“ZAMONAVIY RAQAMLI INFRATUZILMALARDA MA’LUMOTLAR XAVFSIZLIGINI TA’MINLASH VA RSA ALGORITMINING AHAMIYATI”

Rizoqulova Marjonabonu Zokirovna
Buxoro Davlar Texnika Universitet 2 bosqich talabasi

Annotatsiya: Ushbu maqola zamonaviy raqamli infratuzilmalarda axborot xavfsizligini ta'minlashning dolzarb muammolarini va ushbu jarayonda assimetrik kriptografiyaning, xususan, RSA (Rivest-Shamir-Adleman) algoritmining tutgan o‘rnini tadqiq etadi. Maqolada kiberhujumlar sonining ortishi sharoitida ma'lumotlar maxfiyligi, butunligi va foydalanish imkoniyatini ta'minlash (CIA modeli) tahlil qilinadi. Tadqiqot doirasida RSA algoritmining matematik asoslari, uning tub sonlar nazariyasiga tayangan holda kalitlar generatsiyasi hamda shifrlash-deshifrlash mexanizmlari yoritib beriladi. Shuningdek, zamonaviy hisoblash quvvatlari rivojlanishi hamda kvant kompyuterlarining paydo bo‘lishi fonida RSA algoritmining zaifliklari va unga nisbatan tahdidlar tanqidiy baholanadi. Ish yakunida post-kvant kriptografiyasiga o‘tish zarurati va algoritmni xavfsiz joriy etish bo‘yicha amaliy tavsiyalar keltiriladi.

Kalit so‘zlar: Kiberxavfsizlik, RSA algoritmi, assimetrik kriptografiya, ma’lumotlar maxfiyligi, raqamli infratuzilma, butun sonlarni ko‘paytuvchilarga ajratish, kvant tahdidlari.

Kirish

XXI asr insoniyat taraqqiyoti tarixida raqamli transformatsiya davri sifatida muhrlanmoqda. Ma’lumotlar bugungi kunda "yangi asr nefti" deb ta’riflanayotgan bo‘lsa, ushbu ma’lumotlarni saqlash, uzatish va qayta ishlash infratuzilmalari jamiyat va davlat barqarorligining tayanch nuqtalariga aylandi. Biroq, texnologik rivojlanishning yuqori sur’atlari bilan bir qatorda, kiberxavfsizlikka bo‘lgan tahdidlarning murakkabligi va ko‘lami ham eksponentsial tarzda o‘sib bormoqda. Bugungi kunda har qanday raqamli tizim — bank tizimidan tortib, davlat boshqaruvi va shaxsiy kommunikatsiyalargacha — doimiy hujumlar nishonida turibdi.

Axborot xavfsizligining fundamental negizi bo‘lgan CIA modeli (Confidentiality, Integrity, Availability — Maxfiylik, Butunlik va Foydalanish imkoniyati) raqamli infratuzilmalarning sog‘lom ishlashini ta’minlashda yetakchi o‘rin tutadi. Ushbu modelni hayotga tatbiq etishda kriptografik usullar hal qiluvchi ahamiyatga ega. Ayniqsa, internet tarmog‘i orqali uzatilayotgan ma’lumotlarning himoyalanganligini ta’minlash, taraflar o‘rtasida xavfsiz kalit almashinuvini amalga oshirish masalasi kriptografiya fanining markaziy muammolaridan biri hisoblanadi.

Ushbu jarayonda RSA (Rivest-Shamir-Adleman) algoritmi o‘zining assimetrik shifrlash tamoyillari bilan raqamli davrning "tayanch ustuniga" aylandi. 1977-yilda taklif etilgan ushbu algoritmi bugungi kunda nafaqat elektron tijorat va raqamli imzolar tizimida, balki internetning xavfsiz ulanish protokollari (TLS/SSL) negizida ham asosiy texnologiya

bo‘lib xizmat qilmoqda. RSA ning ahamiyati shundaki, u ma’lumotlarni uzatishda oldindan kelishilgan maxfiy kalitga bo‘lgan ehtiyojni bartaraf etdi va ochiq kalitli kriptografiya (Public Key Cryptography) davrini boshlab berdi.

Ushbu maqolaning maqsadi — RSA algoritmining matematik mohiyatini tahlil qilish, uning zamonaviy raqamli infratuzilmalardagi o‘rnini baholash hamda kvant kompyuterlari davrida algoritmni kutayotgan istiqbol va tahdidlarni o‘rganishdan iborat. Shuningdek, ma’lumotlar xavfsizligini ta’minlashda RSA dan foydalanishning optimal usullari va tizim xavfsizligini mustahkamlashga qaratilgan amaliy takliflar keltirib o‘tiladi. Raqamli infratuzilmalarning himoyasi nafaqat texnik yechimlar, balki xavfsizlik nazariyasini chuqur anglashni talab qiladi; ushbu tadqiqot aynan shu nazariy va amaliy ko‘prikni shakllantirishga xizmat qiladi.

Axborot xavfsizligi asoslari va CIA triadasi

Zamonaviy raqamli infratuzilmalarni loyihalashda xavfsizlik shunchaki "qo‘shimcha funksiya" emas, balki tizim arxitekturasining ajralmas qismi hisoblanadi. Axborot xavfsizligini ta’minlashning fundamental yondashuvi **CIA modeli** (yoki CIA triadasi) bo‘lib, u istalgan axborot tizimining himoyalanganlik darajasini o‘lchashda standart mezon vazifasini o‘taydi.

Maxfiylik (Confidentiality)

Maxfiylik deganda ma’lumotlarga faqat ruxsat berilgan subyektlar (shaxslar, jarayonlar yoki qurilmalar) kira olishi tushuniladi. Raqamli infratuzilmada bu ma’lumotlarning tarmoq orqali uzatilishida uchinchi shaxslar tomonidan tutilib qolishini yoki o‘qilishini oldini olishni anglatadi. RSA kabi assimetrik shifrlash algoritmlari aynan shu maqsadga erishishda, ya’ni uzatilayotgan axborotni ochiq kanallarda "o‘qib bo‘lmas" holatga keltirishda qo‘llaniladi.

Butunlik (Integrity)

Ma’lumotlar uzatish jarayonida yoki saqlash vaqtida ruxsatsiz o‘zgartirilmasligini ta’minlash — butunlikning asosiy vazifasidir. Agar hujumchi ma’lumotlar paketini ushlab qolib, uning tarkibiga o‘zgartirish kiritsa, tizim butunligi buziladi. Kriptografik xesh-funksiyalar va raqamli imzolar yordamida ma’lumotning o‘zgartirilmaganligini tekshirish imkoniyati yaratiladi. RSA algoritmi nafaqat shifrlash, balki raqamli imzo yaratishda ham muvaffaqiyatli ishlatiladi, bu esa xabarning haqiqiyligini (authenticity) kafolatlaydi.

Foydalanish imkoniyati (Availability)

Foydalanish imkoniyati tizim va ma’lumotlar vakolatli foydalanuvchilar uchun zarur bo‘lganda doimo ochiq bo‘lishini ta’minlaydi. Garchi kriptografiya asosan maxfiylik va butunlikka qaratilgan bo‘lsa-da, noto‘g‘ri yoki sekin ishlovchi shifrlash mexanizmlari tizim resurslarini haddan tashqari ko‘p sarflab, xizmat ko‘rsatishdan bosh tortish (DoS/DDoS) hujumlariga o‘xshash oqibatlarga olib kelishi mumkin. Shuning uchun, samarali va optimallashtirilgan algoritmlarni tanlash xavfsizlik siyosatining tarkibiy qismidir.

Kriptografik talablar

Raqamli infratuzilmalarda ushbu uchlikni amalga oshirish uchun quyidagi kriptografik vositalar qo‘llaniladi:

Simmetrik shifrlash:

Ma’lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalanadi (masalan, AES). Bu tezkor, lekin kalitni xavfsiz yetkazib berish muammosiga ega.

Assimetrik shifrlash (RSA):

Ochiq (public) va yopiq (private) kalitlar juftligidan foydalanadi. Bu kalit almashinuvi muammosini hal qiladi va infratuzilmaning masshtabli ishlashiga imkon beradi.

Kriptografiya turlari: Simmetrik va Assimetrik yondashuvlar

Raqamli xavfsizlik arxitekturasida ma'lumotlarni himoyalashning ikki asosiy usuli mavjud: simmetrik va assimetrik shifrlash. Ularning har biri o‘ziga xos afzallik va kamchiliklarga ega bo‘lib, zamonaviy tizimlarda ular ko‘pincha gibrid tarzda birgalikda qo‘llaniladi.

Simmetrik shifrlash (Private Key Cryptography)

Simmetrik shifrlashda ma’lumotni shifrlash va uni deshifrlash uchun **bitta umumiy kalitdan** foydalaniladi. Bu jarayon juda yuqori tezlikka ega bo‘lib, katta hajmdagi ma’lumotlarni qayta ishlash uchun juda qulay (masalan, AES – Advanced Encryption Standard).

Muammo:

Asosiy qiyinchilik — "kalitni tarqatish" (key distribution) muammosi. Agar ikkita tomon bir-biridan minglab kilometr uzoqlikda bo‘lsa, ular o‘zlarining maxfiy kalitlarini qanday qilib xavfsiz almashishlari mumkin? Agar kalitni ochiq kanal orqali yuborsalar, uni hujumchi ushlab olishi va barcha xabarlarni o‘qishi mumkin.

Assimetrik shifrlash (Public Key Cryptography)

1970-yillarda yaratilgan assimetrik shifrlash ushbu "kalit almashinuvi" muammosini hal qildi. Bu tizimda har bir foydalanuvchida **kalitlar juftligi** mavjud:

Ochiq kalit (Public Key):

Bu kalit hammaga ma’lum bo‘lishi mumkin. U ma’lumotni shifrlash uchun ishlatiladi.

Yopiq kalit (Private Key):

Bu kalit faqat egasiga ma’lum bo‘lib, faqat u orqali shifrlangan ma’lumotni ochish (deshifrlash) mumkin.

Nima uchun simmetrik shifrlash yetarli emas?

Simmetrik shifrlash tez bo‘lgani bilan, uni keng ko‘lamli tarmoqlarda (masalan, Internetda) mustaqil qo‘llash imkonsiz. Tasavvur qiling, millionlab foydalanuvchilar bir-biri bilan xavfsiz bog‘lanishi kerak. Agar har bir juftlik uchun alohida kalit yaratilsa, kalitlarni boshqarish murakkablashib ketadi.

Gibrid tizimning yechimi:

Zamonaviy raqamli infratuzilmalarda (HTTPS/TLS protokollarida) quyidagi gibrid sxema qo‘llaniladi:

Bosqich 1:

Tomonlar RSA (assimetrik shifrlash) yordamida o‘zaro xavfsiz simmetrik kalitni almashadilar.

Bosqich 2:

Kalit almashinilgandan so‘ng, haqiqiy ma’lumotlar almashinuvi (katta fayllar, video, ovoz) juda tez ishlaydigan **simmetrik shifrlash** (AES) orqali amalga oshiriladi.

RSA algoritmi: Nazariy negiz va matematik asoslar

RSA (Rivest-Shamir-Adleman) algoritmining qudrati uning murakkab matematik funksiyalarga, xususan, **tub sonlar nazariyasiga** asoslanganligidadir. Uning xavfsizligi juda katta sonlarni ko‘paytuvchilarga ajratishning (Integer Factorization) hisoblash jihatidan o‘ta murakkabligiga tayanadi.

Kalit generatsiya jarayoni

RSA tizimini yaratish uchun quyidagi qadamlar amalga oshiriladi:

1. **Ikkita katta tub sonni tanlash:** Ikkita tasodifiy juda katta tub son tanlanadi: p va q.

2. **Modulni hisoblash:** n = p \times q hisoblanadi. Bu son n ham ochiq, ham yopiq kalitning bir qismi bo‘ladi.

3. **Eyler funksiyasini hisoblash:** \phi(n) = (p-1) \times (q-1) qiymati aniqlanadi.

4. **Ochiq eksponentani tanlash (e):** Shunday e soni tanlanadiki, bunda 1 < e < \phi(n) va e hamda \phi(n) o‘zaro tub bo‘lishi kerak (ya’ni, gcd(e, \phi(n)) = 1).

5. **Yopiq eksponentani hisoblash (**d**):** Shunday d soni topiladiki, u quyidagi shartni qanoatlantiradi: d \times e \equiv 1 \pmod{\phi(n)}.

Ochiq kalit: (n, e)

Yopiq kalit: (n, d)

Shifrlash va deshifrlash mexanizmi

Xabar M (raqamli ko‘rinishda) quyidagi tarzda shifrlanadi:

Bu yerda C – shifrlangan xabar (ciphertext). Uni faqat yopiq kalit egasi deshifrlashi mumkin:

Matematik murakkablikning mohiyati

RSA algoritmining xavfsizligi shundaki, hujumchi ochiq kalit (n, e) ni bilgan taqdirda ham, d (yopiq kalit) ni topishi uchun n sonini p va q ko‘paytuvchilariga ajratishi kerak.

Agar n juda katta bo‘lsa (masalan, 2048 yoki 4096 bit), bugungi kundagi eng kuchli superkompyuterlar ham bu sonni ko‘paytuvchilarga ajratish uchun milliardlab yillar sarflashi kerak.

Bu "bir tomonlama funksiya" (one-way function) deb ataladi: ko‘paytirish oson, lekin teskari jarayon (bo‘lish/ajratish) matematik jihatdan o‘ta og‘ir.

Nima uchun bu muhim?

RSA ning asosiy yutug‘i shundaki, u ikki tomon o‘rtasida hech qanday oldindan kelishilgan "maxfiy kanal" talab qilmaydi. Internetda ochiq kanal orqali ochiq kalitni

jo‘natish kifoya, va butun xavfsizlik o‘sha katta sonlarning faktorial qiyinchiligiga tayanadi.

RSA ning texnik xavfsizligi va kvant davridagi tahdidlar

RSA algoritmi o‘nlab yillar davomida kiberxavfsizlikning "oltin standarti" bo‘lib keldi, ammo texnologik taraqqiyot uning himoya qobig‘iga yangi talablar va xavflarni olib kelmoqda.

Butun sonlarni ko‘paytuvchilarga ajratish muammosi (Integer Factorization)

RSA xavfsizligi butunlay n sonini p va q tub ko‘paytuvchilariga ajratishning murakkabligiga bog‘liq. Klassik kompyuterlar uchun 2048-bitli sonni faktorial tahlil qilish imkonsiz vazifa hisoblanadi. Biroq, bu xavfsizlik "matematik qiyinchilik"ka asoslangan. Agar samaraliroq matematik usul (yoki hujum algoritmi) topilsa, RSA ning himoya darajasi keskin pasayadi.

Kvant kompyuterlari tahdidi: Shor algoritmi.

Kvant hisoblash texnologiyalari RSA uchun eng katta xavf hisoblanadi. **Shor algoritmi** deb nomlanuvchi kvant algoritmi katta sonlarni ko‘paytuvchilarga ajratish jarayonini eksponentsial darajada tezlashtirishi mumkin.

Klassik kompyuterlarda:

2048-bitli RSA kalitini yechish uchun milliardlab yillar ketishi mumkin.

Yetarli quvvatdagi kvant kompyuterida:

Shor algoritmi yordamida bu jarayon bir necha soat yoki hatto daqiqalar ichida amalga oshirilishi mumkin.

Bu shuni anglatadiki, bugungi kunda shifrlanib saqlanayotgan maxfiy ma'lumotlar ("hozir saqla, keyin yech" – *Store Now, Decrypt Later* strategiyasi) kelajakda kvant kompyuterlari mavjud bo‘lganda ochiq bo‘lib qolishi mumkin.

Implementatsiya xatolari

RSA ning zaifligi nafaqat uning matematik qismida, balki uni dasturiy ta'minotga noto‘g‘ri joriy etishda ham namoyon bo‘ladi:

Tasodifiy sonlar generatori (RNG):

Agar p va q ni tanlashda foydalaniladigan tasodifiy sonlar generatori yetarli darajada "tasodifiy" bo‘lmasa, hujumchi kalitni osonlikcha hisoblab topishi mumkin.

Side-channel hujumlar:

Kriptografik operatsiyalar bajarilayotganda qurilma iste'mol qiladigan elektr energiyasi yoki protsessor ishlash vaqtini tahlil qilish orqali yopiq kalitni "chaqib" olish imkoniyati mavjud.

Kelajak istiqbollari: Post-Kvant Kriptografiyasi (PQC)

RSA ning kvant kompyuterlari oldidagi ojizligi dunyo kriptografik standartlarini qayta ko‘rib chiqishga majbur qilmoqda. Hozirda **Post-kvant kriptografiyasi (PQC)** bo‘yicha tadqiqotlar faol olib borilmoqda.

Lattice-based cryptography (Panjaraga asoslangan kriptografiya):

Bu algoritmlar kvant hujumlariga qarshi tura oladigan matematik muammolarga asoslangan. NIST (AQSh Standartlar va Texnologiyalar Instituti) hozirda yangi standartlarni qabul qilish jarayonida.

Gibrid o‘tish davri:

Yaqin yillarda RSA ni to‘satdan bekor qilish o‘rniga, RSA va yangi post-kvant algoritmlarini birgalikda ishlatish (gibrid shifrlash) eng xavfsiz yechim sifatida ko‘rilmoqda.

RSA Algoritmining Raqamli Infratuzilmalardagi Amaliy O‘rni

Nazariy jihatdan kuchli bo‘lgan RSA amaliyotda qanday ishlaydi? Bugungi kunda global internet trafigining katta qismi aynan RSA arxitekturasiga tayanadi. Keling, uning asosiy qo‘llanilish sohalarini ko‘rib chiqamiz.

SSL/TLS Protokollari va Veb-Xavfsizlik

Har gal brauzer manzil qatorida "qulf" belgisi (HTTPS) paydo bo‘lganda, fonda RSA (yoki uning muqobillari) ishlayotgan bo‘ladi.

Jarayon:

Foydalanuvchi serverga ulanishni so‘raganda, server o‘zining raqamli sertifikatini (ochiq kalitini o‘z ichiga olgan) yuboradi. Brauzer bu kalit yordamida vaqtinchalik simmetrik "sessiya kaliti"ni shifrlaydi va serverga qaytaradi.

Ahamiyati:

Agar ushbu jarayonda RSA ishlatilmaganda edi, elektron tijorat (Amazon, eBay, mahalliy to'lov tizimlari) va onlayn banking mutlaqo imkonsiz bo‘lar edi. Chunki ochiq tarmoqda kredit karta ma'lumotlarini ishonchli himoya qilib bo'lmasdi.

Raqamli Imzolar (Digital Signatures)

RSA nafaqat ma'lumotni shifrlash, balki uning kimdan kelganligini va o'zgartirilmaganligini tasdiqlash uchun ham xizmat qiladi. Raqamli imzo an'anaviy imzoning raqamli va ancha xavfsiz ekvivalentidir.

Mexanizm qanday ishlaydi?

Jo‘natuvchi xabarning "xeshini" (qisqartirilgan barmoq izini) o‘zining **yopiq kaliti** (private key) bilan shifrlaydi. Buni faqat uning **ochiq kaliti** (public key) orqali ochish mumkin.

Inkor etilmaslik (Non-repudiation):

Xabarni qabul qiluvchi ochiq kalit bilan xeshni ochib tekshirganda, u haqiqatan ham egasi tomonidan yuborilganiga to'liq ishonch hosil qiladi. Bu davlat xizmatlari va elektron hujjat aylanmasida juda muhim.

Xavfsiz Elektron Pochta (PGP - Pretty Good Privacy)

Elektron pochta xabarlarining ochiq matn (plaintext) ko'rinishida o'qib olinishini oldini olish uchun PGP texnologiyasi RSA ga tayanadi. Jurnalistlar, diplomatlar va korporativ rahbarlar maxfiy axborot almashishda ushbu standartdan keng foydalanadilar.

Kriptografik Tahlil va Case-Study: RSA ga qilingan amaliy hujumlar

Maqolaning ilmiy qimmatini oshirish uchun RSA tizimida yo'l qo'yilgan tarixiy xatoliklarni o'rganish (Case-study) maqsadga muvofiqdir. O'z-o'zidan matematika mukammal bo'lsa-da, uni dasturlashda yo'l qo'yiladigan xatolar falokatga olib keladi.

Bleichenbacher Hujumi (Padding Oracle Attack)

1998-yilda kriptograf Daniel Bleichenbacher RSA algoritmining PKCS#1 v1.5 deb nomlangan "padding" (to'ldirish) standartidagi zaiflikni kashf qildi.

Muammo mohiyati:

RSA da qisqa xabarlarni shifrlashdan oldin uni tasodifiy ma'lumotlar bilan ma'lum bir uzunlikka keltirish (padding) kerak. Agar server noto'g'ri to'ldirilgan xabarlarga xato kodlarini (error messages) qaytarsa, hujumchi millionlab sinov so'rovlarini yuborish orqali xato kodlarini tahlil qilib, asl maxfiy kalitni yoki xabarni tiklab olishi mumkin.

Oqibat va yechim:

Bu hujum tarixdagi eng mashhur kiberhujumlardan biri bo'lib, butun dunyo bo'ylab TLS serverlarini yangilashga majbur qildi. Natijada xavfsizroq bo'lgan **OAEP (Optimal Asymmetric Encryption Padding)** standarti joriy etildi.

Coppersmith Teoremasi va Kichik Eksponenta muammosi

Ba'zi tizimlar hisoblash tezligini oshirish maqsadida ochiq kalit eksponentasi e ni juda kichik son (masalan, e = 3) qilib belgilaydi. Agar bir xil xabar uchta turli qabul qiluvchiga shunday kichik eksponenta bilan yuborilsa, hujumchi xabarlarni ushlab qolib, *Xitoy qoldiqlari teoremasi* (Chinese Remainder Theorem) yordamida yopiq kalitsiz ham xabarni o'qiy olishi isbotlangan.

Ushbu xulosalar shuni ko'rsatadiki:

RSA algoritmidan foydalanish katta mas'uliyat talab qiladi va uni xalqaro xavfsizlik standartlariga (masalan, NIST tavsiyalariga) qat'iy amal qilgan holda dasturlash shart.

RSA vs ECC: Kriptografik evolyutsiya

Bugungi kunda RSA o‘z o‘rnini asta-sekin **Elliptik egri kriptografiyasiga (ECC - Elliptic Curve Cryptography)** bo‘shatib bermoqda. Bu qism maqolaning "zamonaviy qarash" qismini mustahkamlaydi.

Nima uchun ECC?

RSA xavfsizlikni ta'minlash uchun juda katta raqamlarni (2048-4096 bit) ishlatishga majbur. ECC esa matematik jihatdan boshqacha yondashuvni (elliptik egri chiziqlar ustidagi nuqtalar logarifmi) qo‘llaydi.

Samaradorlik: 256-bitli ECC kaliti 3072-bitli RSA kaliti bilan bir xil xavfsizlik darajasini ta’minlaydi.

Resurs sarfi: ECC mobil qurilmalar, IoT (Internet of Things) va quvvati cheklangan qurilmalar uchun ancha yengil va tezdir.

Xulosa

Ushbu tadqiqot shuni ko‘rsatadiki, RSA algoritmi 50 yilga yaqin vaqt davomida raqamli dunyoni himoya qilib kelayotgan eng muhim matematik yechimdir. Biroq, xavfsizlik statik emas, u doimiy rivojlanish jarayonidir. "RSA algoritmining xavfsizligi faqat matematik hisob-kitoblarga emas, balki kalitlarni boshqarish tizimining (Key

Management System) qanchalik to‘g‘ri yo‘lga qo‘yilganligiga ham bog‘liq. Korporativ darajada RSA kalitlarini rotatsiya qilish (vaqti-vaqti bilan almashtirish) xavfsizlikning eng muhim qoidalaridan biridir."

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. **Rivest, R. L., Shamir, A., & Adleman, L.** (1978). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM, 21(2), 120-126. (RSA algoritmining asosiy ilmiy manbasi).
2. **Stallings, W.** (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson Education. (Kriptografiya asoslari bo‘yicha fundamental darslik).
3. **NIST (National Institute of Standards and Technology).** (2018). *Recommendation for Key Management (SP 800-57 Part 1 Rev 4)*. U.S. Department of Commerce. (Xavfsizlik standartlari bo‘yicha rasmiy qo‘llanma).
4. **Katz, J., & Lindell, Y.** (2020). *Introduction to Modern Cryptography* (3rd ed.). CRC Press. (Zamonaviy kriptografik protokol va modellarni tushunish uchun).
5. **Bleichenbacher, D.** (1998). *Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1*. Advances in Cryptology—CRYPTO '98, 1–12. (RSA dagi padding zaifliklari bo‘yicha tadqiqot).
6. **Shor, P. W.** (1994). *Algorithms for quantum computation: discrete logarithms and factoring*. Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134. (RSA ning kvant kompyuterlari oldidagi ojizligi haqidagi asosiy ish).
7. **Bernstein, D. J.** (2009). *Introduction to post-quantum cryptography*. In Post-Quantum Cryptography, Springer, Berlin, Heidelberg. (Kelajakdagi kriptografik tendensiyalar uchun).
8. **Barker, E., & Roginsky, A.** (2016). *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. NIST Special Publication 800-131A.