AES ALGORITMIDA KALITLARNI GENERATSIYALASH VA SHIFRLASHNI VIZUALIZATSIYA QILUVCHI WEB-ILOVA ISHLAB CHIQISH

Salayev Alisher Kuralbayevich[1], Po'latov Valijon Dilmurod o'g'li[1]

[1]Abu Rayhon Beruniy Nomidagi Urganch davlat universiteti,
E-mail valijonpolatov11@gmail.com

K E Y W O R D S

AES, shifrlash vizualizatsiyasi, JavaScript, axborot xavfsizligi, ECB/CBC/CTR, S-box, interaktiv ta'lim

A B S T R A C T

Mazkur maqolada AES (Advanced Encryption Standard) simmetrik shifrlash algoritmini interaktiv tarzda o'rganish va qo'llash imkonini beruvchi zamonaviy web-ilova ishlab chiqish jarayoni batafsil bayon etilgan. Axborot xavfsizligi sohasida kriptografik algoritmlarni chuqur tushunish bugungi kunda muhim ahamiyat kasb etmoqda. Biroq ta'lim jarayonida AES kabi murakkab algoritmlarni o'qitish ko'pincha qiyinchiliklar tug'diradi, chunki SubBytes, ShiftRows, MixColumns kabi operatsiyalar ko'p o'quvchilar uchun mavhum tushunchalar bo'lib qolaveradi. Ushbu muammoni hal qilish maqsadida Next.js (React), TypeScript, Tailwind CSS va CryptoJS asosida qurilgan interaktiv web-ilova taqdim etiladi. Ilova ECB, CBC va CTR ish rejimlarini, AES-128/192/256 kalit uzunliklarini, PKCS#7 va ANSI X.923 to'ldirish usullarini, shuningdek, Base64, Hexadecimal va Binary chiqish formatlarini qo'llab-quvvatlaydi. Foydalanuvchi interfeysi shifrlash jarayonini bosqichma-bosqich vizualizatsiya qiladi, S-box jadvalini interaktiv ko'rsatadi va kalit generatsiyasini real vaqtda namoyon etadi. Ilovaning kriptografik qismi CryptoJS kutubxonasi orqali amalga oshirilgan bo'lib, Next.js (React) asosidagi frontend arxitekturasi tez va barqaror ishlashni ta'minlaydi. Ilova zamonaviy brauzerlarda qo'llash uchun ishlab chiqilib, asosiy funksiyalari amaliy tekshiruvlar bilan baholangan. Maqolada ilovaning funksional imkoniyatlari, sinov natijalari va kelgusidagi rivojlantirish yo'nalishlari ham muhokama qilinadi.

I. KIRISH

Zamonaviy axborot xavfsizligi sohasida kriptografik algoritmlarni nafaqat qo'llash, balki ularning ishlash mexanizmlarini chuqur tushunish ham muhim ahamiyat kasb etadi. Ta'lim muassasalarida va mustaqil o'rganishda kriptografiya kurslarini o'qitish ko'pincha murakkab matematikaviy tushunchalar bilan to'qnashuvni taqozo etadi[1]. Dunyo bo'ylab internet trafigining katta qismi shifrlangan holda uzatiladi va turli xil axborot tizimlari foydalanuvchi ma'lumotlarini himoya qilish uchun kriptografik protokollarga tayanadi. Shu bois kriptografiyani o'rganish nafaqat mutaxassislar, balki har bir axborot texnologiyalari sohasidagi mutaxassis uchun muhim ko'nikma hisoblanadi[1].

AES (Advanced Encryption Standard) 2001-yilda NIST tomonidan rasmiy standart sifatida tasdiqlangan va bugungi kunda dunyo bo'ylab eng keng qo'llaniladigan simmetrik shifrlash algoritmidir. U bank tizimlari, HTTPS protokoli, fayllarni shifrlash va boshqa yuzlab muhim sohalarda qo'llaniladi[2]. AES Rijndael algoritmi asosida ishlab chiqilgan bo'lib, 128, 192 va 256 bitli kalit uzunliklarini qo'llab-quvvatlaydi. Algoritm 128 bitli blok o'lchami bilan ishlaydi va shifrlash uchun 10, 12 yoki 14 ta raund bajaradi. Uning kriptografik mustahkamligi va ishlash tezligi boshqa algoritmlar bilan solishtirganda yuqori ekanligi NIST tomonidan o'tkazilgan keng ko'lamli tekshiruvlar orqali tasdiqlangan[2].

Biroq algoritmni o'rganuvchilar uchun SubBytes, ShiftRows, MixColumns kabi

© A.K. Salayev, V.D. Po'latov

operatsiyalar ko‘pincha mavhum tushunchalar bo‘lib qoladi. Vizualizatsiya vositalari bu muammoni hal qilishda samarali usul hisoblanadi. Web-texnologiyalar esa bunday vositalarni maxsus o‘rnatmasdan, brauzer orqali foydalanish imkonini beradi[3]. Mavjud o‘quv resurslari ko‘pincha faqat matn va formulalar asosida tushuntirishlar beradi. Bunday yondashuv algoritmning abstrakt mohiyatini yanada murakkablashtiradi. Shu sababli interaktiv vizualizatsiya vositalariga bo‘lgan ehtiyoj yil sayin ortib bormoqda[3]. Zamonaviy brauzer texnologiyalari esa bunday vositalarni qulay tarzda qo‘llash imkonini beradi.

Ushbu maqolada taqdim etilgan web-ilova foydalanuvchiga quyidagilarni interaktiv, bosqichma-bosqich bajarish imkonini beradi. Bundan tashqari, ilova axborot xavfsizligi bo‘yicha kurs o‘tuvchi o‘qituvchilar uchun ham samarali demonstratsiya vositasi bo‘lib xizmat qilishi mumkin. Hozirda mavjud o‘xshash vositalar asosan ingliz tilida bo‘lib, mahalliy tilda interaktiv kriptografiya o‘quv platformalari juda kam.

- Turli kalit uzunliklari (AES-128/192/256) bilan shifrlash va deshifrlash
- ECB, CBC va CTR ish rejimlarini solishtirish
- PKCS#7, ANSI X.923 va None to'ldirish usullarini qo'llash
- Base64, Hexadecimal va Binary chiqish formatlarini ko'rish
- S-box jadvalini interaktiv tarzda o'rganish
- Shifrlash jarayonini animatsiya ko'rinishida kuzatish

II. ASOSIY QISM

1-bosqich. Dasturda qo‘llanilgan texnologiyalar va vositalar

Ilova Next.js (React) asosida ishlab chiqilgan bo‘lib, AES hisob-kitoblari va vizualizatsiya jarayonlarining asosiy qismi foydalanuvchi brauzerida bajariladi. Shu sababli foydalanuvchi bilan interaktiv ishlash tezligi yuqori bo‘ladi, server tomoni esa asosan sahifa va statik resurslarni yetkazib berish hamda deploy infratuzilmasini ta’minlash vazifasini bajaradi. Bunday yondashuv server yukini kamaytiradi va ilovani kengaytirishni soddalashtiradi.

1-jadval.

Ilovada qo'llaniladigan texnologiyalar steki

Texnologiya	Vazifasi
HTML5	Sahifa strukturasi va semantik belgilash
CSS3	Dizayn, responsiv joylashuv, animatsiya
JavaScript (ES)	AES logikasi va UI interaktivligi
Next.js	Frontend framework, routing
React + ReactDOM	Komponentli UI va state boshqaruvi
TypeScript	Tip xavfsizligi, xatoni oldindan kamaytirish
CryptoJS	AES shifrlash/deshifrlash, formatlar, IV generatsiya
Tailwind CSS	Tez va responsiv UI stilizatsiyasi
PostCSS + Autoprefixer	CSS preprocessing va brauzer prefikslari

CryptoJS JavaScript uchun kriptografik kutubxona bo‘lib, AES, DES, Triple DES, RC4, MD5, SHA-1, SHA-256 kabi algoritmlarni qo‘llab-quvvatlaydi[4]. Ushbu loyihada CryptoJS AES shifrlash va deshifrlash natijalarini referens tarzda tekshirish uchun qo‘llanadi. Ya’ni ilovada bosqichma-bosqich vizual hisoblashlar alohida ko‘rsatiladi, yakuniy natija esa CryptoJS orqali qayta olinib solishtiriladi.

Kutubxona loyihaga npm orqali ulangan. Amaliy jarayonda kalit Hex formatdan WordArray formatiga o‘tkaziladi. CBC va CTR rejimlarida IV foydalanuvchi tomonidan berilishi yoki avtomatik ravishda 16 baytli tasodifiy qiymat sifatida yaratilishi mumkin. To‘ldirish usullari sifatida PKCS7, ANSI X.923 va NoPadding variantlari qo‘llanadi. Shifrlash natijasi birlamchi ko‘rinishda Base64 formatda olinadi, so‘ngra Hex va Binary ko‘rinishlarga ham konvertatsiya qilinadi.

Quyida dasturdagi realAesEncrypt funksiyasidan AES-CBC uchun mos kod fragmenti keltirilgan:

(cc) BY © A.K. Salayev, V.D. Po‘latov

```
const keyWordArray = CryptoJS.enc.Hex.parse(keyHex);
let iv;
if (ivString) {
  iv = CryptoJS.enc.Hex.parse(ivString.replace(/\s/g, ''));
} else {
  iv = CryptoJS.lib.WordArray.random(16);
}
const modeOption = {
  mode: CryptoJS.mode.CBC,
  iv: iv,
  ...paddingOption
};
const encrypted = CryptoJS.AES.encrypt(plaintext, keyWordArray, modeOption);
const base64Output = encrypted.toString();
```

1-rasm. CryptoJS yordamida AES-CBC shifrlash

2-bosqich. Ilovaning funksional imkoniyatlari va foydalanuvchi interfeysi.

Ilova foydalanuvchiga bir sahifali interaktiv interfeys orqali AES algoritmining asosiy amallarini boshqarish va natijalarni bosqichma-bosqich kuzatish imkonini beradi. Foydalanuvchi kalit uzunligi, rejim, padding, chiqish formati va kalit kiritish usulini tanlaydi; tizim esa shifrlash/deshifrlash natijasi bilan birga vizual tushuntirishlarni ham taqdim etadi.

2-jadval.

Ilovaning funksional imkoniyatlari

Funksional soha	Parametrlar
Kalit uzunligi	AES-128, AES-192, AES-256
Shifrlash rejimlari	ECB, CBC, CTR
To'ldirish usullari	PKCS#7, ANSI X.923, None
Chiqish formatlari	Base64, Hex, Binary
Kalit kiritish	Hex, Matn, Random
Vizualizatsiya	Shifrlash bosqichlari, kalit generatsiyasi, S-box jadvali
Deshifrlash	Kiritilgan shifrlangan matn bo‘yicha

Ilovada uchta rejim qo‘llab-quvvatlanadi: ECB, CBC va CTR. Har bir rejim uchun jarayon bosqichma-bosqich vizual ko‘rsatiladi. Har bir rejim uchun ilovada vizual animatsiya va bosqichli ko‘rsatish imkoni mavjud.

ECB (Electronic Codebook) rejimida har bir 16 baytli blok mustaqil shifrlanadi va bloklar o‘rtasida bog‘lanish mavjud emas. Shu sababli bir xil ochiq matn bloklari bir xil shifrlangan bloklarni beradi; bu holat ma’lumot naqshlarini saqlab qolishi mumkin. Ilovada ECB rejimi asosan o‘quv va taqqoslash maqsadida ko‘rsatiladi.

CBC (Cipher Block Chaining) rejimida har bir blok shifrlashdan oldin oldingi shifrlangan blok bilan XOR qilinadi, birinchi blok esa IV bilan XOR qilinadi. Dasturda IV qiymati foydalanuvchi tomonidan berilishi yoki avtomatik tarzda generatsiya qilinishi mumkin. Bu yondashuv ECBga nisbatan yaxshiroq himoya beradi, chunki bir xil bloklar turli natijalar hosil qiladi.

CTR (Counter) rejimida ochiq matn to‘g‘ridan-to‘g‘ri blok sifatida shifrlanmaydi; avval nonce/counter bloki AES orqali shifrlanadi, so‘ng hosil bo‘lgan oqim ochiq matn bilan XOR qilinadi. Ilovada har bir keyingi blok uchun counter oshirib boriladi va natija bosqichma-bosqich aks ettiriladi. CTR rejimi amaliyotda yuqori unumdorlik va parallel hisoblash imkoniyati bilan ajralib turadi.

AES blokli shifrlash algoritmi bo‘lgani sababli kiruvchi ma’lumot 16 baytli bloklarga ajratiladi. Agar oxirgi blok to‘liq bo‘lmasa, ilovada quyidagi to‘ldirish usullari qo‘llanadi. To‘ldirish usulini to‘g‘ri tanlash shifrlash xavfsizligi va ma’lumotlarning to‘liq qayta tiklanishi uchun muhim ahamiyatga ega. Noto‘g‘ri padding ba’zan “padding oracle” hujumlariga yo‘l ochishi mumkin, shu bois amaliy tizimlarda PKCS#7 eng ko‘p tavsiya etiladigan usul hisoblanadi[3].

- PKCS7: yetishmayotgan baytlar soniga teng qiymat bilan to‘ldiriladi. Masalan, 3 bayt yetishmasa 03 03 03 qo‘shiladi.
- ANSI X.923: oxirgi baytga to‘ldirish uzunligi yoziladi, undan oldingi to‘ldirish baytlari 00 bilan to‘ldiriladi (masalan, 00 00 03).
- None: avtomatik padding qo‘llanmaydigan rejim sifatida tanlanadi; amaliy qo‘llashda ma’lumot uzunligi 16 baytga karrali bo‘lishi tavsiya etiladi. Ilovaning vizual hisoblash oqimida bloklarga ajratish uchun zarur bo‘lganda 00 bilan tekislash ishlatiladi.

Ilovadagi S-box bo‘limi AES algoritmining SubBytes bosqichini interaktiv tarzda tushuntirish uchun ishlab chiqilgan. S-box – 256 ta qiymatdan iborat almashtirish jadvali bo‘lib, har bir kirish baytiga mos chiqish baytini beradi[5]. Dasturda ushbu jadval 16×16 ko‘rinishda taqdim etiladi. S-box AES algoritmining yagona nolinear komponenti bo’lib, u kriptoanaliz hujumlariga qarshi asosiy himoya sifatida xizmat qiladi. Galois

(cc) BY © A.K. Salayev, V.D. Po‘latov

maydoni GF(2^8) da multiplikativ inversiya va affin transformatsiya operatsiyalari birlashtirib S-box qiymatlarini hosil qiladi[5]. Vizualizatsiya orqali talabalar ushbu matematik operatsiyalarning amaliy natijasini ko’rishlari mumkin.

Foydalanuvchi S-box bilan ikki usulda ishlashi mumkin:

1. Hex qiymat kiritish orqali (AB kabi) mos qator va ustunni topish;
2. Jadvaldagi kataklarni bosish/hover qilish orqali kirish va chiqish qiymatini ko‘rish.

Interfeysda kirish baytining yuqori 4 biti qatorni, quyi 4 biti ustunni bildiradi; mos kesishma katagi ajratib ko‘rsatiladi. Tanlangan qiymat uchun S-box[row][col] = output natijasi alohida chiqariladi. Shuningdek, shifrlashning SubBytes bosqichida matritsadagi bayt bosilganda shu baytning S-box jadvalidan qanday olingani vizual ravishda ko‘rsatiladi.

3-bosqich. Dastur arxitekturasi va asosiy dasturiy modullar

Ilovada kalit bilan ishlash uchta usulda amalga oshiriladi: Random, Hex va Matn. Bu yondashuv foydalanuvchiga kalit uzunligi va kiritish formatlari bilan ishlash haqida amaliy tasavvur beradi. Random kalit generatsiyasida JavaScript asosidagi tasodifiy son generatoridan foydalaniladi.

Random usulida kalit uzunligiga qarab (AES-128/192/256) mos ravishda 16/24/32 baytli kalit yaratiladi. Joriy implementatsiyada tasodifiy baytlar Math.random() asosida hosil qilinadi va keyin Hex ko‘rinishga o‘tkazilib interfeysda ko‘rsatiladi. Hex va Matn usullarida esa foydalanuvchi kiritgan qiymat tanlangan kalit uzunligiga moslashtiriladi. Ilovada kalit vizualizatsiyasi foydalanuvchiga har bir baytni alohida ko‘rish va ularning hexadecimal qiymatlarini real vaqtda kuzatish imkonini beradi. Bu kalit uzunligi va bit soni o‘rtasidagi bog‘liqlikni aniq ko‘rsatadi.

```
export const generateRandomKey = (keyLength: KeyLength = KeyLength.AES_128): number[] => {
  const keyBytes = getKeyBytesLength(keyLength);
  const bytes = [];
  for (let i = 0; i < keyBytes; i++) {
    bytes.push(Math.floor(Math.random() * 256));
  }
  return bytes;
};
```

2-rasm. Kriptografik xavfsiz kalit generatsiyasi.

Shifrlash yakunlangach, natija foydalanuvchi tanlagan formatga mos ko‘rinishda chiqariladi. Dasturda bu jarayon realAesEncrypt funksiyasi ichida bajariladi: avval birlamchi natija Base64 ko‘rinishda olinadi, so‘ng u Hex va Binary formatlarga konvertatsiya qilinadi. Natijada interfeysda bir vaqtning o‘zida uchala format ham taqdim etiladi. Base64 format Internet protokollarida keng qo‘llaniladi va ma’lumotlarni matn ko‘rinishida uzatish uchun qulay. Hexadecimal format esa kriptografiya sohasida standart hisoblangan bo‘lib, har bir baytni ikki xonali hex raqam sifatida ifodalaydi. Binary format esa algoritmning past darajadagi operatsiyalarini o‘rganuvchilar uchun ayniqsa foydali, chunki XOR va boshqa bit-darajadagi amallarni bevosita kuzatish imkonini beradi[6].

Binary ko‘rinishni olishda Hex satr juftliklarga ajratilib, har bir bayt 8 bitli binar satrga o‘tkaziladi. Ushbu yondashuv formatlar o‘rtasida izchil va tekshirishga qulay natija beradi.

```
const base64Output = encrypted.toString();
const cipherParams = CryptoJS.lib.CipherParams.create({
  ciphertext: CryptoJS.enc.Base64.parse(base64Output)
});
const hexOutput = CryptoJS.format.Hex.stringify(cipherParams);
const hexBytes = hexOutput.match(/.{2}/g)!.map(hex => parseInt(hex, 16));
const binaryOutput = bytesToBinary(hexBytes, ' ');
let primaryOutput: string;
switch (outputFormat) {
  case OutputFormat.HEX:
    primaryOutput = hexOutput;
    break;
  case OutputFormat.BINARY:
    primaryOutput = binaryOutput;
    break;
  default:
    primaryOutput = base64Output;
    break;
}
```

3-rasm. Natijani formatlash funksiyasi

4-bosqich. Shifrlash jarayonini vizual ko‘rsatish.

Ilovaning asosiy afzalliklaridan biri shifrlash jarayonini interaktiv, qadamma-qadam ko‘rsatishidir. Foydalanuvchi shifrlashni ishga tushirgandan so‘ng vizualizatsiya bo‘limida quyidagi bosqichlar aks ettiriladi. Har bir bosqich alohida panel ko‘rinishida taqdim etilib, foydalanuvchi “Keyingi” tugmasini bosib algoritmning keyingi amalini kuzatishi mumkin. Bu interaktiv yondashuv o‘quvchilarga AES algoritmini qadamma-qadam o‘rganish va har bir operatsiyaning natijasini real vaqtda ko‘rish imkonini beradi[5].

(cc) BY © A.K. Salayev, V.D. Po‘latov

1. Ochiq matnning baytlarga ajratilishi va 4×4 holat matritsasiga joylashtirilishi.
2. AddRoundKey – boshlang‘ich kalit bilan XOR amali.
3. Har bir raund uchun SubBytes, ShiftRows, MixColumns, AddRoundKey ketma-ketligi.
4. Yakuniy raundda MixColumns bajarilmasligi.
5. Rejimga bog‘liq qo‘shimcha bosqichlar: CBCda IV/oldingi blok bilan XOR, CTRda counter shifrlanib ochiq matn bilan XOR qilinishi.
6. Yakuniy shifrlangan natijaning Base64, Hex va Binary formatlarda chiqarilishi.

Ilovada S-box jadvali to‘liq 16×16 interaktiv ko‘rinishda berilgan. Foydalanuvchi hex bayt qiymatini kiritishi yoki jadvaldan katak tanlashi mumkin; natijada mos qator, ustun va chiqish qiymati ajratib ko‘rsatiladi. Shifrlashdagi SubBytes bosqichida tanlangan bayt uchun S-box lookup jarayoni alohida vizual blokda ko‘rsatiladi. Bunday vizual yondashuv S-box tuzilishini tushunishni sezilarli osonlashtiradi va talabalar uchun GF(2^8) maydoni ustida bajariladigan matematik operatsiyalarni intuitiv ravishda idrok etishga yordam beradi.

S-box qiymatlari AES standarti bo‘yicha tayyor jadvaldan olinadi; ya’ni ilovada GF(2^8) inversiya va affinn transformatsiya formulalari hisoblab qurilmaydi, balki ularning standart natijasi amaliy ko‘rinishda ishlatiladi[6].

III. TAJRIBALAR VA NATIJALAR

A. Shifrlash to'g'riligi tekshirish

Ilovadagi AES hisoblash natijalari ikki yo‘l bilan tekshirildi. Qo‘shimcha ravishda, turli kalit uzunliklari, rejimlar va kirish formatlari bo‘yicha natijalar o‘zaro solishtirildi. Bu ilovaning funksional barqarorligini va parametrlar bo‘yicha izchilligini baholash imkonini berdi.

1. Ilovaning bosqichma-bosqich vizual hisoblash natijasi;
2. CryptoJS asosidagi referens natija.

Bir xil kalit, rejim, IV va matn uchun natijalar mos chiqdi. Shuningdek, NIST (FIPS 197) vektori asosida ECB holati ham tekshirilib, moslik tasdiqlandi. Sinovlarda D(K, E(K, M)) = M sharti bajarildi.

4-jadval.

Shifrlash to'g'riligi sinov natijalari

Sinov holati	Kalit	Rejim	Natija
Standart matn	AES-128	CBC	Mos
Bo'sh matn	AES-128	ECB	Mos
Unicode matn	AES-256	CTR	Mos
NIST test vektori	AES-128	ECB	Mos

B. Ishlash unumdorligi natijalari

CryptoJS asosidagi shifrlash tezligi brauzer muhitida (Chrome 120+, Windows 11 Pro, Intel Core i5-12450, 16 GB RAM) turli hajmdagi ma’lumotlar uchun o‘lchandi. Sinovlarda CBC rejimi qo‘llanildi.

5-jadval.

JavaScript (CryptoJS) shifrlash tezligi

Ma'lumot hajmi	AES-128 (ms)	AES-256 (ms)	Rejim
100 bayt	< 1	< 1	CBC
10 KB	1.2	1.5	CBC
1 MB	42	54	CBC
10 MB	418	537	CBC

IV. XULOSA

Tadqiqot doirasida AES algoritmini o‘rganish va amaliy sinash uchun qulay, funksional hamda interaktiv vizualizatsiya dasturi ishlab chiqildi. Dasturda foydalanuvchi bir tomondan shifrlash/deshifrlash natijasini oladi, ikkinchi tomondan esa algoritmning ichki bosqichlarini interaktiv tarzda kuzatadi. Olib borilgan amaliy tekshiruvlar shuni ko‘rsatadiki, ilova AES bo‘yicha ko‘rib chiqilgan ish rejimlari va test holatlarida barqaror natija beradi. Shu bilan birga, loyiha modulli tuzilishda ishlab chiqilgani sababli uni keyinchalik turli ehtiyojlarga moslashtirish mumkin. Bu yondashuv nazariy bilimni amaliy jarayon bilan bog‘lashga yordam beradi.

Ilovaning asosiy yutuqlari quyidagilardan iborat:

1. ECB, CBC, CTR rejimlarini qo‘llash va taqqoslash imkoniyati;
2. Kalit bilan ishlashning uch usuli: Hex, Matn va Random generatsiya;

(cc) BY © A.K. Salayev, V.D. Po‘latov

3. AES-128/192/256 kalit uzunliklarini qo‘llab-quvvatlash;
4. S-box jadvali mexanizmi orqali SubBytes bosqichini vizual o‘rganish;
5. Shifrlash jarayonining bosqichma-bosqich (AddRoundKey, SubBytes, ShiftRows, MixColumns) ko‘rsatilishi;
6. Natijani Base64, Hex, Binary formatlarda chiqarish;
7. Zamonaviy brauzerlarda barqaror ishlashi.

Kelgusida ilovani quyidagi yo‘nalishlarda rivojlantirish maqsadga muvofiq: fayl shifrlash/deshifrlash modulini qo‘shish, autentifikatsiyalangan rejimlarni kiritish, RSA kabi asimmetrik algoritmlar bilan kengaytirish, ko‘p tilli interfeysni rivojlantirish (o‘zbek, ingliz, rus), shifrlash zanjirining yanada to‘liq animatsion ko‘rinishini yaratish va ta’limiy test/reyting modulini joriy etish.

ADABIYOTLAR

1. Daemen J., Rijmen V. (2002). The Design of Rijndael: AES – The Advanced Encryption Standard. Springer-Verlag, Berlin Heidelberg.
2. NIST FIPS 197 (2001). Advanced Encryption Standard (AES). National Institute of Standards and Technology, U.S. Department of Commerce.
3. Stallings W. (2017). Cryptography and Network Security: Principles and Practice. 7th Edition. Pearson Education Limited.
4. CryptoJS (2023). JavaScript implementations of standard and secure cryptographic algorithms.
5. Daemen J., Rijmen V. (1999). AES Proposal: Rijndael. Version 2. AES Algorithm Submission, September 3, 1999.
6. Ferguson N., Schneier B., Kohno T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley Publishing.
7. W3C Web Cryptography API (2017).
8. Xolmatov B., Narzullayev O., "O‘zbekistonda axborot xavfsizligi tizimini rivojlantirish istiqbollari," RTvaSI jurnali, 2023, 2-son, 45–52-betlar.
9. Menezes A.J., van Oorschot P.C., Vanstone S.A. (1996). Handbook of Applied Cryptography. CRC Press.
10. Mozilla Developer Network (2024). Web Crypto API — SubtleCrypto interface.

© A.K. Salayev, V.D. Po‘latov