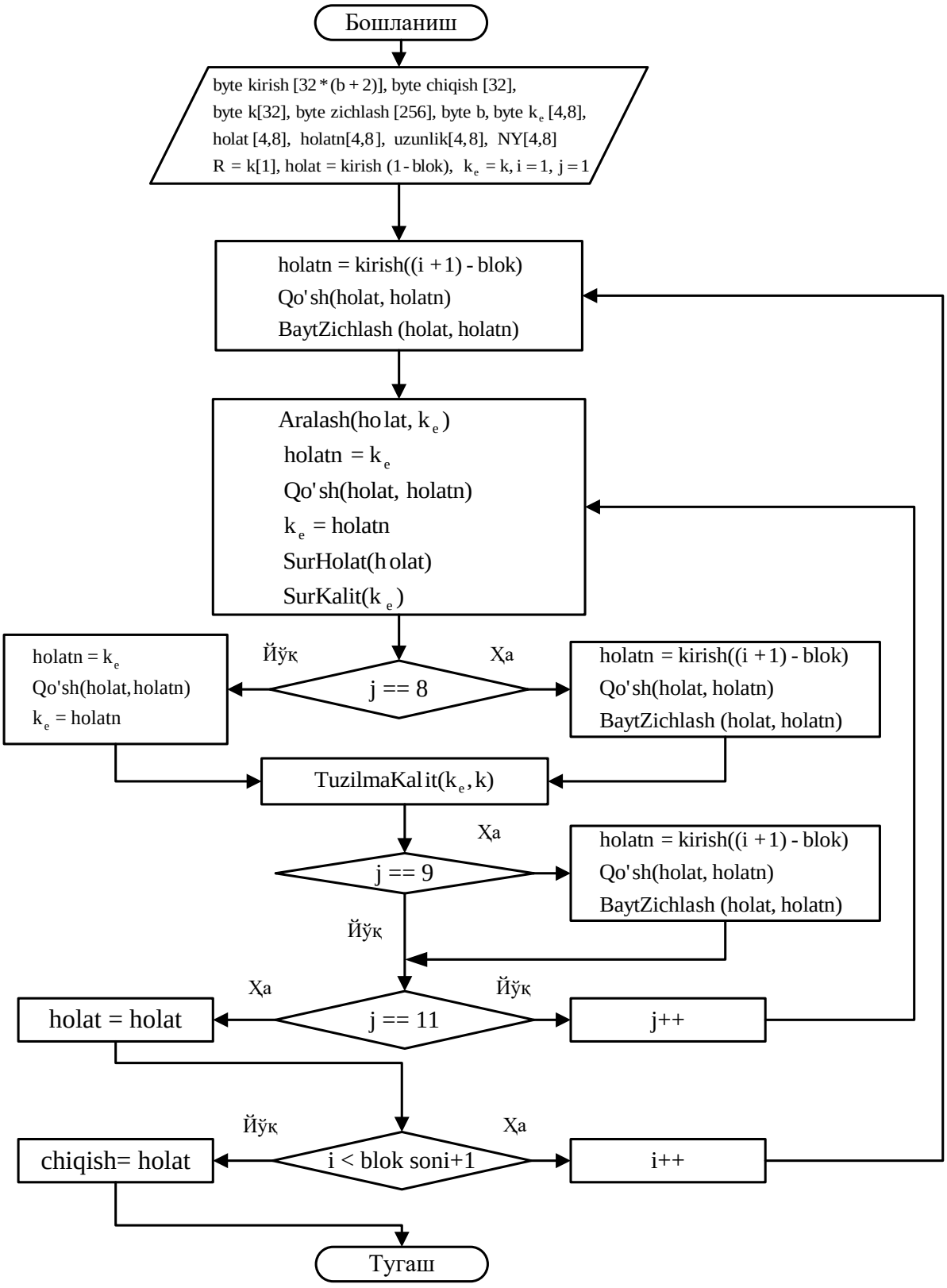
*V** - B={0,1} alifbodagi barcha chekli so‘zlar to‘plami. So‘zlarning o‘qilishi va alifbo belgilari (simvollari)ning raqamlanishi o‘ng tomondan chapga qarab amalga oshiriladi (so‘zning o‘ng tomonidagi simvol raqami birga teng, o‘ngdan ikkinchisiniki – ikkiga teng va h.k.);

$|A|$ - so‘z uzunligi $A \in B^*$;

$V_k(2)$ - *k* uzunlikdagi barcha binar so‘zlar to‘plami;

$A||B$ - $A, B \in B^*$ so‘zlarining konkatenatsiyasi - $|A|+|B|$ uzunlikdagi so‘z, bunda chap $|A|$ simvollar *A* so‘zini shakllantiradi, o‘ng $|B|$ simvollar esa, *B* so‘zini shakllantiradi. Shuningdek $A||B = AB$ belgidan ham foydalanish mumkin;

A^k - A ($A \in B^*$) so‘zining *k* nusxalari konkatenatsiyasi;



2.2.1-rasm. O‘z DSt 1106:2009 standarti 1-algoritmining blok-sxemasi

$\langle N \rangle_k$ - N butun manfiy bo‘lmagan soni $N \ (mod \ 2^k)$ chegirmasining ikkilik ifodasini o‘z ichiga oluvchi k uzunlikdagi so‘z;

$\hat{A}$ - A ($A \in B^*$) ikkilik ifodaga ega bo‘lgan, manfiy bo‘lmagan butun son;

$\oplus$ - *XOR* amalining simvoli (2 moduli bo‘yicha qo‘shish amali);

$\oplus'$ - $A \oplus' B = < \hat{A} + \hat{B} >_k$, ($k = |A| = |B|$) qoidasi bo‘yicha qo‘shish;

M - dastlabki ma’lumotlar (xabar);

h - $M \in B^*$ ketma-ketlikni $h(M) \in V_{256}$ (2) so‘ziga aks ettiruvchi xesh-funksiya;

h(M) - xesh-qiymat;

$E_k(A)$ - *A* so‘zini oddiy ($K \in V_{256}$ (2), $A \in V_{64}$ (2)) almashtirish rejimida GOST 28147 bo‘yicha shifrlash algoritmidan foydalangan holda *K* kalitida shifrlash natijasi;

H - boshlang‘ich xeshlash vektori;

e: = g - *e* parametrga *g* qiymatni biriktirish.

Xeshlash qadam funksiyasini hisoblashning 2-algoritmi ketma-ket amalga oshiriluvchi uchta qismini o‘z ichiga oladi:

- kalitlarni generatsiya qilish – *256* bit uzunlikdagi so‘zlarni;
- shifrlovchi o‘zgartirish - oddiy almashtirish rejimida GOST 28147 bo‘yicha algoritmdan foydalanib, K_i ($i=1,2,3,4$) kalitlarda *H* so‘zining 64-bitli so‘z qismlarini shifrlash;
- shifrlash natijasini aralashtiruvchi o‘zgartirish.

Kalitlarni generatsiya qilish

$X = (b_{256}, b_{255}, \ldots, b_1) \in V_{256}$ (2) vektor berilgan.

Faraz qilinsin $X = x_4 || x_3 || x_2 || x_1 = \eta_{16} || \eta_{15} || \ldots || \eta_1 = \xi_{32} || \xi_{31} || \ldots || \xi_1$ bo‘lsin,

bu yerda: $x_i = (b_{ix64}, \ldots, b_{(i-1)x64+1}) \in V_{64}(2), i = \overline{1,4}$;

$\eta_j = (b_{jx16}, \ldots, b_{(j-1)x16+1}) \in V_{16}(2), j = \overline{1,16}$;

$\xi_k = (b_{kx8}, \ldots, b_{(k-1)x8+1}) \in V_8(2), k = \overline{1,32}$.

$A(X) = (x_1 \oplus x_2) || x_4 || x_3 || x_2$ deb belgilansin.

$\xi_{32} || \ldots || \xi_1$ so‘zini $\xi_{\varphi(32)} || \ldots || \xi_{\varphi(1)}$ so‘ziga aks ettirish uchun P: V_{256} (2)$\rightarrow V_{256}$ (2) o‘zgartirishdan foydalaniladi, bu yerda, $\varphi(i+1+4(k-1)) = 8i+k$, $i = 0 \div 3$, $k = 1 \div 8$.

Kalitlarni generatsiya qilish uchun quyida keltirilgan dastlabki ma’lumotlardan foydalanish lozim:

- $H, M \in V_{256}(2)$ so‘zlari;

- parametrlari: $S_2=S_4=0^{256}$ va $S_3=1^80^81^{16}0^{24}1^{16}0^8(0^81^8)^21^80^8(0^81^8)^4\,(1^80^8)^4$ qiymatlarga ega bo‘lgan $C_i\,(i=2,3,4)$ so‘zlar.

Kalitlarni hisoblash jarayonida quyidagi algoritm amalga oshiriladi:

1) qiymatlar berilsin:

$i:=1, U:=H, V:=M;$

2) hisoblash bajarilsin:

$W=U \oplus V, \quad K_1 = P(W);$

3) $i:=i+1$ berilsin;

4) $i=5$ sharti tekshirilsin;

Shart bajarilsa, 7-qadamga o‘tilsin. Bajarilmagan holda 5-qadamga o‘tilsin;

5) hisoblash bajarilsin:

$U:=A(U) \oplus S_i, V:=A(A(V)), W:=U \oplus V, K_i = R(W)$.

6) 3-qadamga o‘tilsin;

7) algoritm ishi tugatilsin.

Shifrlovchi o‘zgartirish

Ushbu bosqichda $K_i\,(i=1,2,3,4)$ kalitlarda H so‘zining 64-bitli so‘z qismlarini shifrlash amalga oshiriladi.

Shifrlovchi o‘zgartirish uchun quyidagi dastlabki ma’lumotlardan foydalanish zarur:

- $\boldsymbol{H = h_4 \| h_3 \| h_2 \| h_1, h_i \in V_{64}(2), i = \overline{1,4}}$;

- K_1, K_2, K_3, K_4 kalitlar to‘plami..

Shifrlash algoritmi amalga oshiriladi va

$$s_i=E_K(h_i),\ (i=1,2,3,4)$$

so‘zlar olinadi.

Ushbu bosqich natijasida $S=s_4||s_3||s_2||s_1$ ketma-ketlik hosil qilinadi.

Aralashtiruvchi o‘zgartirish

Ushbu bosqichda siljitish registrini qo‘llagan holda olingan ketma-ketlikni aralashtirish amalga oshiriladi.

Dastlabki ma’lumotlar quyidagilar:

- $H, M \in V_{256}(2)$ so‘zlari;

- $S \in V_{256}(2)$ so‘zi.

Faraz qilinsin, $\psi: \in V_{256}(2) \dashrightarrow V_{256}(2)$ akslantirish

$\eta_{16} \| \eta_{15} \| ... \| \eta_1, \eta_i \in V_{16}(2), i = \overline{1,16}$; so‘zini

$$\eta_1 \oplus \eta_2 \oplus \eta_3 \oplus \eta_4 \oplus \eta_{13} \oplus \eta_{16} || \eta_{16} || \eta_{15} || \ldots || \eta_2.$$

so‘ziga o‘zgartirsin.

U holda xeshlash qadam funksiyasi qiymati sifatida

$$x(M, H) = \psi^{61}(H \oplus \psi(M \oplus \psi^{12}(S)))),$$

so‘zi qabul qilinadi, bu yerda,: ψ^i - ψ funksiyasining i- darajasi.

Xesh-funksiyani hisoblash protsedurasi

Xeshlanishi lozim bo‘lgan $M \in B^*$ ketma-ketlik h xeshlash funksiyasi qiymatini hisoblash protsedurasi uchun dastlabki ma’lumotlar hisoblanadi. $V_{256}(2)$ to‘plamda aniqlangan ixtiyoriy qayd qilingan H - boshlang‘ich xeshlash vektori parametr hisoblanadi.

h funksiyani hisoblash protsedurasi har bir iteratsiyada quyidagi kattaliklardan foydalanadi:

$M \in B^*$ - oldingi iteratsiyalarda xeshlash protsedurasidan o‘tmagan M ketma-ketlik qismi;

$H \in V_{256}(2)$ - xesh-funksiyaning joriy qiymati;

$\Sigma \in V_{256}(2)$ - nazorat summasining joriy qiymati;

$L \in V_{256}(2)$ - M ketma-ketlikning oldingi iteratsiyalarida qayta ishlangan qismi uzunligining joriy qiymati.

h funksiyani hisoblash algoritmi quyidagi bosqichlarni o‘z ichiga oladi:

1-bosqich

Joriy kattaliklarning dastlabki qiymatlari berilsin

1.1 $M:=M$

1.2 $H:=H$

1.3 $\Sigma:=0^{256}$

1.4 $L:=0^{256}$

1.5 2-bosqichga o‘tish.

2-bosqich

2.1 $|M|>256$ sharti tekshirilsin. Shart bajarilsa, 3-bosqichga o‘tilsin, aks holda quyidagi hisoblashlar ketma-ketligi bajarilsin:

2.2 $L:=\langle L+|\mathrm{M}|\rangle_{256}$

2.3 $M':=0^{256-|\mathrm{M}|}||M$

2.4 $\Sigma:=\Sigma\oplus' M'$

2.5 $H:=x(M',H)$

2.6 $H:=x(L,H)$

2.7 $H:=x(\Sigma,H)$

2.8 Algoritm ishi tugatilsin.

3-bosqich

3.1 $M(M=M_p||M_s)$ so‘zining $M_s \in V_{256}$ (2) so‘z qismi hisoblansin. So‘ngra quyidagi hisoblashlar ketma-ketligi bajarilsin:

3.2 $H:=x(M_s, H)$

3.3 $L:=\langle L+256\rangle_{256}$

3.4 $\Sigma:=\Sigma\oplus' M_s$

3.5 $M:=M_p$

3.6 2-bosqichga o‘tilsin.

2.7-qadamda hosil qilingan H kattalikning qiymati $h(M)$ xeshlash funksiyasining qiymati hisoblanadi.

2.3. O‘z DSt 1092:2009 va O‘z DSt 2826:2014 - elektron raqamli imzoni shakllantirish va tekshirish standartlari

Ushbu bo‘limda elektron raqamli imzo algoritmlari bilan tanishib o‘tiladi. ERI bo‘yicha respublikamizda ikkita standart mavjud bo‘lib, ular quyidagilar:

- O‘z DSt 1092:2009;
- O‘z DSt 2826:2014.

O‘z DSt 1092:2009 standarti. Ushbu standart «UNICON.UZ» - Fan-texnika va marketing tadqiqotlari markazi davlat unitar korxonasi («UNICON.UZ» DUK) tomonidan ishlab chiqilgan va kiritilgan hamda uni ishlab chiqishda O‘zbekiston Respublikasining «Elektron raqamli imzo to‘g‘risida»gi va «Elektron hujjat almashuvi to‘g‘risida»gi qonunlarining normalariga amal qilingan [5].

Ushbu stantda quyidagi asosiy atamalardan foydalanilgan:

– *maxsus shaxsiy kalit (specific rrivate key)*: Ochiq bo‘lmagan va faqat vakolatli sub’ekt bilan bog‘liq bo‘lgan asimmetrik va simmetrik kriptografik algoritmlarda foydalaniladigan kriptografik kalit (masalan, parametrlar uchligi (R, g, k_h), bunda R – daraja parametri, g – asos, k_h – xeshlash kaliti).

– *daraja parametri muammosi (problem of power parameter*): Agar parametrli gruppa $(F_p; ®)$ da gruppa tashuvchisi F_p ning g va y elementlari berilgan bo‘lsa, R parametr va daraja ko‘rsatkichi x ni toping; bu yerda $y \equiv g^{\backslash x}$ $(\mathrm{mod}\ r)$ p moduli bo‘yicha R parametr bilan g ning x-darajasini ifodalaydi, bunda p – tub son, $R < p$.

Mazkur standart ham ikkita algoritmdan iborat bo‘lib, ular mos holda birinchi algoritm va ikkinchi algoritm deb yuritiladi. Ularda foydalanilgan umumiy belgilinishlar quyidagilar:

M – ixtiyoriy chekli uzunlikdagi ikkilik kodi bilan aks ettirilgan foydalanuvchining xabari;

r – tub son, $r > 3$;

q – tub son;

R – natural son - parametr;

(x, u) – butun sonlar juftligi – ERI yopiq kaliti;

(y, z) – butun sonlar juftligi – ERI ochiq kaliti;

g – natural son – asos;

(r, s) – butun sonlar juftligi – M xabar ostidagi elektron raqamli imzo;

(R_1, y_1) – butun sonlar juftligi – nazorat kaliti va ochiq seans kaliti juftligidan tarkib topgan ERI qalbakiligini aniqlash kaliti;

(R, g, k_h) – vakolatlangan sub'ektning maxsus shaxsiy kaliti;

k_h – xeshlash kaliti;

® – modul bo'yicha sonlarni R parametr bilan ko'paytirish amalining simvoli;

$\backslash^{e}$ – modul bo'yicha ye darajaga parametr bilan ko'tarish amalining simvoli;

$\backslash^{-1}$ – modul bo'yicha parametr bilan teskarilash amalining simvoli;

$^{-1}$ – modul bo'yicha teskarilash amalining simvoli;

"+"– elliptik egri chiziq nuqtalari gruppasida qo'shish amalining simvoli;

[k] – elliptik egri chiziq nuqtalari gruppasida k marta qo'shishni bajarish amali simvoli;

F_r – r ta $\{0,1,\ldots, r-1\}$ butun sonlar to'plamidan iborat chekli tub maydon;

b (mod r) – b bilan r modul bo'yicha taqqoslanuvchi, eng kichik musbat son;

a, b – elliptik egri chiziq koeffitsientlari;

w – elliptik egri chiziq nuqtalari gruppasi tartibi;

t – elliptik egri chiziq nuqtalari gruppasi qism gruppasining tartibi;

0 – elliptik egri chiziqning nol nuqtasi;

N – elliptik egri chiziqning t tartibli nuqtasi;

d – butun son – ERI yopiq kaliti;

T – elliptik egri chiziq nuqtasi, ERIning ochiq kaliti;

RM – ro‘yxatga olish markazi;

OK – ochiq kalit.

Har ikkala algoritmlar ham quyidagi 3 ta jarayondan iborat:

- ERI kalitlarini generatsiyalash;
- ERIni shakllantirish;
- ERIni tekshirish (haqiqiyligini tasdiqlash).

Mazkur standartdagi birinchi algoritm ikki rejimni (seans kalitili va seans kalitisiz) qo‘llab quvvatlab, parametrli darajaga ko‘tarish muammosiga asoslangan. Ikkinchi algoritm esa diskret maydonda elliptik egri chiziqlarda nuqtalarni qo‘shish va ko‘paytirishga asoslangan.

Birinchi algoritm doirasida quyidagi parametrlardan foydalanilgan:

a) p – modul, tub son. Bu sonning yuqori chegarasi elektron raqamli imzo algoritmi muayyan amalga oshirilganda kriptografik modulning tipiga bog‘liq holda aniqlanishi kerak: $p > 2^{255}$ maxsus apparat tipi uchun, $p > 2^{1023}$ dasturiy, gibrid va apparat tipidagilar uchun.

b) q – p-1 ning faktori (tub ko‘paytuvchisi) bo‘lgan tub son, bu yerda $2^{254} < q < 2^{256}$.

s) R – parametr, $R < q$ shartni qanoatlantiruvchi natural son; R parametri foydalanuvchilarning cheklangan guruhi uchun ochiq, birgalikdagi maxfiy kalit yoki vakolatlangan sub’ektning maxsus shaxsiy kalitining tashkil etuvchisi bo‘lishi mumkin;

d) $m = H(M)$ – M xabarni 256 bit uzunlikdagi qatorda aks ettiruvchi xesh-funksiya; kriptografik modulning dasturiy, gibrid va apparat tiplarida kalitsiz xesh-funksiya, maxsus apparat tipida esa kalitli xesh-funksiyadan foydalaniladi.

Birinchi algoritmning har bir foydalanuvchisi quyidagi shaxsiy kalitlarga ega bo‘lishi kerak:

a) (x, u) – butun sonlar juftligi – ERI yopiq kaliti,

bu yerda: x, u – yopiq kalitlar, $1<x$, $u<q$ shartlarni qanoatlantiruvchi tasodifiy yoki psevdotasodifiy generatsiyalangan butun sonlar;

b) g – yopiq yoki ochiq parametr, $g \equiv h^{\backslash(r-1)/q}$ $(\mathrm{mod}\ p)$ yordamida hisoblanadigan butun son;

bu yerda: $h < p$ – natural son bo‘lib, ωning $1 \div q$ qiymatlar diapozonida faqat $\omega=q$ bo‘lgandagina $g^{\backslash\omega}$ $(\mathrm{mod}\ p) \equiv 0$ shartni qanoatlantiradi;

s) (y, z) – butun sonlar juftligi – ERI ochiq kaliti,

bu yerda: y, z – ochiq kalitlar, $y \equiv g^{\backslash x}$ $(\mathrm{mod}\ p)$ va $z \equiv g^{\backslash u}$ $(\mathrm{mod}\ p)$ ifodalar yordamida hisoblanadi; agar ochiq parametr (asos) g dan foydalanilsa, unda $u=1$ va $z=g$;

d) (R_1, y_1) – butun sonlar juftligi – ERI qalbakiligini aniqlash kaliti (faqat seans kalitli rejimda);

bu yerda: R_1 – nazorat kaliti (ochiq yoki yopiq), $1 \div q\text{-}1$ diapozondan tanlab olingan; agar R_1 yopiq bo‘lsa, unda R_1 imzolovchi shaxs va tekshiruvchi tomon uchun birgalikdagi maxfiy kalit bo‘lishi kerak;

y_1 – seans (ochiq) kaliti, har bir elektron raqamli imzo uchun parametr bilan darajaga ko‘tarish natijasi kabi hisoblanadi.

Foydalanuvchilar guruhi uchun p, q tub sonlari ochiq va umumiy bo‘lishi mumkin.

Ikkinchi algoritmda esa quyidagi parametrlardan foydalanilgan:

a) r tub son – $r > 2^{255}$ tengsizlikni qanoatlantiruvchi, elliptik egri chiziq moduli. Ushbu sonning yuqori chegarasi ERIni muayyan amalga oshirish jarayonida belgilanadi;

b) o‘zining $J(E)$ invarianti yoki a, $b \in F_r$ koeffitsientlari bilan berilgan E elliptik egri chiziq;

d) w butun son - E elliptik egri chiziq nuqtalari gruppasining tartibi;

e) t tub son - quyidagi shartlar bajarilgan E elliptik egri chiziq nuqtalari gruppasi siklik qism gruppasining tartibi:

$$\begin{cases} w = lt, l \in Z, l \geq 1 \\ 2^{254} < t < 2^{256} \end{cases}$$

f) (x_r, y_r) koordinatali va $[t]N=0$ tenglikni qanoatlantiruvchi E elliptik egri chiziqning $N \neq 0$ nuqtasi;

g) $m = H(M)$ – M xabarni 256 bit uzunlikdagi qatorda aks ettiruvchi xesh-funksiya.

Yuqorida keltirilgan ERIA parametrlariga quyidagi talablar qo‘yiladi:

- barcha butun $i=1,2\ldots, B$ sonlar uchun $r^i \neq 1 \pmod t$ shart bajarilishi lozim, bu yerda, V uchun $B \geq 31$ tengsizlikni qanoatlantiradi;

- $w \neq r$ tengsizlik bajarilishi lozim;

- egri chiziq invarianti $J(E) \neq 0$ yoki 1728 shartlarini qanoatlantirishi lozim.

Ikkinchi algoritmning har bir foydalanuvchisi quyidagi shaxsiy kalitlarga ega bo‘lishi kerak:

a) ERI yopiq kaliti d – $0<d<t$ tengsizlikni qanoatlantiruvchi butun son;

b) ERI ochiq kaliti T – (x_t, y_t) koordinatali, $[d]N=T$ tenglikni qanoatlantiruvchi elliptik egri chiziqning nuqtasi.

Yuqorida keltirilgan parametrlar mavjud bo‘lganda algoritmlarni amalga oshirish imkoniyati bo‘ladi. Birinchi algoritmda ERIni shakllantirish jarayoni quyidagicha:

M xabar ostiga qo‘yiladigan elektron raqamli imzo va seans kalitini yaratish uchun 1-algoritm bo‘yicha quyidagi amallarni (qadamlarni) bajarish zarur:

1-qadam: xabarning xesh-funksiyasini hisoblang: $m = H(M)$ va $c=x$ ni qabul qiling;

2-qadam: $k=H(m+(1+mR)c)$ ni hisoblang. Agar $k = 0$ bo‘lsa, unda $c = c + 2$ ni qabul qiling va 2–qadamga qayting;

3-qadam: R parametr bilan $T \equiv g^{\backslash -k} \pmod p$ ni hisoblang;

4-qadam: $r \equiv m + (1+ mR)T \pmod p$ ni hisoblang. Agar $r \pmod q = 0$ bo‘lsa, unda $k \equiv k+1 \pmod p$ ni qabul qiling va 3-qadamga qayting;

5-qadam: $s_1 \equiv k - rx \ (\text{mod } q)$ ni hisoblang. Agar $s_1 = 0$ bo‘lsa, unda $k \equiv k + 1 \ (\text{mod } p)$ ni qabul qiling va 3-qadamga qayting;

6-qadam: $s \equiv s_1 u^{-1} \ (\text{mod } q)$ ni hisoblang. Agar $\mu = 0$ bo‘lsa, unda r, s ni chiqishga bering va hisoblashni to‘xtating;

7-qadam: $r_1 \equiv R_1 + (1 + RR_1)r \ (\text{mod } q)$ ni hisoblang. Agar $r_1 = 0$ bo‘lsa, unda $k \equiv k + 1 \ (\text{mod } p)$ ni qabul qiling va 3-qadamga qayting;

8-qadam: $x_1 \equiv (k - suR_1)r_1^{-1} \ (\text{mod } q)$ ni hisoblang. Agar $x_1 = 0$ bo‘lsa, unda $k \equiv k + 1 \ (\text{mod } p)$ ni qabul qiling va 3-qadamga qayting;

9-qadam: RR_1 parametr bilan $y_1 \equiv (gR_1^{-1})^{\backslash x1} \ (\text{mod } p)$ ni hisoblang va r, s, y_1 larni chiqishga bering.

Bu jarayon uchun dastlabki (kirishdagi) ma’lumotlar bo‘lib rejim $\mu \in \{1, 0\}$, xabar M, ERIning yopiq kaliti (x, u), parametr g, nazorat kaliti R_1, modul r va q soni hisoblanadi. $\mu = 1$ rejimda chiqish natijasi bo‘lib (s, r, y_1) va k (ushbu standartga xos protokoldan foydalanilganda), rejim $\mu = 0$ uchun esa s, r hisoblanadi. Seans kalitli rejim uchun $\mu = 1$, seans kalitsiz rejim uchun esa $\mu = 0$ qabul qilinadi.

Bundan keyin imzolangan xabar (xabar va to‘ldiruvchi) qabul qiluvchi tomonga uzatiladi. Agar seans kalitli rejimdan foydalanilsa, u holda qabul qiluvchi tomonga ham seans kaliti uzatiladi.

Ikkala rejimda, odatda, ochiq kalitlar infratuzilmalarida (OKI) foydalaniladigan xabarlarni almashuvchi umumiy qabul qilingan protokollari qo‘llaniladi. Seans kalitli rejimdan foydalanilganda ushbu standartga xos protokoldan foydalanishga ruxsat beriladi.

Birinchi algoritm bo‘yicha ERIni tekshirish jarayoni esa quyidagi qadamlardan iborat:

Olingan M xabar ostiga qo‘yilgan ERIning haqiqiyligini tasdiqlash uchun birinchi algoritm bo‘yicha quyidagi amallarni (qadamlarni) bajarish zarur:

1–qadam: $m = H(M)$ xesh – funksiyani hisoblang;

2–qadam: agar $L(s) <= L(q)$ *AND* $L(r) <= L(p)$ bo‘lsa, unda keyingi qadamga o‘ting, aks holda «imzo haqiqiy emas» qabul qilinadi;

3–qadam: R parametr bilan $z_0 \equiv z^{\backslash s} \pmod{p}$ ni hisoblang;

4–qadam: $r' \equiv r \pmod{q}$ ni hisoblang;

5–qadam: R parametr bilan $y_2 \equiv y^{\backslash r'} \pmod{p}$ ni hisoblang;

6–qadam: $z_1 \equiv z_0 + (1 + z_0 R) y_2 \pmod{p}$ ni hisoblang;

7–qadam: $y_3 \equiv z_1 + (1 + z_1 R) r \pmod{p}$ ni hisoblang;

8–qadam: agar $\mu = 0$ va $m = y_3$ bo‘lsa, unda chiqishga “imzo haqiqiy” ni bering; agar $\mu = 1$ va $m = y_3$, unda keyingi qadamga o‘ting, agar $m \neq y_3$, unda «imzo haqiqiy emas» qabul qilinadi;

9–qadam: $g_3 \equiv z_1 R_1^{-1} \pmod{p}$ ni hisoblang;

10–qadam: $s_1 \equiv s R_1 \pmod{q}$ ni hisoblang;

11–qadam: $r_1 \equiv R_1 + r'(1 + R R_1) \pmod{q}$ ni hisoblang;

12–qadam: $z_2 \equiv z R_1^{-1} \pmod{p}$ ni hisoblang;

13–qadam: $y_4 \equiv y_1$ ni qabul qiling;

14–qadam: RR_1 parametr bilan $z_3 \equiv z_2^{\backslash s1} \pmod{p}$ ni hisoblang;

15–qadam: RR_1 parametr bilan $y_5 \equiv y_4^{\backslash r1} \pmod{p}$ ni hisoblang;

16–qadam: $g_4 \equiv z_3 + (1 + z_3 R R_1) y_5 \pmod{p}$ ni hisoblang;

17–qadam: agar $g_3 = g_4$, unda “imzo haqiqiy” qabul qilinadi, aks holda “imzo haqiqiy emas” qabul qilinadi.

Bu jarayon uchun dastlabki (kirishdagi) ma’lumotlar bo‘lib imzolangan M xabar, elektron raqamli imzo s, r, ochiq kalitlar y, z, nazorat kaliti R_1, seans kaliti y_1, modul p va q soni, chiqish natijasi bo‘lib esa, mazkur ERIning haqiqiyligi yoki haqiqiy emasligi haqidagi axborot hisoblanadi. ERI qalbakiligini aniqlash kaliti (R_1, y_1) faqat seans kalitli rejimda qo‘llaniladi.

Ikkinchi algoritm bo‘yicha ERIni hosil qilish uchun quyidagi ketma-ketliklardan foydalaniladi:

M xabar ostiga qo‘yiladigan ERIni olish uchun ikkinchi algoritm bo‘yicha quyidagi amallarni (qadamlarni) bajarish zarur:

1-qadam: xabarning xesh-funksiyasini hisoblang: $m=H(M)$;

2-qadam: $e \equiv m \pmod{t}$ ni hisoblang. Agar $ye=0$ bo‘lsa, u holda $ye=1$ ni aniqlang;

3-qadam: ushbu $0 < k < t$ tengsizlikni qanoatlantiruvchi tasodifiy (psevdotasodifiy) k butun sonini generatsiya qiling;

4-qadam: elliptik egri chiziqning $C=[k]N$ nuqtasini hisoblang va $r=x_s \pmod{t}$ ni aniqlang, bu yerda x_s – S nuqtaning x koordinatasi. Agar $r=0$ bo‘lsa, u holda 3-qadamga qayting;

5-qadam: $s \equiv (rd+ke) \pmod{t}$ ifodaning qiymatini hisoblang. Agar $s=0$ bo‘lsa, 3-qadamga qayting;

6-qadam: r va s larni ERI sifatida chiqishga bering.

Ushbu jarayon uchun dastlabki (kirishdagi) ma’lumotlar M xabar va ERIning yopiq kaliti d, chiqish natijasi bo‘lib esa, (r, s) elektron raqamli imzo hisoblanadi.

ERIni tekshirish jarayoni esa quyidagicha:

Olingan M xabar ostiga qo‘yilgan ERI haqiqiyligini tasdiqlash uchun ikkinchi algoritm bo‘yicha quyidagi amallarni (qadamlarni) bajarish zarur:

1-qadam: agar $0 < r < t$, $0 < s < t$ tengsizliklar bajarilsa, navbatdagi qadamga o‘ting, aks holda, “imzo haqiqiy emas” qabul qilinadi;

2-qadam: M xabar bo‘yicha xesh-funksiyani hisoblang: $m=H(M)$;

3-qadam: $e \equiv m \pmod{t}$ ni hisoblang. Agar $ye=0$ bo‘lsa, u holda $ye=1$ ni aniqlang;

4-qadam: $v \equiv e^{-1} \pmod{t}$ ifodaning qiymatini hisoblang;

5-qadam: ushbu $z_1 \equiv sv \pmod{t}$, $z_2 \equiv -rv \pmod{t}$ ifodalar qiymatlarini hisoblang;

6-qadam: elliptik egri chiziqning $C=[z_1]N$ “+” $[z_2]T$ nuqtasini hisoblang va $R \equiv x_s \pmod{t}$ ni aniqlang, bu yerda x_s - S nuqtaning x koordinatasi.

7-qadam: agar $R=r$ tenglik bajarilsa, u holda “imzo haqiqiy”, aks holda “imzo haqiqiy emas” qabul qilinsin.

Ushbu jarayon uchun dastlabki (kirishdagi) ma’lumotlar bo‘lib, imzolangan *M* xabar, *(r, s)* elektron raqamli imzo va ERI ochiq kaliti, chiqish natijasi bo‘lib esa, mazkur ERI haqiqiyligi yoki haqiqiy emasligi haqidagi axborot hisoblanadi.

O‘z DSt 2826:2014 standarti. Ushbu standartni ishlab chiqishda O‘z DSt 1092:2009, O‘z DSt 1106:2009, O‘z DSt 1109:2013 va O‘z DSt 1204:2009 standartlaridan foydalanilgan. Ushbu standart parametrli algebra va elliptik egri chiziq kombinatsiyasiga asoslangan bo‘lib, quyidagi belgilanishlardan foydalaniladi [9]:

M – ixtiyoriy chekli uzunlikdagi ikkilik kodi bilan taqdim etilgan foydalanuvchining xabari

r – tub son (elliptik egri chiziq xarakteristikasi)

R – natural son - parametr

F_r – *r* ta *{0,1,…, r-1}* butun sonlar to‘plamidan iborat chekli tub maydon

*b (*mod *r)* – *b* bilan *r* modul bo‘yicha taqqoslanuvchi, eng kichik musbat son

a, *b* – elliptik egri chiziq koeffitsientlari

V – parametrli elliptik egri chiziq koeffitsienti

w – parametrli elliptik egri chiziq nuqtalari gruppasi tartibi

q – parametrli elliptik egri chiziq nuqtalari qism gruppasining tartibi

0_E – parametrli elliptik egri chiziqning nol nuqtasi

G – parametrli elliptik egri chiziqning *q* tartibli nuqtasi

d – butun son – elektron raqamli imzoning (ERI) yopiq kaliti

Y – parametrli elliptik egri chiziq nuqtasi, ERI ochiq kaliti

S – boshlang‘ich qiymat, parametrli elliptik egri chiziq «tasodifiy tanlash» strategiyasi asosida generatsiya qilinganda tizim parametrlari tarkibiga kiritiladi

H – xesh-funksiya;

h – xesh–funksiya qiymati, bunda *h = H(.)*

l – butun son, kofaktor

D – domen (tizim parametrlari), foydalanuvchi tomonidan generatsiya va verifikatsiya qilinuvchi *(p*, parametrli elliptik egri chiziq, *a, b, G, q, l, H(.), S*).

(r, s) – butun sonlar juftligi – *M* xabar ostidagi ERI

® – modul bo‘yicha sonlarni *R* parametr bilan ko‘paytirish amalining simvoli

$\backslash^{-1}$ – modul bo‘yicha parametr bilan teskarilash amalining simvoli

$^{-1}$ – modul bo‘yicha teskarilash amalining simvoli

$+\backslash$ – parametrli elliptik egri chiziq nuqtalari gruppasida qo‘shish amalining simvoli

$[k]\cdot\backslash$ – parametrli elliptik egri chiziq nuqtalari gruppasida *k* marta qo‘shishni bajarish amali simvoli.

Ananaviy elliptik egri chiziqda asoslangan tengliklardan farqli ravishda nuqtalarni qo‘shishda quyidagi tengliklardan foydalanilgan.

T_1 va T_2 nuqtalar koordinatalari uchun $x_1 \neq x_2$ shart qanoatlantirilsin. U holda, bu nuqtalarning yig‘indisi deb, koordinatalari quyidagi taqqoslashlar bilan aniqlanuvchi $T_3(x_3, y_3)$ nuqtaga aytiladi:

$$\begin{cases} x_3 \equiv (L^2 - 3)R^{-1} - x_1 - x_2 \pmod p, \\ y_3 \equiv L(x_1 - x_3) + y_1^- \pmod p, \end{cases}$$

bu yerda, $L \equiv (y_2 - y_1)(x_2 - x_1)^{-1} \pmod p$.

Agar $x_1 = x_2$ va $y_1 = y_2 \neq 0$ tenglik bajarilsa, u holda T_3 nuqtaning koordinatalari quyidagicha aniqlanadi:

$$\begin{cases} x_3 \equiv (L^2 - 3)R^{-1} - 2x_1 \pmod p, \\ y_3 \equiv L(x_1 - x_3) + y_1^- \pmod p, \end{cases}$$

bu yerda: $L \equiv (3(R\,x_1^{\backslash 2} + 1) + a)(2(R\,y_1 + 1))^{-1} \pmod p$.

Ushbu standartda foydalanilgan parametrlar quyidagilar:

a) *r* – $r > 2^{255}$ tengsizlikni qanoatlantiruvchi tub son. Ushbu sonning yuqori chegaralari ERIni muayyan amalga oshirish jarayonida belgilanishi kerak;

b) elliptik egri chiziq *RE* o‘zining *J(RE)* invarianti yoki $4a^3+27(B\cdot R-a)^2(mod p)\neq 0$ shartni qanoatlantiruvchi $a,V\in RE(F_r)$ koeffitsientlar bilan berilgan;

s) R – *RE* parametrli elliptik egri chiziq parametri, bunda $2^{160} < R < 2^{255}$ shart bajariladi;

d) butun son $w=\#PE(F_p)$ - *RE* parametrli elliptik egri chiziq nuqtalari gruppasining tartibi;

e) *q* tub son - quyidagi shartlar bajarilgan *RE* parametrli elliptik egri chiziq nuqtalari gruppasi siklik qism gruppasining tartibi:

$$\begin{cases} w = lq, \quad l \in Z, \quad 1 \le l \le 4 \\ 2^{254} < q < 2^{256} \end{cases},$$

bu yerda: *l* – kofaktor, $l=\#PE(F_p)/q$;

f) $G=(x_3, y_3)$ – *R* parametrli *RE* elliptik egri chiziqlarning $q\cdot G=0_E$ shartni qanoatlantiruvchi bazaviy nuqtasi, bunda 0_E - parametrli elliptik egri chiziqning nol nuqtasi, $\cdot$ – *R* parametrli ko‘paytirish amali simvoli;

g) *H* – xesh-funksiya;

h) *S* – boshlang‘ich qiymat, parametrli elliptik egri chiziqlar «tasodifiy tanlash» strategiyasi bo‘yicha generatsiya qilinganda, tizim parametrlari tarkibiga kiritiladi.

Standart asosida ERIni shakllantirish jarayoni quyidagi ketma-ketliklardan iborat:

M xabar ostiga qo‘yiladigan ERIni yaratish uchun algoritm bo‘yicha quyidagi amallarni (qadamlarni) bajarish zarur:

1-qadam: *M* xabar, uchlik parametrlar *R*, *a* va *V* konkatenatsiyasining xesh-funksiyasi $h=H(M||R||a||V)$ hisoblanadi;

2-qadam: $e\equiv h(mod\ q)$ hisoblanadi. Agar $ye=0$ bo‘lsa, u holda $ye=1$ deb qabul qilinadi;

3-qadam: ushbu $2^{160}<k_i<q-2^{160}$ tengsizlikni qanoatlantiruvchi tasodifiy k_i son generatsiya qilinadi;

4-qadam: tasodifiy k_A songa ko‘ra parametrli elliptik egri chiziqning $[k_i]\cdot G=(x_1, y_1)$ nuqtasi hisoblanadi;

5-qadam: $r_i \equiv x_1 \ (mod\ q)$ hisoblanadi, agar $r=0$ bo‘lsa, u holda 3-qadamga qaytiladi;

6-qadam: $s_i \equiv (r_i d_i + k_i e)(mod\ q)$ hisoblanadi, agar $s=0$ bo‘lsa, u holda 3-qadamga qaytiladi;

7-qadam: dasturiy kriptografik modul chiqishida (r_i, s_i) ERI hosil qilinadi.

Ushbu jarayon uchun dastlabki ma’lumotlar bo‘lib d_i - yopiq kalit va imzolanuvchi xabar, chiqish natijasi bo‘lib esa, (r_i,s_i) ERI hisoblanadi.

ERIni tekshirish jarayoni esa quyidagi ketma-ketlikdan iborat:

Olingan M xabar ostiga qo‘yilgan ERI haqiqiyligini tasdiqlash uchun algoritm bo‘yicha quyidagi amallarni (qadamlarni) bajarish zarur:

1-qadam: $0<r_i,\ s_i<q$ shart bajarilishi tekshiriladi, agar shart bajarilsa, navbatdagi qadamga o‘tiladi, aks holda, dasturiy kriptografik modulning chiqishida «ERI haqiqiy emas» xabari paydo bo‘ladi;

2-qadam: M xabar, uchlik parametrlar R, a va V konkatenatsiyasining xesh-funksiyasi $h=H(M||R||a||V)$ hisoblanadi;

3-qadam: $e \equiv h(mod\ q)$ hisoblanadi. Agar $ye=0$ bo‘lsa, u holda $ye=1$ deb qabul qilinadi;

4-qadam: $v \equiv e^{-1}(mod\ q)$ ifodaning qiymati hisoblanadi;

5-qadam: $z_1 \equiv s_i v(mod\ q)$ va $z_2 \equiv -r_i v(mod\ q)$ ifodalar qiymatlari hisoblanadi;

6-qadam: agar ochiq kalit x ko‘rinishida kiritilgan bo‘lsa, u holda x_i bo‘yicha $y_i^{\backslash 2} \equiv x_i^{\backslash 3} + ax_i + B(mod\ p)$ va $y_i \equiv (x_i^{\backslash 3} + ax_i + B)^{\backslash 0.5}(mod\ p)$ hisoblanib, parametrli elliptik egri chiziqning $Y_i=(x_i, y_i)$ nuqtasi hosil qilinadi;

7-qadam: parametrli elliptik egri chiziqning $C=[z_1]\cdot G+[z_2]\cdot Y_i$ nuqtasi hisoblanadi va $X \equiv x_c \ (mod\ q)$ deb qabul qilinadi, bunda x_c – S nuqtaning x koordinatasi;

8-qadam: $X=r_i$ tenglik tekshiriladi, agar tenglik bajarilsa, u holda chiqishda «ERI haqiqiy» xabari, aks holda – «ERI haqiqiy emas» xabari paydo bo‘ladi.

Tanlangan parametrlarga qo‘yilgan talablar va na’munaviy misollar mazkur standartlarda ilova tarzida havola qilingan bo‘lib, ishlab chiqilgan dasturiy ta’minotni tekshirish uchun foydalanish mumkin.

II bob bo‘yicha xulosalar

1. Ishlab chiqilgan shifrlash, xesh-funksiya va ERI bo‘yicha milliy standartlarda oddiy diskret logarifmlash muammosiga qaraganda bardoshli bo‘lgan parametrli algebraga asoslanilgani aniqlandi.
2. Milliy standartlarda parametrli algebradan foydalanilgani ularni kutubxona sifatida shakllantirish uchun mos modul ishlab chiqilishini taqqazo qilishi aniqlandi.
3. Bundan tashqari milliy ERI standartlarini dasturiy amalga oshirishda elliptik egri chiziqda asoslanilgani, chekli maydonda elliptik egri chiziqlarda nuqtalarni qo‘shish va parametrli elliptik egi chiziqlarda nuqtalarni qo‘shish amallarini dasturiy tomondan yaratishni talab etishi aniqlandi.
4. Milliy standartni dasturiy amalga oshirish uchun aniqlangan talablarga ko‘ra mos asos kutubxona sifatida OpenSSL kutubxonasidan foydalanish belgilab olindi.

III bob. Milliy algoritmlarning kriptografik kutubxonasini ishlab chiqish va undan foydalanish

3.1. Milliy algoritmlarga asoslangan kriptografik kutubxonaning arxitekturasi

Axborotning kriptografik himoyasi qolgan himoya usullari orasida o‘zining ishonchligi va matematik tasdiqga egaligi bilan ajralib turadi. Axborotning kriptografik himoya usullari apparat-dasturiy va dasturiy ko‘rinishlarda amalga oshiriladi. Simmetrik kriptografik tizimlar ko‘proq apparat ko‘rinishga amalga oshirishga qulay bo‘lsa, yuqori hisoblash imkoniyatini talab etuvchi assimetrik kriptotizimlar esa dasturiy ko‘rinishlarda amalga oshiriladi. Dasturiy ko‘rinishlardagi kriptografik himoya vositalar odatda maxsus dastur yoki protokol ko‘rinishda bo‘lib, odatda biror kriptografik kutubxonaga asosan yaratiladi.

Hozirda turli turli kriptografik algoritmlarni o‘ziga mujassam qilgan ko‘plab kutubxonalar mavjud bo‘lib, ular yordamida qator dasturlash tillaridan foydalanib maxsus dasturiy vositalarni ishlab chiqish mumkin. Mavjud kriptografik kutubxonalarda asosan xalqaro kriptografik algoritmlar yoki turli davlatlarga tegishli bo‘lgan standartlar amalga oshirilgan bo‘lib, ular milliy standartlarni qamrab olmagan. Shu sababli, ushbu maqolada milliy standartlarni o‘zida mujassam qilgan kriptografik kutubxonani ishlab chiqish usullari va ketma-ketligi bilan tanishib chiqiladi.

Kriptografik kutubxonalarni yaratish ko‘p vaqt talab etuvchi va yuqori narx talab etuvchi jarayon bo‘lganligi sabab foydalanuvchilar odatda Open Soure turidagi kriptografik kutubxonalardan foydalanishni afzal ko‘radilar. Biroq bu kriptografik kutubxonalar har doim ham o‘ziga qo‘yilgan ishonchni oqlamasligi mumkin. Shunday ekan kriptografik kutubxonalarni sifatiga baho berishda nimlarga e’tibor berish kerak? Yaxshi kriptografik kutubxona quyidagi xususiyatlarga ega bo‘lishi kerak:

- kutubxona barcha mavjud kriptografik protokollar versiyalarini o‘zida jam qilgan bo‘lishi;

- kriptografik kutubxonada zaiflik bo‘lmasligi uchun turli testlashdan o‘tgan bo‘lishi;
- tashkilot loyihani amalga oshirishda javobgar bo‘lishi va loyihaga xizmat ko‘rsatish ishonchli bo‘lishi;
- kutubxona kodi litsenziyasi amalga oshiriluvchi loyihada foydalanishni madadlashi zarur.

Kriptografik kutubxonalar odatda o‘zida turli kriptografik algoritmlar, simmetrik shifrlash algoritmlari va ularning rejimlari, xesh-funksiyalar, ma’lumotlarni autentifikatsiyalash kodlari, ERI algoritmlari, kalitlarni generatsiyalash algoritmlari, sonlarni turli formatlarda ifodalash standartlarini va h.larni mujassam qilgan bo‘ladi. Hozirda respublikamizda quyidagi kriptografik standartlar mavjud:

- O‘z DSt 1105:2009 - ma’lumotlarni shifrlash algoritmi;
- O‘z DSt 1106:2009 - xeshlash funksiyasi;
- O‘z DSt 1092:2009 va O‘z DSt 2826:2014 - elektron raqamli imzoni shakllantirish va tekshirish standartlari.

Mazkur standartlar asosida kriptografik kutubxonani ishlab chiqishda quyidagi vazifalar qo‘yildi:

- yaratilayotgan kriptografik kutubxona ixcham bo‘lishi;
- yaratilayotgan kriptografik kutubxona portativ bo‘lishi;
- foydalanishga qulay bo‘lishi;
- yaratilayotgan kriptografik kutubxona tezkor bo‘lishi;
- yaratilayotgan kriptografik kutubxonani yangilash imkoni mavjud bo‘lishi.

Milliy standartlar asosida kriptografik kutubxonani ishlab chiqishda qo‘yilgan vazifalarni bajarish uchun asos sifatida OpenSSL kutubxonasi olindi. Ushbu kriptografik kutubxonaning quyidagi amallaridan milliy kriptogarfik kutubxonani yaratishda foydalanildi:

- katta uzunlikdagi sonlarni ifodalash formati BIGNUM klassidan;
- tasodifiy sonlarni generatsiyalash algoritmi RAND.C klassidan;

- sonlarni tasodifiylikga tekshirish imkonini beruvchi, Rabin-Miller testiga asoslangan klassdan.

OpenSSL kutubxonasiga asoslangan holda taklif etilayotgan milliy standartlarni o‘z ichiga olgan kriptografik kutubxonaning arxitekturasi quyidagi 3.1-rasmda keltirilgan [31].

3.1.1-rasm. Milliy standartlarga asoslangan kriptografik kutubxona arxitekturasi (OpenSSL asosida)

Yuqorida aytilgani kabi milliy kriptografik standartlar OpenSSL kutubxonasi o‘zagida mavjud bo‘lgan amallarga asoslanadi. Bunda milliy standartlarni amalga oshirishi uchun tasodifiy qiymatlarni, tub sonlarni, katta uzunlikdagi *integer* tipidagi sonlarni zarur bo‘lishi inobatga olindi. OpenSSL kutubxonasida asoslangani uchun milliy kutubxona S++ dasturiy tili yordamida amalga oshiriladi. OpenSSL amallari asosida yuqoridagi 4 ta standartga algoritmlari amalga oshiriladi. Ishlab chiqilgan kriptografik kutubxonadan foydalanish uchun standart ilova moduli mavjud bo‘lib, u foydalanuvchiga kriptografik algoritm-lardan foydalanish imkoniyatini taqdim etadi. Aynan OpenSSL o‘zagi asosida standart algoritmlar amallari qurilma sathiga o‘tkaziladi va xotiraga yuklanadi.

Agar dasturchi yuqori dasturlash tilidan foydalanishni maqsad qilgan bo‘lsa u holda C# dasturlash tilidan foydalanishi mumkin. Yuqorida keltirilgan 3.1 – rasmdagi ko‘rinish esa quyidagicha ko‘rinishda bo‘ladi (3.2-rasm).

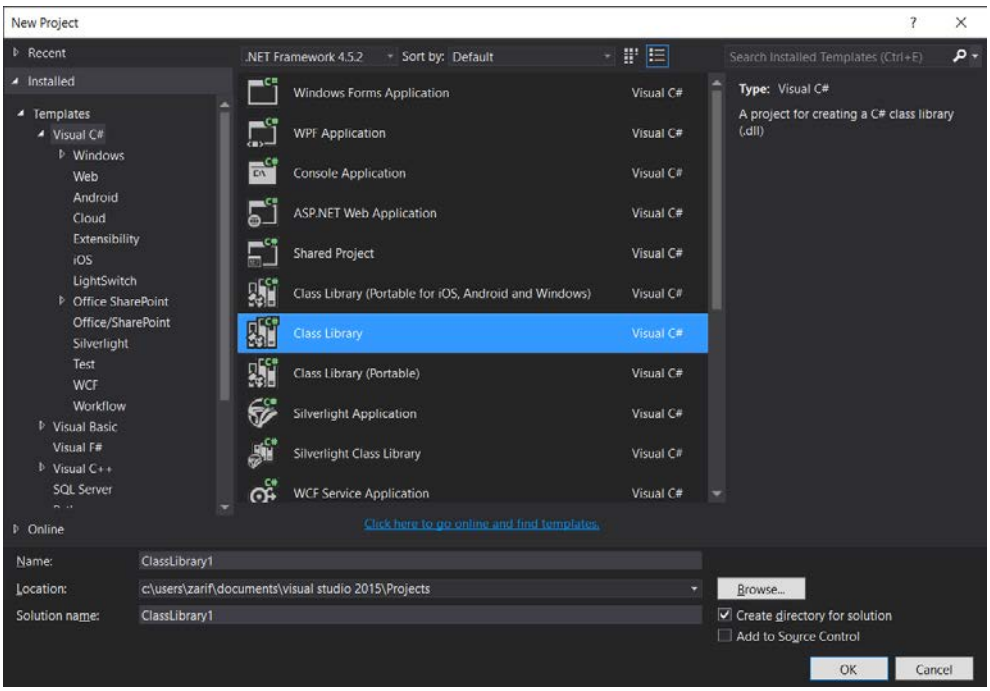
3.1.2-rasm. Milliy standartlarga asoslangan kriptografik kutubxona arxitekturasi (.NETFramework asosida)

Taklif etilgan arxitektura C# dasturlash tiliga amalga oshirilishi uning tezkorligi va qo‘yilgan vazifalarni bajarishiga asosiy omil bo‘lib xizmat qiladi.

3.2. Milliy algoritmlarning kriptografik kutubxonasini ishlab chiqish

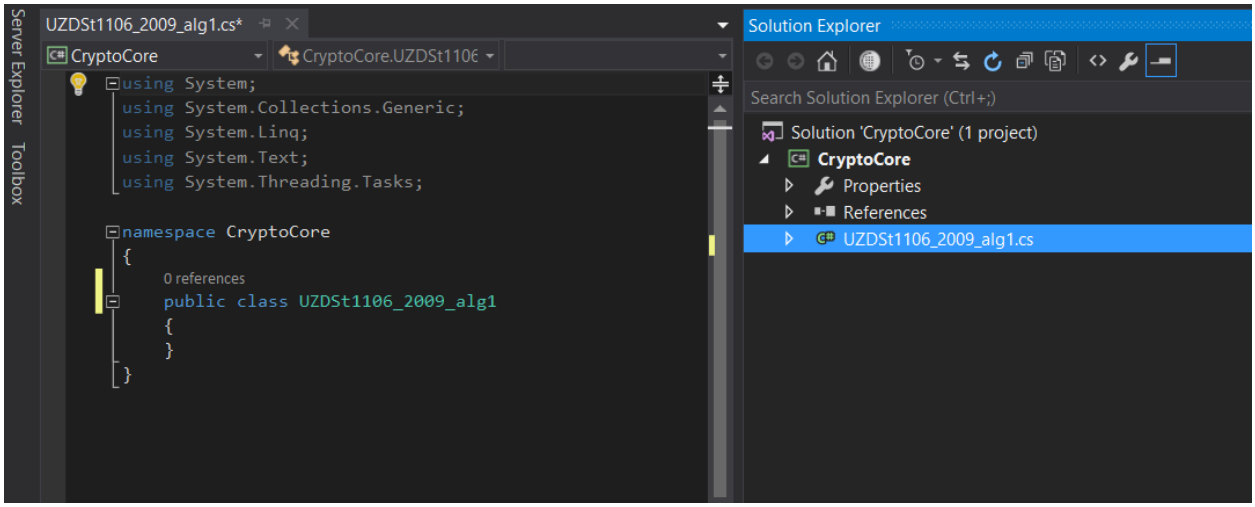
Milliy kriptografik algoritmlar asosida kutubxonani yaratishda yuqori dasturlash tili hisoblangan C# dan foydalanildi. Ushbu dasturlash tili yordamida dinamik havolalar kutubxonasi (Dynamic Link library, DLL)ni yaratish imkoniyati mavjud. Bunda ishlab chiqilgan .dll kutubxona faylidan bir vaqtda ko‘plab dasturlar foydalanishi mumkin bo‘ladi. Quyida sodda holatda C# dasturlash tilidan foydalanib .dll fayl yaratish va undan foydalanish tartibi keltirilgan.

.dll kutubxona yaratish. Visual Studio 2015 dasturlash tillari kompleksidan foydalangan holda .dll faylni yaratishda quyidagi ketma-ketlikdan foydalaniladi. Dastlab “File” → “New” → “Project...” bandi va undan so‘ng “Visual C#” → “Class library” bandi tanlanadi (3.3 - rasm).



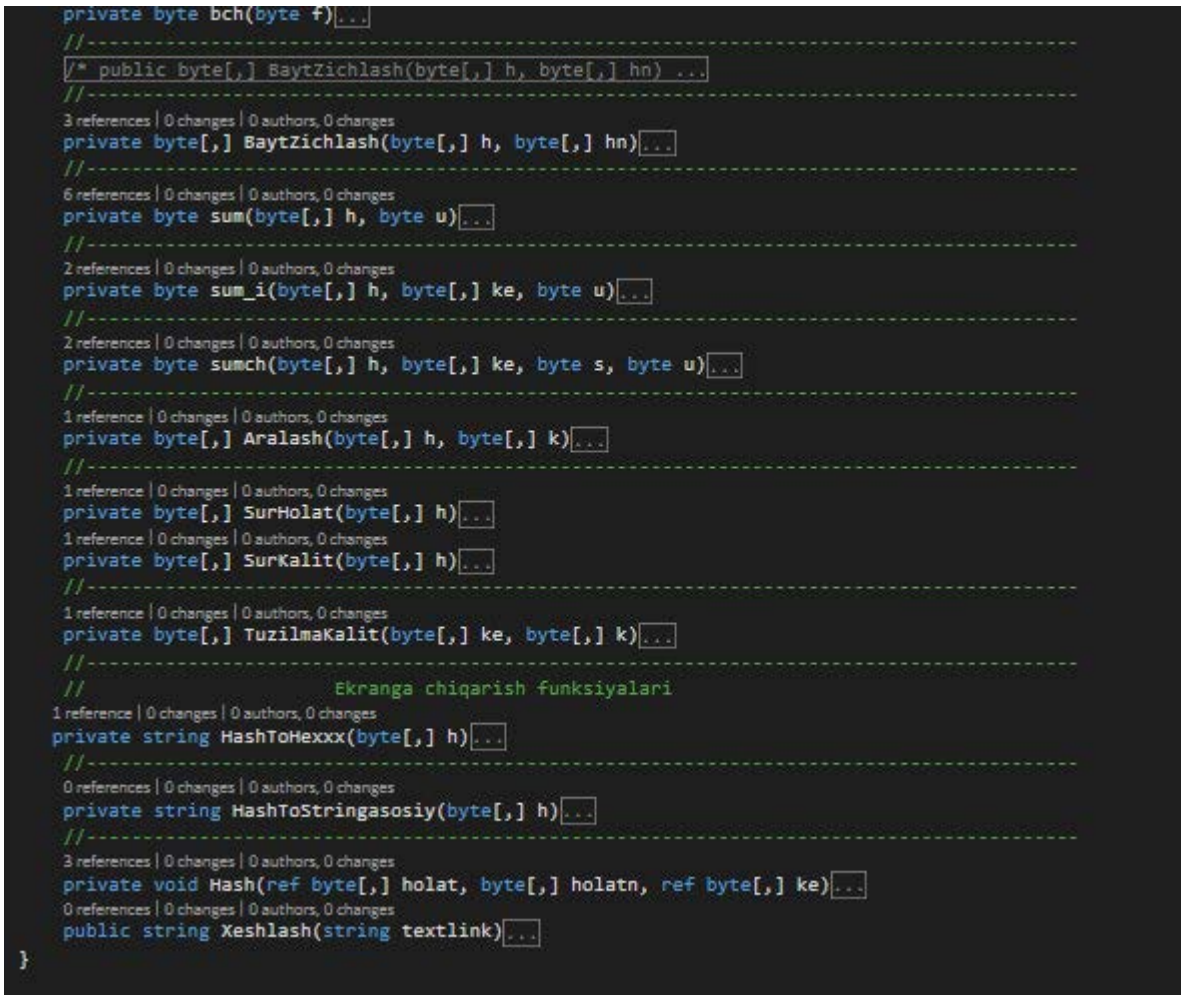
3.2.1 – rasm. C# dasturlash tilida kutubxona yaratish

Yaratilayotgan kriptografik kutubxonaga mos bo‘lgan nom beriladi va OK tugmasi bosiladi (3.4-rasm). Mazkur holatda O‘z DSt 1106:2009 xesh standartining 1-algoritmini yaratish tartibi keltirilgan.



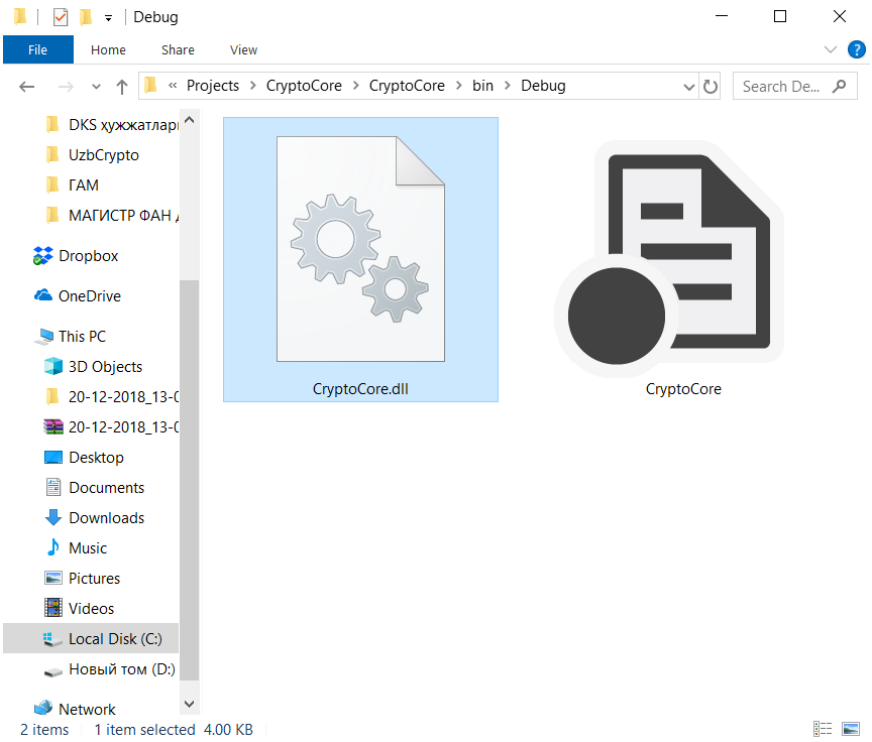
3.2.2-rasm. Yaratilgan kutubxona

Shundan so‘ng CryptoCore.UZDSt1106_2009_alg1 klassi to‘liq holatda yaratib chiqiladi. Quyida ushbu kodlar qatorining qisqartirilgan ko‘rinishi keltirilgan (3.5-rasm).



3.2.3 – rasm. CryptoCore.UZDSt1106_2009_alg1 klasining qisqartirilgan ko‘rinishi

UZDSt1106_2009_alg1 algoritm to‘liq amalga oshirilgandan so‘ng, dastur “RUN” qilinadi. Shundan so‘ng, talab etilgan kutubxona .dll fayl hosil bo‘ladi (3.6-rasm).

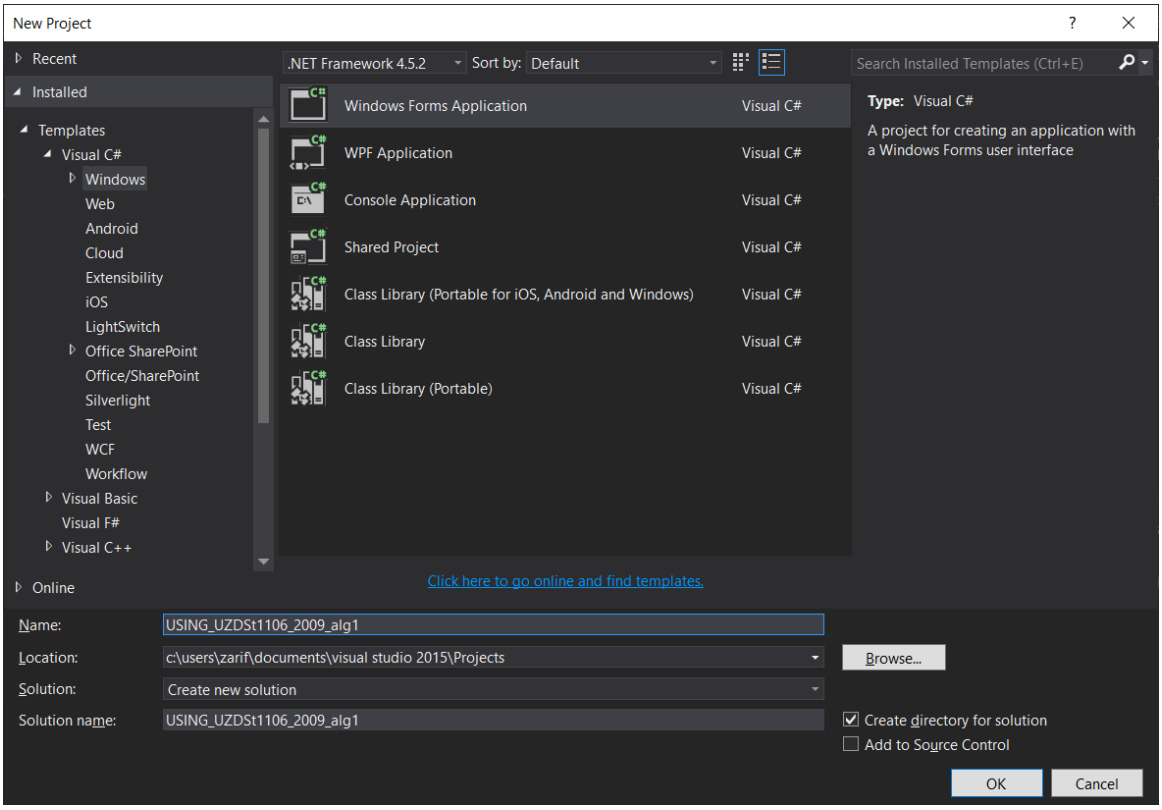


3.2.4 – rasm. Hosil qilingan CryptoCore kutubxona fayli

Xuddi shu asnoda qolgan algoritmlar ham to‘liq realizatsiya qilinadi. Umumiy holatda yaratilgan CryptoCore kutubxonasining umumiy arxitekturasi quyidagi ko‘rinishda bo‘ladi (3.2.7 - rasm).

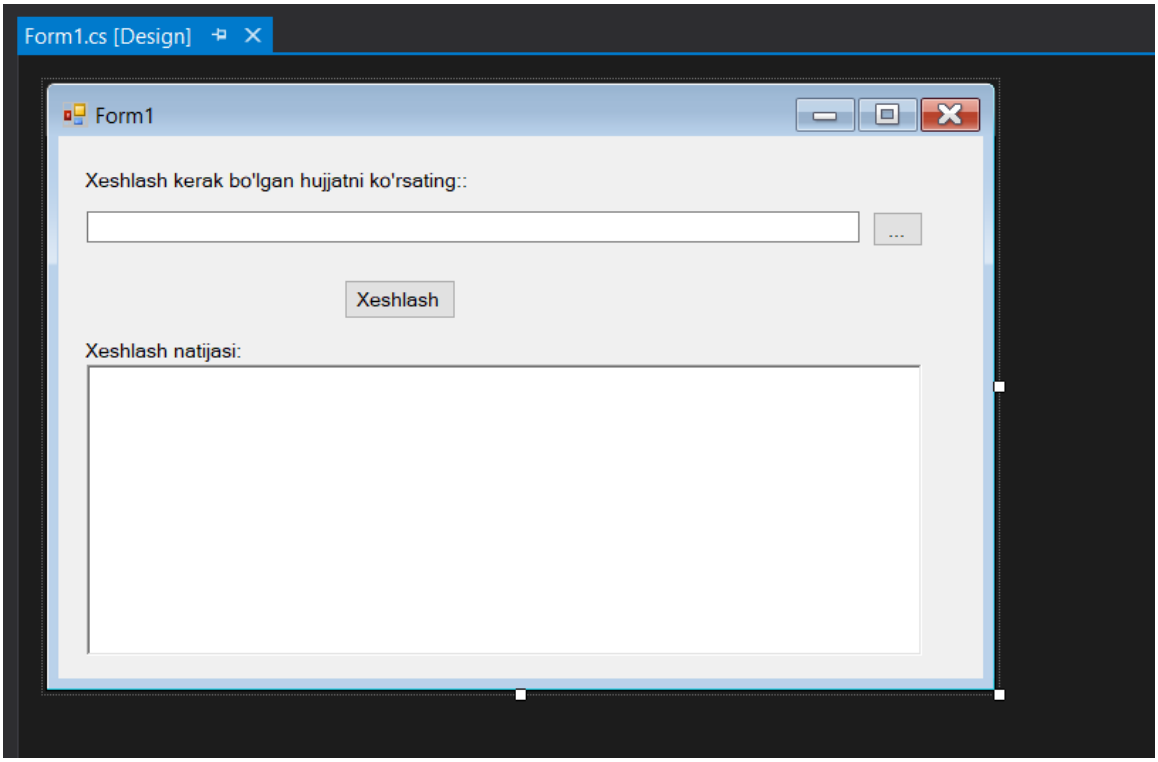
3.3. Milliy algoritmlarning kriptografik kutubxonasidan foydalanish va uning tahlili

Yaratilgan dinamik kutubxona CryptoCore dan foydalanish uchun Microsoft Visual Studio 2015 dasturlar paketidan foydalanib, yangi loyiha yaratiladi va unga “USING_UZDSt1106_2009_alg1” deb nom berildi (3.3.1 - rasm).



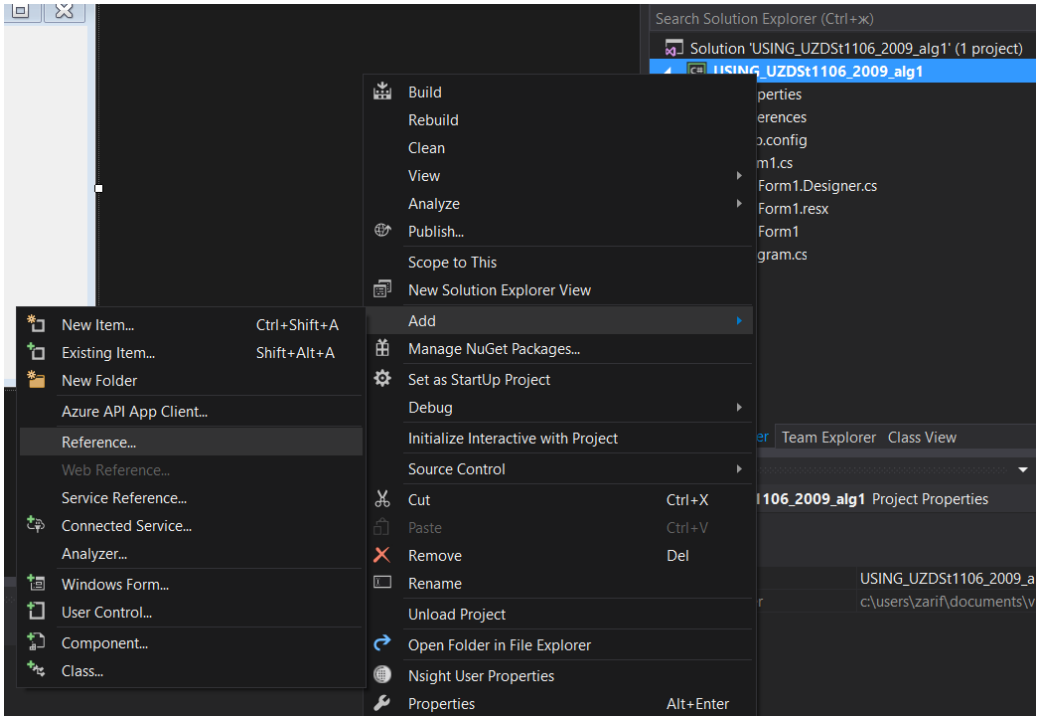
3.3.1-rasm. USING_UZDSt1106_2009_alg1 nomli loyiha ishlab chiqish

Shundan so‘ng ishlab chiqilgan kriptogarfik kutubxonadan foydalanish uchun quyidagi interfeysga ega forma yaratiladi (3.9-rasm).



3.3.2-rasm. USING_UZDSt1106_2009_alg1 loyihasida Form1 oynasini yaratish

Yaratilgan kutubxonani mazkur loyiha ulash uchun loyiha ustiga sichqonchaning o‘ng tugmasi bosiladi. Bu yerdan “Add reference” tugmasi tanlanadi va shundan so‘ng talab etilgan “CryptoCore” kutubxonasi tanlanadi (3.10 - rasm).



3.3.3-rasm. “CryptoCore” kutubxonasini loyihaga ulash

“CryptoCore” kutubxona loyihaga ulangandan so‘ng “Solution Explorer” oynasida ushbu kutubhona namoyon bo‘ladi (3.3.4-rasm).

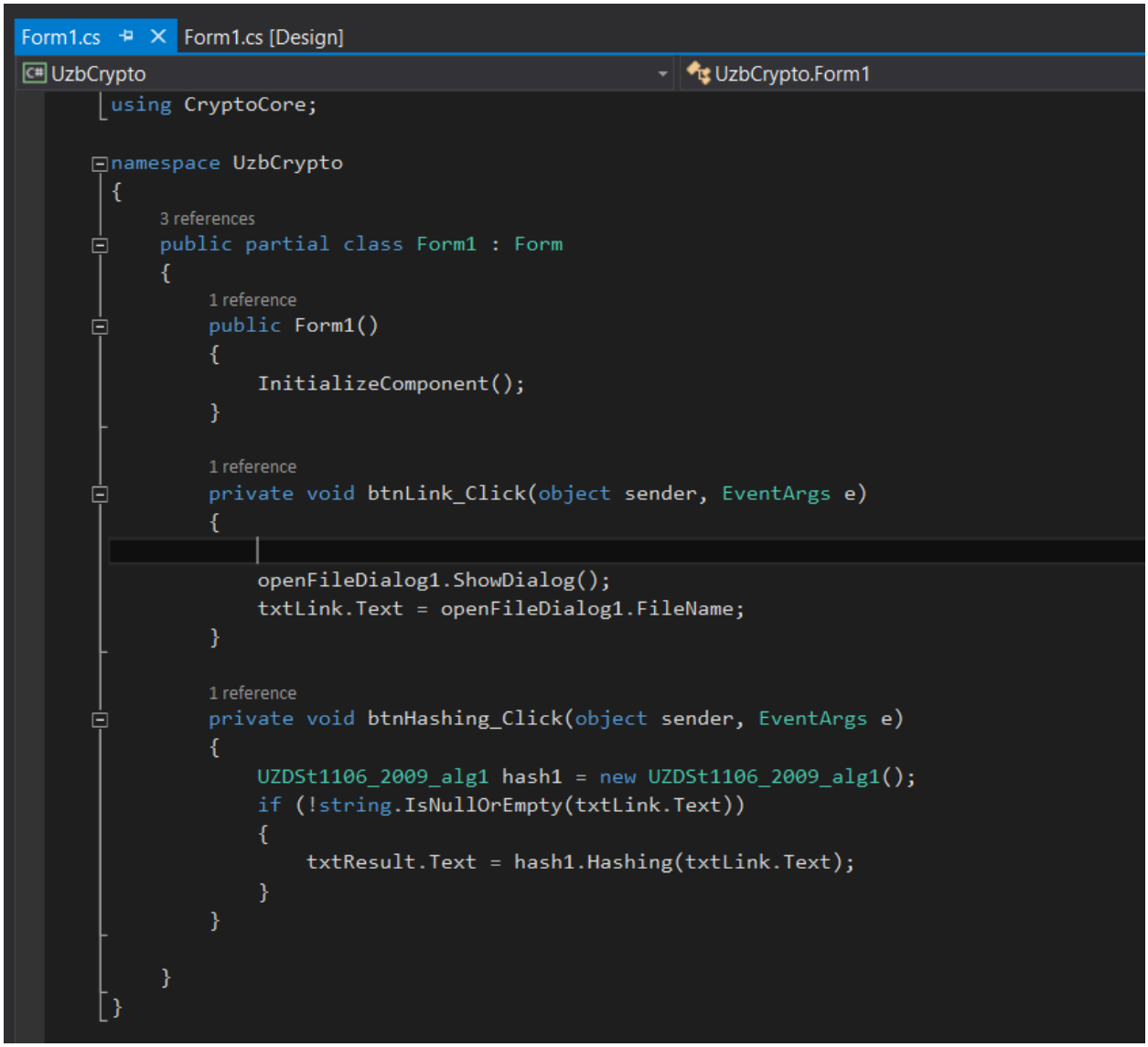
```
0 references | 0 changes | 0 authors, 0 changes
public class UZDSt1106_2009_alg1
{

    int g = -1 % 5;
    private byte[,] Blok0 =  {{19, 23, 27, 31, 131, 142, 153, 166},
                             {20, 41, 28, 37, 132, 145, 158, 169 },
                             {21, 25, 29, 33, 137, 147, 163, 171},
                             {22, 27, 30, 35, 139, 150, 169, 174}};
    private static byte[,] Key = {{200, 110, 212, 178, 117, 109,  241, 205},
                                  {107, 110, 202, 129, 212, 65 ,  128, 146},
                                  {33 , 171, 129, 187, 160, 199,  193, 80 },
                                  {68 , 190, 143, 235, 147, 79 ,  149, 162}};
    private byte[,] jadval =  {{5, 13, 6,    11, 1,  10, 15, 8,  0,  4,  7,  9,  2,  12, 3,  14},
                               {8, 7, 2,  14, 15, 3,  11, 6,  1,  12, 13, 10, 5,  4,  9,  0},
                               {14, 2, 13, 4, 12, 7,  1,  11, 6,  9,  0,  5,  3,  10, 8,  15},
                               {0, 14, 9, 12, 3,  13, 7,  4,  15, 6,  5,  1,  11, 2,  10, 8},
                               {3, 10, 7, 2,  4,  12, 9,  1,  14, 13, 15, 8,  0,  5,  11, 6},
                               {2, 3, 1,  8, 0, 14,   5,  9,  12, 11, 6,  7,  10, 15, 13, 4},
                               {10, 4, 14, 15, 9, 5,  8,  2,  11, 0,  1,  3,  12, 6,  7,  13},
                               {11, 9, 10, 1, 6,  4,  13, 15, 3,  5,  14, 0,  8,  7,  2,  12},
                               {1, 0, 3,  7,  13, 11, 10, 12, 9,  14, 4,  6,  15, 8,  5,  2},
                               {4, 8, 11, 9,  14, 6,  2,  5,  10, 3,  12, 15, 7,  13, 0,  1},
                               {9, 12, 15, 0, 2,  1,  14, 10, 5,  8,  11, 13, 4,  3,  6,  7},
                               {6, 11, 8, 13, 7,  9,  0,  3,  4,  15, 10, 2,  14, 1,  12, 5},
                               {15, 1, 0, 5,  10, 8,  3,  7,  13, 2,  9,  12, 6,  14, 4,  11},
                               {12, 5, 4, 10, 11, 2,  6,  13, 8,  7,  3,  14, 1,  0,  15, 9},
                               {7, 15, 12, 6, 5,  0,  4,  14, 2,  10, 8,  11, 13, 9,  1,  3},
                               {13, 6, 5, 3,  8,  15, 12, 0,  7,  1,  2,  4,  9,  11, 14, 10}};

    private int p = 256, round = 0;
```

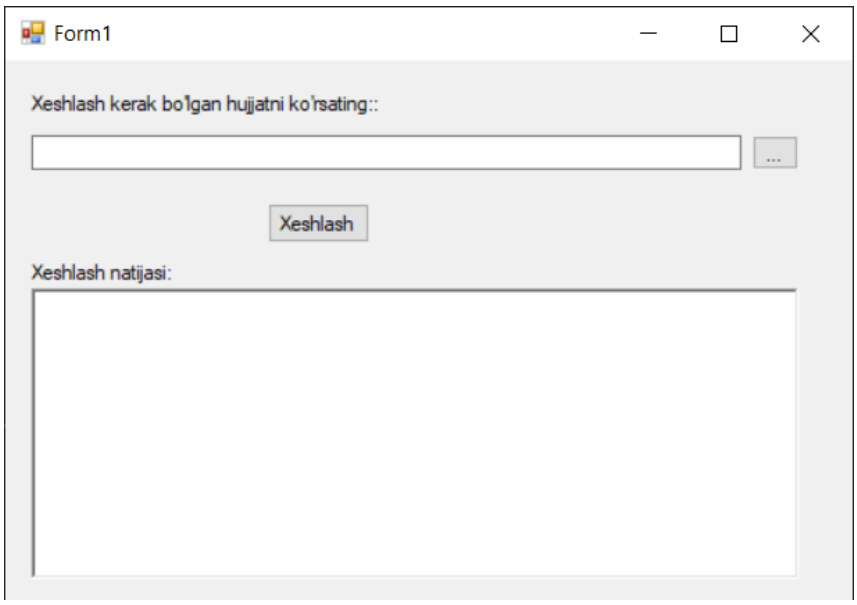
3.3.4-rasm. Qo‘shilgan “CryptoCore” kutubxona

Shundan so‘ng, `using CryptoCore;` buyrug‘idan foydalangan holda kutubxona joriy klass (Form1 klasi uchun) uchun ulanadi. Ushbu oynadagi faylni tanlash va xeshlash tugmalari uchun quyida keltirilgan vazifalarni bajaruvchi buyruqlar yoziladi (3.3.5-rasm).



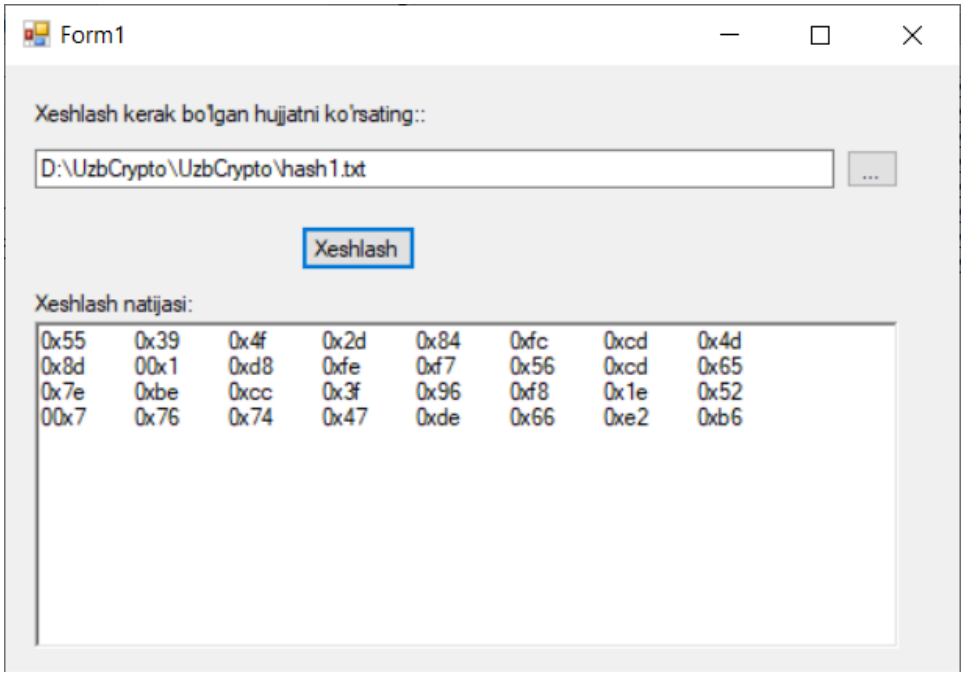
3.3.5-rasm. Form1 oynasining dasturiy kodi

Shundan so‘ng dastur yuklanganda (Run buyrug‘i asosida) quyidagi oyna hosil bo‘ladi (3.3.6 - rasm).



3.3.6-rasm. Form1 oynasi

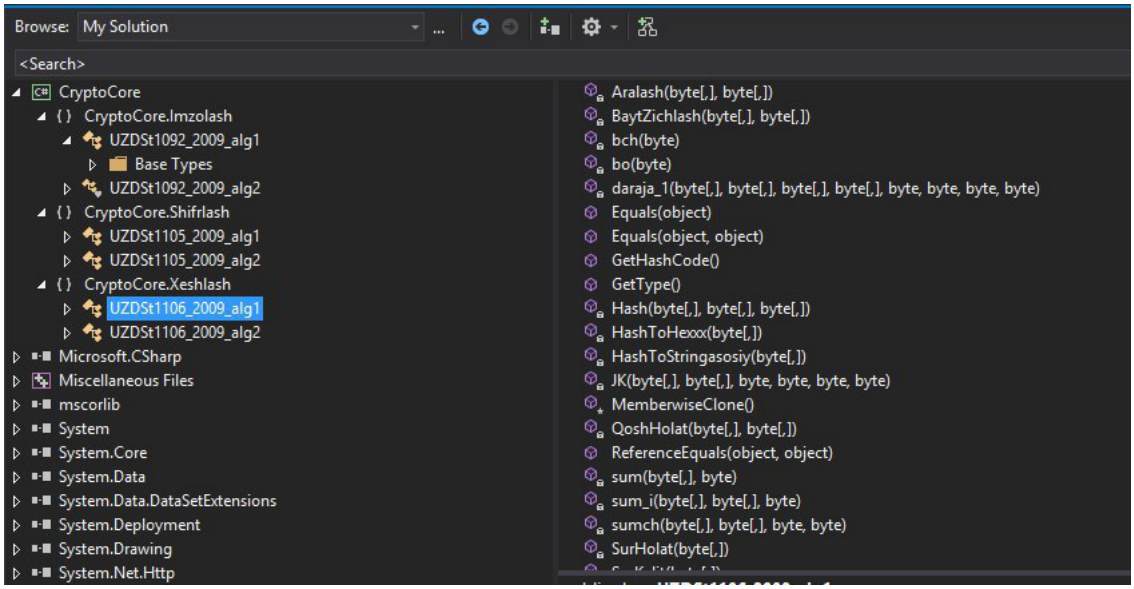
Mazkur oynadan kerakli bo‘lgan xeshlanuvchi fayl tanlanadi va “Xeshlash” tugmasi bosiladi. Ma’lumotning xesh qiymati esa quyidagi oynada namoyon bo‘ladi (3.3.7 - rasm). Algoritm ishlashini to‘g‘ri ishlayotganini tekshirish ma’lumot sifatida “*funksiyaxeshirovaniyainformasionnayatexnologiyakriptograficheska*” olingan. Bundan tashqari dastur standartda keltirilgan parametrlar asosida sozlangan.



3.3.7 - rasm. “Xeshlash” tugmasi bosilgandan keyingi natija

Olingan natijadan ko‘rinadiki, UZDSt1106_2009_alg1 algoritmining dasturiy kodi to‘g‘ri yozilgan va natijalar standartdagi kabi bir xil ko‘rinishda.

Bundan tashqari ishlab chiqilgan barcha algoritmlar ham shu asnoda tekshirib chiqiladi (3.3.8 - rasm).



3.3.8 – rasm. CryptoCore” kutubxonasining umumiy ko‘rinishi

III bob bo‘yicha xulosalar

Dissertatsiya ishining uchinchi bobi bo‘yicha quyidagi natijalar va xulosalar olindi:

1. Sathga asoslangan kriptografik kutubxonaning arxitekturasi tushunishga katta amaliy yordam beradi.

2. Kriptografik algoritmlarni kriptgrafik kutubxona sifatida shakllantirish undan bir vaqtda ko‘plab loyihalarda foydalanish imkoniyatini yaratadi.

3. Kriptografik kutubonalarni yaratishda foydalaniluvchi muhit Windows bo‘lganda, C# dasturlash tilidan foydalanish samara va xavfsizlik muammolarini kamaytirish imkoniyatini beradi.

4. Kriptogarfik kutubxonani yuqori dasturlash tilida amalga oshirish quyi darajada amalga oshirilganiga ko‘ra ishlashdagi tezkorligi pastligi bilan farq qiladi.

Xulosa

Ushbu dissertatsiya ishida milliy kriptografik algoritmlarga asoslangan kutubxonani ishlab chiqish amalga oshirilgan bo‘lib, quyidagi natijalarga ega bo‘lindi:

1. Axborotning kriptografik himoyasining o‘rni muhimligi asoslanildi.
2. Kriptografik dasturiy himoya vositalari va ularni yaratish usullari tahlil qilindi.
3. Hozirda mavjud kriptografik kutubxonalar foydalanilgan algoritmlar xili, foydalanilgan dasturlash tili, samaradorligi va amalga oshirish muhitiga ko‘ra tahlillandi.
4. Milliy kriptografik algoritmlar dasturiy tomondan amalga oshirilish darajasiga ko‘ra tahlillandi.
5. Milliy kriptografik algoritmlarga asoslangan kriptografik kutubxona C# dasturlash tilida ishlab chiqildi.
6. Ishlab chiqilgan kriptografik kutubxonadan foydalanish bo‘yicha yo‘riqnomalar ishlab chiqildi.

Foydalanilgan adabiyotlar ro‘yxati

1. O‘zbekiston Respublikasi Prezidentining 2017 yil 7 fevraldagi PF-4947-son «O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida» gi Farmoni.
2. O‘zbekiston Respublikasi Prezidentining 2018 yil 14 martdagi PF-5379-son «O‘zbekiston Respublikasining davlat xavfsizligi tizimini takomillashtirish chora-tadbirlari to‘g‘risida»gi Farmoni.
3. O‘zbekiston Respublikasi Prezidentining 2018 yil 19 fevraldagi PF-5349-son « Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to‘g‘risida»gi Farmoni.
4. O‘zbekiston Respublikasi Prezidentining 2007 yil 3 apreldagi PQ-614-son «O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to‘g‘risida»gi Qarori.
5. O‘z DSt 1092:2009 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari.
6. O‘z DSt 1106:2009 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi.
7. O‘z DSt 1109:2013 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta’riflar.
8. O‘z DSt 1204:2009 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Kriptografik modullarga xavfsizlik talablari.
9. O‘z DSt 2826:2014 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elliptik egri chiziqlarga asoslangan elektron raqamli imzoni shakllantirish va tekshirish jarayonlari.
10. O‘z DSt 1047:2003 Axborot texnologiyalari. Atamalar va ta’riflar.
11. O‘z DSt 1109:2006 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta’riflar.

12. O‘z DSt 1105:2009 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi.

13. GOST 28147-89 Sistemы obrabotki informatsii. Zaщita kriptograficheskaya. Algoritmы kriptograficheskogo preobrazovaniya.

14. GOST R 34.11-94 Informatsionnaya texnologiya. Kriptograficheskaya zaщita informatsii. Funksiya xeshirovaniya.

15. GOST R 34.10-2001 Informatsionnaya texnologiya. Kriptograficheskaya zaщita informatsii. Protsessы formirovaniya i proverki elektronnoy sifrovoy podpisi.

16. O‘z DSt 1109:2013 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta’riflar.

17. D.Ye.Akbarov. “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi”. Toshkent, 2008 – 394 bet.

18. Apparatno-programmnыe sredstva i metodы zaщitы informatsii. S.K. Varlataya, M.V. Shaxanova. Vladivostok 2007.

19. Metodы i sredstva kriptograficheskoy zaщitы informatsii. O.N. Jdanov v. V. Zolotarev. Krasnoyarsk 2007.

20. Applied Cryptography Second Edition Protocols, Algorthms, and Source Code in C. Bruce Schneier. Publication Date: 01/01/96.

21. Akbarov D.Ye. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi // Toshkent, 2008, -B. - 394.

22. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, -P. – 606.

23. Daemen J., Rijmen V. Announcing the advanced encryption standard (AES) //Federal Information Processing Standards Publication. – 2001. – T. 197.

24. Natsionalnыy standart Rossiyskoy federatsii. Informatsionnaya texnologiya. Kriptograficheskaya zaщita informatsii. Blochnыe shifrы. GOST R 34.12-2015.

25. Dworkin M. J. SHA-3 standard: Permutation-based hash and extendable-output functions. – 2015. – №. Federal Inf. Process. Stds.(NIST FIPS)-202.

26. Natsionalnыy standart Rossiyskoy federatsii. Informatsionnaya texnologiya. Kriptograficheskaya zaщita informatsii. Funksiya xeshirovaniya. GOST R 34.11-2012.

27. Locke G., Gallagher P. Fips pub 186-3: Digital signature standard (dss) //Federal Information Processing Standards Publication. – 2009. – T. 3. – S. 186-3.

28. *https://dotnet.microsoft.com/learn/dotnet/what-is-dotnet*

29. *https://www.oracle.com/java/technologies/java-se.html*

30. https://en.wikipedia.org/wiki/Comparison_of_cryptography_libraries

31. Tojiakbarova U.U. Kriptografik kutubxonalarni yaratish usullari. Axborot-kommunikatsiya texnologiyalarini rivojlantirish sharoitida innovatsiyalar mavzusidagi Respublika ilmiy-amaliy anjumani. Qarshi – 2016. 357-359 b.

32. Tojiakbarova U.U. Kriptografik kutubxonalarni qiyosiy tahlili. Axborot-kommunikatsiya texnologiyalarini rivojlantirish sharoitida innovatsiyalar mavzusidagi Respublika ilmiy-amaliy anjumani. Qarshi – 2016. 370-372 b.

33. Nazaruk V., Rusakov P. Implementation of Cryptographic Algorithms in Software: An Analysis of the Effectiveness //Scientific Journal of Riga Technical University. Computer Sciences. – 2010. – T. 41. – №. 1. – S. 97-105.

```
//Kutubxonanin kodlari


public class UZDSt1106_2009_alg1
{

int g = -1 % 5;
      private byte[,] Blok0 =  {{19, 23, 27, 31, 131, 142, 153, 166},
                          {20, 41, 28, 37, 132, 145, 158, 169 },
                          {21, 25, 29, 33, 137, 147, 163, 171},
                          {22, 27, 30, 35, 139, 150, 169, 174}};
      private static byte[,] Key = {{200, 110, 212, 178, 117, 109,  241, 205},
                            {107, 110, 202, 129, 212, 65 ,  128, 146},
                            {33 , 171, 129, 187, 160, 199,  193, 80 },
                            {68 , 190, 143, 235, 147, 79 ,  149, 162}};
      private byte[,] jadval =  {{5, 13, 6,    11, 1,  10, 15, 8,  0,  4,  7,  9,  2,  12, 3,
14},
                          {8, 7, 2,  14, 15, 3,  11, 6,  1,  12, 13, 10, 5,  4,  9,  0},
                          {14, 2, 13, 4, 12, 7,  1,  11, 6,  9,  0,  5,  3,  10, 8,  15},
                          {0, 14, 9, 12, 3,  13, 7,  4,  15, 6,  5,  1,  11, 2,  10, 8},
                          {3, 10, 7, 2,  4,  12, 9,  1,  14, 13, 15, 8,  0,  5,  11, 6},
                          {2, 3, 1,  8, 0, 14,   5,  9,  12, 11, 6,  7,  10, 15, 13, 4},
                          {10, 4, 14, 15, 9, 5,  8,  2,  11, 0,  1,  3,  12, 6,  7,  13},
                          {11, 9, 10, 1, 6,  4,  13, 15, 3,  5,  14, 0,  8,  7,  2,  12},
                          {1, 0, 3,  7,  13, 11, 10, 12, 9,  14, 4,  6,  15, 8,  5,  2},
                          {4, 8, 11, 9,  14, 6,  2,  5,  10, 3,  12, 15, 7,  13, 0,  1},
                          {9, 12, 15, 0, 2,  1,  14, 10, 5,  8,  11, 13, 4,  3,  6,  7},
                          {6, 11, 8, 13, 7,  9,  0,  3,  4,  15, 10, 2,  14, 1,  12, 5},
                          {15, 1, 0, 5,  10, 8,  3,  7,  13, 2,  9,  12, 6,  14, 4,  11},
                          {12, 5, 4, 10, 11, 2,  6,  13, 8,  7,  3,  14, 1,  0,  15, 9},
                          {7, 15, 12, 6, 5,  0,  4,  14, 2,  10, 8,  11, 13, 9,  1,  3},
                          {13, 6, 5, 3,  8,  15, 12, 0,  7,  1,  2,  4,  9,  11, 14, 10}};

      private int p = 256, round = 0;

      private byte R = Key[0, 0];
```

```
        //---------- Teskari funksiya son ni p modul bo'yicha teskari qiymatini
topadi----------
        private byte teskari(byte son)
        {
            byte l, res, c;
            for (c = 1; c <= 256; c++)
            {
                l = (byte)((c * son) % p);
                if (l == 1)
                    goto tugat;
            }
            tugat: res = (byte)(c % p);
            return res;
        }
        //-----------------------------------------------------------------------------------
        private byte[,] uzlashtir(byte[,] hol)
        {
            byte[,] holT = new byte[4, 8];
            byte s, u;
            for (s = 0; s < 4; s++)
                for (u = 0; u < 8; u++)
                    holT[s, u] = hol[s, u];
            return holT;
        }
        //-----------------------------------------------------------------------------------
        private void JK(byte[,] holat, byte[,] holatn, out byte J_h, out byte J_hn, out
byte K_h, out byte K_hn)
        {
            byte s, u, delta;
            byte h, hn;
            J_h = 0; K_h = 1;
            J_hn = 0; K_hn = 1;
            for (s = 0; s < 4; s++)
                for (u = 0; u < 8; u++)
                {
                    if (holat[s, u] % 2 == 0)
                        h = (byte)((holat[s, u] + 1) % p);
                    else
                        h = holat[s, u];
```

```
                J_h = (byte)((J_h + holat[s, u]) % p);
                K_h = (byte)((K_h * h) % p);
                if (holatn[s, u] % 2 == 0)
                    hn = (byte)((holatn[s, u] + 1) % p);
                else
                    hn = holatn[s, u];
                J_hn = (byte)((J_hn + holatn[s, u]) % p);
                K_hn = (byte)((K_hn * hn) % p);
            }
        if (K_h == (J_hn + 1) || K_h == (byte)(-(J_hn + 1)))
            delta = 10;
        else
            delta = 0;
        K_h = (byte)((K_h + delta) % p);
        if (K_hn == (J_h + 1) || K_hn == (byte)(-(J_h + 1)))
            delta = 10;
        else
            delta = 0;
        K_hn = (byte)((K_hn + delta) % p);
    }
    //-------------------------------------------------------------------------------------
------------
    private void daraja_1(byte[,] holat, byte[,] holatn, out byte[,] h1, out byte[,]
hn1, out byte J1h, out byte J1hn, out byte K1h, out byte K1hn)
    {
        h1 = new byte[4, 8];
        hn1 = new byte[4, 8];
        byte s, u, delta_A1h, delta_A1hn;
        byte A1h, A1hn, B1h, B1hn;
        JK(holat, holatn, out J1h, out J1hn, out K1h, out K1hn);
        if (J1hn % 2 == 1)
            delta_A1h = 0;
        else
            delta_A1h = 1;
        if (J1h % 2 == 1)
            delta_A1hn = 0;
        else
            delta_A1hn = 1;
        for (s = 0; s < 4; s++)
```

```
            for (u = 0; u < 8; u++)
            {
                A1h = (byte)((J1hn + 2 * holatn[s, u] + delta_A1h) % p);
                A1hn = (byte)((J1h + 2 * holat[s, u] + delta_A1hn) % p);
                B1h = (byte)((K1h - 2 * holat[s, u]) % p);
                B1hn = (byte)((K1hn - 2 * holatn[s, u]) % p);
                h1[s, u] = (byte)(-A1h * holat[s, u] * teskari((byte)(B1h + R *
holat[s, u])) % p);
                hn1[s, u] = (byte)(-A1hn * holatn[s, u] * teskari((byte)(B1hn + R *
holatn[s, u])) % p);
            }
        }
        //----------------------------------------------------------------------------
        private void QoshHolat(ref byte[,] h, ref byte[,] hn)
        {
            byte[,] h2 = new byte[4, 8];
            byte[,] hn2 = new byte[4, 8];
            byte[,] h3 = new byte[4, 8];
            byte[,] hn3 = new byte[4, 8];
            byte[,] h1 = new byte[4, 8];
            byte[,] hn1 = new byte[4, 8];
            byte s, u, delta_A2h, delta_A2hn;
            byte J1h, J1hn, K1h, K1hn;
            byte J2h, J2hn, K2h, K2hn;
            byte A2h, A2hn, B2h, B2hn;
            daraja_1(h, hn, out h1, out hn1, out J1h, out J1hn, out K1h, out K1hn);
            JK(h1, hn1, out J2h, out J2hn, out K2h, out K2hn);
            if ((J1hn + J2hn) % 2 == 1)
                delta_A2h = 0;
            else
                delta_A2h = 1;
            if ((J1h + J2h) % 2 == 1)
                delta_A2hn = 0;
            else
                delta_A2hn = 1;
            for (s = 0; s < 4; s++)
                for (u = 0; u < 8; u++)
                {
                    A2h = (byte)((J1hn + J2hn + 2 * hn1[s, u] + delta_A2h) % p);
```

```
                if (A2h == 0)
                    A2h = 1;
                A2hn = (byte)((J1h + J2h + 2 * h1[s, u] + delta_A2hn) % p);
                if (A2hn == 0)
                    A2hn = 1;
                B2h = (byte)((K1h * K2h - 2 * h1[s, u]) % p);
                B2hn = (byte)((K1hn * K2hn - 2 * hn1[s, u]) % p);
                h2[s, u] = (byte)(-A2h * h1[s, u] * teskari((byte)(B2h + R * h1[s,
u])) % p);
                if (h2[s, u] == 0)
                    h2[s, u] = (byte)((A2h + B2h) % p);
                h[s, u] = (byte)(-A2h * h2[s, u] * teskari((byte)(B2h + R * h2[s, u]))
% p);
                hn2[s, u] = (byte)(-A2hn * hn1[s, u] * teskari((byte)(B2hn + R *
hn1[s, u])) % p);
                if (hn2[s, u] == 0)
                    hn2[s, u] = (byte)((A2hn + B2hn) % p);
                hn[s, u] = (byte)(-A2hn * hn2[s, u] * teskari((byte)(B2hn + R *
hn2[s, u])) % p);
            }
        }
        //-------------------------------------------------------------------------------
        private byte bo(byte f)
        {
            f = (byte)(f & 240);
            f = (byte)(f / 16);
            return f;
        }
        //------------------------------


//Kutubxonadan foydalasnish

using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
```

```
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using CryptoCore.Xeshlash;

namespace UzbCrypto
{
   public partial class Form1 : Form
   {
      public Form1()
      {
         InitializeComponent();
      }

      private void btnLink_Click(object sender, EventArgs e)
      {

         openFileDialog1.ShowDialog();
         txtLink.Text = openFileDialog1.FileName;
      }

      private void btnHashing_Click(object sender, EventArgs e)
      {
         UZDSt1106_2009_alg1 hash1 = new UZDSt1106_2009_alg1();
         if (!string.IsNullOrEmpty(txtLink.Text))
         {
            txtResult.Text = hash1.Xeshlash(txtLink.Text);
         }
      }

      private void label1_Click(object sender, EventArgs e)
      {

      }
   }
}
```