RSA ALGORITMI

Eshonqulova Feruza Abdirazoq qizi
TDShU "Tashqi iqtisodiy faoliyat" kafedrasi o'qituvchisi.

Annotatsiya: *Ushbu ilmiy maqolada Rsa shifrlash algoritmi, uning kelib chiqish tarixi va bugungi kundagi ahamiyati haqida so'z boradi.*

Kalit so'zlar: *RSA, algoritm, shirlash kaliti, shaxsiy kalit, ommoviy kalit, elektron imzo, kriptografiya.*

RSA shifrlash algoritmi, 1977 yilda Ron Rivest, Adi Shamir va Leonard Adleman tomonidan yaratilgan, asimmetrik kriptografiya usulidir. U jamoatchilik kaliti (public key) va shaxsiy kaliti (private key) orqali ishlaydi, bu esa ma'lumotlarni xavfsiz shifrlash va deshifrlash imkonini beradi. RSA ning asosiy xususiyati, uning matematik qiyinchiliklari bo'lib, bu faktorlash muammosiga asoslangan. Kalitlar uzunligi xavfsizlik darajasini belgilaydi, hozirgi vaqtda 2048 bit yoki undan yuqori uzunlikdagi kalitlar xavfsiz deb hisoblanadi. RSA keng qo'llanuvchi va ishonchli bir usul hisoblanadi, bu uni elektron imzolar, veb saytlar uchun SSL/TLS sertifikatlari va boshqa ko'plab xavfsizlikka oid dasturlarda keng qo'llanilishini ta'minlaydi.

Asimmetrik RSA kriptografiya algoritmi, kelib chiqish sanasi 1976 yil deb hisoblanadi, hozirda ma'lumotlar almashinuvi, dasturiy ta'minot manbasini tekshirish va ma'lumotlar almashinuvi yoki jo'natuvchini tekshirish zarur bo'lgan boshqa sohalarda juda faol qo'llaniladi. Bundan tashqari, u HTTPS protokolining asosiy qismi bo'lib, Yandex.Radar ma'lumotlariga ko'ra Rossiyada foydalanish 98% ga yetdi. Masalan, sevimli buvingizga mashhur messenjer orqali qo'ng'iroq qilganda yoki onlayn bozorda bank kartangiz ma'lumotlarini kiritganda, video tasvir yoki bank kartasi ma'lumotlarini almashishdan oldin, autentifikatsiya jarayoni amalga oshiriladi va RSA algoritmi yordamida shifrlash kaliti almashtiriladi.

Biznes egalaridan internet-saytlar va tranzaksiyalarni xakerlardan himoya qilish hamda ishonchni mustahkamlash bo‘yicha harakatlarida moslashuvchanlik va kengaytiriluvchanlik talab etiladi. Xakerlar xavfsizlikni buzish va biznesga yoki uning mijozlariga zarar yetkazish uchun tobora murakkab usullarni ishlab chiqishda davom etmoqda. Mas'uliyatli biznes egalari internetdagi faoliyatini ishonchli uchinchi tomon — Sertifikatlash Markazi (SM) tomonidan taqdim etilgan SSL sertifikatlari yordamida himoya qilish zarurligini allaqachon anglab yetgan.

SSL sertifikatlaridan foydalanish veb-serverni autentifikatsiya qilish, maxfiy ma’lumotlarni uzatish va mijozlar uchun tan olingan va ishonchli xavfsizlik belgisi sifatida

xizmat qiladi. An’anaviy ravishda SSL sertifikatlar RSA algoritmiga asoslangan ochiq va yopiq kalitli shifrlashdan foydalangan. Bu kalitlar xavfsiz bo‘lib qolayotgan bo‘lsa-da, tobora kuchayib borayotgan kompyuterlar tahdidi Milliy Standartlar va Texnologiyalar Instituti (NIST) kabi tashkilotlarni onlayn shifrlashni kuchaytirishga chaqirishga undadi.

Hozirda kompaniyalar RSA algoritmiga asoslangan himoyani ta'minlovchi sertifikatlarni tanlash, ECC va DSA kabi muqobil algoritmlardan foydalanish yoki uchalasi asosida yaratilgan sertifikatlarni serverga o‘rnatish imkoniyatiga ega. Bunday moslashuvchanlik biznes egalariga turli vaziyatlar, infratuzilmalar hamda mijozlar yoki hamkorlar guruhlari uchun yanada kengroq shifrlash variantlarini taqdim etish imkonini beradi.

U jamoatchilik kaliti (public key) va shaxsiy kaliti (private key) orqali ishlaydi, bu esa ma'lumotlarni xavfsiz shifrlash va deshifrlash imkonini beradi. RSA ning asosiy xususiyati, uning matematik qiyinchiliklari bo'lib, bu faktorlash muammosiga asoslangan. Kalitlar uzunligi xavfsizlik darajasini belgilaydi, hozirgi vaqtda 2048 bit yoki undan yuqori uzunlikdagi kalitlar xavfsiz deb hisoblanadi. RSA keng qo'llanuvchi va ishonchli bir usul hisoblanadi, bu uni elektron imzolar, veb saytlar uchun SSL/TLS sertifikatlari va boshqa ko'plab xavfsizlikka oid dasturlarda keng qo'llanilishini ta'minlaydi.

RSA algoritmi hali ham samarali shifrlash usuli hisoblanadi. Biroq, kalit uzunligi eksponentsial tarzda oshishda davom etadi. Internet hamjamiyati kuchli kompyuterlardan foydalanib, 1024 bitga yaqin kalitlarni buzish xavfini sezdi. Shu sababli, AQSh Milliy Standartlar va Texnologiyalar Instituti (NIST) 2013-yil oxirigacha sertifikatlash markazlariga 2048 bitdan kam bo‘lgan RSA ochiq kalitiga ega yangi SSL/TLS sertifikatlarini berishni to‘xtatishni tavsiya qildi. Shu bilan birga, alternativ shifrlash va raqamli imzolash algoritmlari — elliptik egri chiziqli kriptografiya (ECC) va raqamli imzo algoritmi (DSA) — AQSh federal hukumati tomonidan qabul qilindi va ular asosida ko‘rsatmalar ishlab chiqildi. Bu ko‘rsatmalar allaqachon hukumat uchun majburiy bo‘lib, NIST Suite B tavsiyalari ko‘plab tijorat kompaniyalari tomonidan ham ilg‘or amaliyot sifatida qabul qilinmoqda.

RSA algoritmida imzolangan sertifikatlar yillar davomida keng qo‘llanilib kelinmoqda, biroq NIST tavsiyalari asosidagi algoritmik moslashuvchanlik korxonalarga RSA, DSA va ECC algoritmlaridan foydalangan holda imzolangan sertifikatlarni tanlash imkonini beradi. TLS tuzilmasi turli algoritmlarni alohida yoki birgalikda ishlashga imkon beradi. Shu sababli, algoritmik moslashuvchanlik tufayli biznes egalari o‘zlarining internetdagi faoliyati va infratuzilmasiga eng mos keladigan ochiq kalitli algoritmni yoki ularning kombinatsiyasini tanlash imkoniga ega.

Shifrlash algoritmi — bu ma’lumotlarni kodlash uchun matematik amallar yoki qadamlar to‘plamidir. RSA bugungi kunda eng keng tarqalgan shifrlash algoritmi

hisoblanadi. ECC — bu zamonaviy va mobil ilovalar uchun kichikroq kalit o‘lchamiga ega yangi shifrlash algoritmidir. DSA esa odatda davlat pudratchilari va ularning subpudratchilari tomonidan ishlatiladi.

RSA ochiq kalitli shifrlash algoritmi uning uchta kashfiyotchisi — Ron Rivest, Adi Shamir va Leonard Adleman — nomi bilan atalgan. RSA asimmetrik algoritmlarga kiradi, bunda shifrlash kaliti va deshifrlash kaliti bir xil emas. Kalitlardan biri hammaga ochiq bo‘ladi (atayin), u "ochiq kalit" deb ataladi, ikkinchisi esa faqat egasiga tegishli va boshqalarga noma’lum bo‘ladi. Bunday tizimda bir kalit yordamida faqat bitta yo‘nalishda amallar bajariladi: agar xabar bir kalit bilan shifrlangan bo‘lsa, uni faqat ikkinchisi bilan deshifrlash mumkin. Agar kalitning uzunligi yetarlicha katta bo‘lsa, bir kalitdan ikkinchisini topish juda qiyin (deyarli imkonsiz) bo‘ladi.

RSA algoritmi shifrlashning asosiy afzalliklaridan biri - uning xavfsizligi, chunki u faktorlashning qiyinligiga asoslanadi: katta tub sonlarning ko'paytmasini faktorlash juda qiyin hisoblanadi. Bu esa RSA'ni ko'plab elektron imzo va shifrlash tizimlarida ishlatilishini ta'minlaydi.

RSA shifrlash algoritmining asosiy xususiyatlari quyidagilardir:

Asimmetrik Kalitlar: RSA algoritmi jamoatchilik kaliti (public key) va shaxsiy kaliti (private key) orqali ishlaydi. Jamoatchilik kaliti ma'lumotlarnishifrlash uchun ochiq bo'lsa, shaxsiy kalit ma'lumotlarni deshifrlash uchun maxfiy qolinadi.

Xavfsizlik: RSA ning xavfsizligi uning kalitlarining uzunligiga bog'liq. Kalit uzunroq bo'lsa, uni buzish qiyinroq bo'ladi. Hozirgi kunda 2048 bit yoki undan katta uzunlikdagi kalitlar xavfsiz deb hisoblanadi.

Ko'p qirralilik: RSA nafaqat ma'lumotlarni shifrlash va deshifrlash, balki elektron imzolar yaratish va tasdiqlash uchun ham ishlatiladi. Elektron imzo yaratish uchun, foydalanuvchi o'zining shaxsiy kaliti bilan ma'lumotni shifrlaydi; imzoni tekshirish uchun esa jamoatchilik kaliti bilan deshifrlanadi.

Keng Qo'llanilishi: RSA algoritmi ko'plab dasturlar va protokollarda, jumladan TLS/SSL (veb sahifalarning xavfsiz ulanishini ta'minlaydi), elektron pochta xavfsizligi (PGP, S/MIME), VPN larda va boshqa ko'plab xavfsizlikka asoslangan texnologiyalarda qo'llaniladi.

Matematik asoslar: RSA matematik nazariyasi, ayniqsa tub sonlar nazariyasi va modular arifmetika kabi sohalarga chuqur asoslangan. Bu asoslar algoritmning xavfsizligi va samaradorligini ta'minlaydi. Shunday qilib, RSA algoritmi asimmetrik shifrlashning eng mashhur va keng tarqalgan usullaridan biri hisoblanadi, uning xavfsizligi matematik jihatdan isbotlangan va yillar davomida sinovdan o'tgan.

RSA shifrlash algoritmining xavfsizligi uning matematik asoslariga, xususan katta tub sonlarni faktorlash muammosining qiyinchiligiga bog'liq. Kalitlarning uzunligi, masalan

2048 bit yoki undan yuqori, algoritmni kuchli qiladi, chunki bu kalitlarni buzish uchun kerak bo'ladigan hisoblash quvvati hozirgi texnologiya bilan amalga oshirish deyarli mumkin emas. Biroq, kvant kompyuterlarining kelajagi bu xavfsizlikni xavf ostiga qo'yishi mumkin, chunki ular juda tez faktorlash qobiliyatiga ega bo'lishi mumkin.

RSA shifrlash algoritmi, asimmetrik kriptografiyaning eng muhim va keng tarqalgan usullaridan biri sifatida, ma'lumotlarni xavfsiz shifrlash va deshifrlash imkonini taqdim etadi. Ushbu tadqiqotda RSA algoritmining xavfsizlik xususiyatlarini, ayniqsa kalit uzunliklarining xavfsizlik darajasiga ta'sirini chuqurroq tahlil qildik. Kalit uzunliklarining oshirilishi bilan shifrlashning xavfsizligi ham oshadi, ammo bu oshirish shifrlash/deshifrlash jarayonlarining samaradorligiga ta'sir qiladi. Shuning uchun, kalit uzunligini tanlashda xavfsizlik va samaradorlik o'rtasida muvozanat topish zarur.

FOYDALANILGAN ADABIYOTLAR:

1. Boneh, D., & Shacham, H. (2018). "Twenty Years of Attacks on the RSA Cryptosystem." Notices of the AMS, 45(2), 203-213.

2. Lenstra, A. K., & Verheul, E. R. (2001). "Selecting Cryptographic Key Sizes." Journal of Cryptology, 14(4), 255-293.

3. Boyquziyev I.M., Rahmatullayev I.R. “RSA shifrlash algoritmining maxfiy kalitini aniqlash algoritmi” Muhammad al-Xorazmiy nomidagi TATU Farg‘ona filiali “Al-Farg‘oniy avlodlari” elektron ilmiy jurnali ISSN 2181-4252 Tom: 1 | Son: 2 | 2024-yil

4. Столлингс В. Криптография и защита сетей. Принципы и практика. Изд.:Лори Вильямс, 2001.

5. Молдовян А.А., Молдовян Н.А. Введение в криптосистемы с открытым ключом. Санкт – Петербург «БХВ-Петербург» 2005.