[3]. A.M.Bagno. Wave propagation in an elastic layer interacting with a viscous liquid layer // International Applied Mechanics. 2016, 52, № 2, DOI 10.1007/s10778-016-0740-z

[4]. H.Yajuan, Sh.Yunhui, P.Panpan. Theoretical study on fluid velocity for viscous fluid in a circular cylindrical shell // The Open Mechanical Engineering Journal. 2015, 9, p. 826–830.

[5]. Худойназаров Х.Х. Нестационарное взаимодействие круговых цилиндрических упругих и вязкоупругих оболочек и стержней с деформируемой средой. Ташкент, изд-во им. Абу Али ибн Сино, 2003, 325 с.

[6]. K.Mamasoliev, E.A.Ismoilov, Z.Khudoyberdiyev. Formulation of a Boundary Value Problem for Longitudinal-Radial Vibrations of a Transversely Isotropic Cylindrical Shell Interacting With a Viscous Fluid // AIP Conf. Proc. 3405, 370001 (2026). https://doi.org/10.1063/12.0043271

[7]. Kh.Khudoynazarov, K.Mamasoliyev, E.A.Ismoilov, E.V.Ovchinnikov. Non-Stationary Influence of a Transverse-Isotropic Cylindrical Shell With a Viscous Compressed Fluid // AIP Conf. Proc. 3177, 050005 (2025) https://doi.org/10.1063/5.0294882

[8]. Beer F.P., Johnston E.R., DeWolf J.T., Mazurek D.F. Mechanics of Materials. 9th ed. New York, McGraw-Hill Education, 2020, 912 p.

Boltayev Sherzod Tuyliboyevich (Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti "Axborot xavfsizligi" kafedrasi mudiri, dotsent, PhD; e-mail: sherzodboltaev@gmail.com),
Abduqaxxorova Nigora Doniyor qizi (Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti 2-kurs magistranti; e-mail: nigoraabduqaxxorova26@gmail.com; UDK 004.056.55)

RSA VA EL-GAMAL ASSIMETRIK SHIFRLASH ALGORITMLARIGA ASOSLANGAN ELEKTRON RAQAMLI IMZO ALGORITMLARINING TADQIQI

Annotatsiya. *Ushbu maqolada RSA algoritmining katta tub sonlarni ko'paytuvchilarga ajratish, El-Gamal algoritmining diskret logarifmlash masalasining hisoblash murakkabligi asosida elektron raqamli imzo hosil qilish va uni tekshirish jarayonlari tahlil qilinib ularning xavfsizlik darajasi, hisoblash murakkabligi, kalitlar bilan ishlash xususiyatlari hamda amaliy qo'llanish imkoniyatlari o'zaro solishtiriladi. Tadqiqot natijasida RSA va El-Gamal asosidagi elektron raqamli imzo algoritmlarining afzalliklari va xususiyatlari aniqlanadi.*

Kalit so'zlar: *RSA algoritmi, El-Gamal algoritmi, elektron raqamli imzo, assimetrik kriptografiya, xesh funksiya, diskret logarifm, tub sonlar, axborot xavfsizligi.*

ИССЛЕДОВАНИЕ АЛГОРИТМОВ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ, ОСНОВАННЫХ НА АСИММЕТРИЧНЫХ АЛГОРИТМАХ ШИФРОВАНИЯ RSA И EL-GAMAL

Аннотация. *В данной статье анализируются процессы формирования и проверки электронной цифровой подписи на основе алгоритма RSA, основанного на сложности факторизации больших простых чисел, а также алгоритма El-Gamal, основанного на вычислительной сложности задачи дискретного логарифмирования. Рассматриваются и сравниваются уровни их безопасности, вычислительная сложность, особенности работы с ключами и возможности практического применения. В результате исследования определены преимущества и особенности алгоритмов электронной цифровой подписи, основанных на RSA и El-Gamal.*

Ключевые слова: *алгоритм RSA, алгоритм El-Gamal, электронная цифровая подпись, асимметричная криптография, хеш-функция, дискретный логарифм, простые числа, информационная безопасность.*

RESEARCH OF ELECTRONIC DIGITAL SIGNATURE ALGORITHMS BASED ON RSA AND EL-GAMAL ASYMMETRIC ENCRYPTION ALGORITHMS

Annotation. *This article analyzes the processes of generation and verification of electronic digital signatures based on the RSA algorithm, which relies on the computational difficulty of factoring large prime numbers, and the El-Gamal algorithm, which is based on the computational complexity of the discrete logarithm problem. The study compares their security levels, computational complexity, key management features, and practical application capabilities. As a result of the research, the advantages and distinctive features of electronic digital signature algorithms based on RSA and El-Gamal are identified.*

Key words: *RSA algorithm, El-Gamal algorithm, electronic digital signature, asymmetric cryptography, hash function, discrete logarithm, prime numbers, information security.*

Kirish. Raqamli axborot almashinuvi kengayib borayotgan hozirgi davrda elektron hujjatlarning haqiqiyligi, yaxlitligi va muallifligini tasdiqlash axborot xavfsizligining muhim vazifalaridan biri hisoblanadi.

Mazkur jarayonda elektron raqamli imzo hujjatning butunligini ta'minlash va imzolovchi shaxsni autentifikatsiya qilishga xizmat qiladi.

Elektron raqamli imzo algoritmlarining rivojlanishi ochiq kalitli kriptografiya shakllanishi bilan bevosita bog'liq. 1977-yilda R.Rivest, A.Shamir va L.Adleman tomonidan taklif etilgan RSA algoritmi katta tub sonlar ko'paytmasini faktorlash masalasining murakkabligiga asoslanadi. 1985-yilda T.ElGamal tomonidan ishlab chiqilgan El-Gamal algoritmi esa diskret logarifmlash masalasiga tayanadi. Har ikki algoritm, dastlab, assimetrik kriptografik algoritm sifatida taklif etilgan bo'lib, keyinchalik, elektron raqamli imzo tizimlarida keng qo'llanila boshlandi.

RSA va El-Gamal algoritmlariga asoslangan elektron raqamli imzo elektron hujjatlarning ishonchliligini ta'minlashda muhim o'rin tutadi. Shu bilan birga, ularning matematik asosi, imzo yaratish, hisoblash murakkabligi va xavfsizlik xususiyatlari jihatidan farqlanadi.

Assimetrik algoritmlarga asoslangan electron raqamli imzo jarayoni (A va B foydalanuvchilar bo'yicha, A foydalanuvchi imzolaydi B foydalanuvchi tekshiradi):

Umumiy papametrlar

RSA algotirmi asosidagi ERI

Ishonchli markaz tomonidan katta p, q tub sonlar tanlanadi (odatda, 1024–4096 bit).

Modul n hisoblanadi: $n = p \times q$

Eyler qiymati hisoblanadi:

$$\varphi(n) = (p-1)(q-1)$$

Bu $n, \varphi(n)$ qiymatlarni hosil qilamiz.

El-Gamal algoritmi asosidagi ERI

Ishonchli markaz tomonidan katta p tub son va $1 < g < p$ shartni qanoatlantiruvchi g sonlari tanlanadi.

Bu p, g qiymatlarni tanlaymiz.

moduli bo'yicha noldan farqli qoldiqlar multiplikativ guruhida bajariladi:

$$\mathbb{Z}_p^* = \{1,2,3,\dots,p-1\}$$

Yuqorida keltirilgan qiymatlar elektron raqamli imzo foydalanuvchilar uchun maxfiy va ochiq kalitlarni hamda ma'lumotlarni imzolash uchun foydalaniladi.

Kalitlar generatsiyasi

A foydalanuvchi ochiq kalitni quyidagi shart asosida tanlaydi:

$$EKUB(e_A, \varphi(n)) = 1$$
$$1 < e_A < \phi(n)$$

Bu shart e_A va $\phi(n)$ sonlari o'zaro tub ekanligini bildiradi, ya'ni ular o'zaro bo'linmaydi.

Yopiq kalit quyidagicha d_A hisoblanadi:

$$d_A \equiv {e_A}^{-1} (mod\ \varphi(n))$$

Bu shuni anglatadiki, d_A– e_A ning modul $\phi(n)$ bo'yicha teskari elementi.

A va B foydalanuvchilarning kalit juftligi quyidagicha bo'ladi:

Ochiq kalit: (e_A, n), (e_B, n) – imzoni tekshirish uchun ishlatiladi.

Yopiq kalit: (d_A, n), (d_B, n) – xabarni imzolash uchun ishlatiladi.

A foydalanuvchi quyidagi oraliqdan maxfiy kalit tanlaydi:

$$x_A \in \{1,2,\dots,p-1\}$$

Maxfiy kalit asosida ochiq kalit hisoblanadi:

$$y_A = g^{x_A} mod p$$

Agar hisoblash natijasida $y_A = 0$ yoki $y_A = 1$ bo'lsa, u holda maxfiy kalit x_A qayta tanlanadi va ochiq kalitni hisoblash jarayoni takrorlanadi.

Natijada A va B foydalanuvchilarning kalit juftligi quyidagicha bo'ladi:

Ochiq kalit:(p, g, y_A), (p, g, y_B)

Yopiq kalit: x_A, x_B

Foydalanuvchilarning ochiq kalitlari ishonchli markazda saqlanadi.

Elektron raqamli imzo yaratish jarayoni (A foydalanuvchi).

A foydalanuvchi yuboriladigan hujjatni, avvalo, kriptografik xesh-funksiya yordamida heshlaydi. Natijada xabarning xesh qiymat hosil qilinadi:

$$h = H(M)$$

bu yerda $H(M)$ xabarning xesh qiymati bo'lib $(h < p)$, u xabar uzunligidan qat'i nazar, fiksirlangan uzunlikdagi qiymatga akslantiriladi.

Keyingi bosqichda hosil qilingan xesh qiymat A foydalanuvchining yopiq kaliti yordamida imzolanadi:

$$S = h^{d_A} \bmod n$$

S elektron raqamli imzo hisoblanadi.

Quyidagi shartni qanoatlantiruvchi tasodifiy son k ni tanlaydi:

$$1 \le k \le p-2,$$
$$EKUB\ (k, p-1) = 1$$

Shundan so'ng imzo quyidagicha hosil qilinadi:

Bu yerda imzo qiymati ham modul n bo‘yicha hosil bo‘ladi:

$$0 \le S < n$$

Bu formuladan ko‘rinadiki, xabar xesh qiymati maxfiy kalit yordamida o‘zgartiriladi va natijada elektron raqamli imzo hosil bo‘ladi.

Natija: S

$$r = g^k \pmod p$$
$$s \equiv k^{-1}(h - x_A \cdot r) \pmod{p-1}$$

Agar hisoblash natijasida $r = 0, r = 1$ yoki $s = 0, s = 1$ bo‘lsa, u holda tasodifiy k soni qayta tanlanadi va hisoblash jarayoni takrorlanadi.

Natija: $S = (r, s)$

Shifrlash. A foydalanuvchi xabarni B foydalanuvchiga yuborishi uchun qabul qiluvchining ochiq kalitidan foydalanib shifrlaydi. Qabul qiluvchi o‘zining maxfiy kaliti orqali ma’lumotni tiklaydi.

Shifrlashdan oldin ochiq matn baytlar ketma-ketligiga o‘tkaziladi va uzunligi l bo‘lgan bloklarga ajratiladi:

$$l = log_{\,2}\, n$$

Matin uzunligi anqlanadi:

$$M = \{m_1, m_2, \dots m_i\}$$

A foydalanuvchi xabarni B foydalanuvchining ochiq kaliti (e_B, n) bilan shifrlaydi:

$$c_i = m_i^{e_B}\ mod\ n, i = \overline{1,n}$$

Har bir shifrlangan blok quyidagi oraliqda bo‘ladi:

$$0 \le c_i < n$$

Natijada barcha bloklar shifrlangandan so‘ng shifrlangan matn quyidagi ko‘rinishda hosil bo‘ladi:

$$C = \{c_i\}$$

A foydalanuvchi xabarni B foydalanuvchining ochiq kaliti (p, g, y_B) bilan shifrlaydi:

A foydalanuvchi tasodifiy k sonini tanlaydi: $1 \le k \le p-1$

Shifrlashdan oldin ochiq matn baytlar ketma-ketligiga o‘tkaziladi va uzunligi l bo‘lgan bloklarga ajratiladi:

$$l = log_{\,2}\, p$$

Birinchi qism hisoblanadi:

$$c_0 = g^k \bmod p$$

Ikkinchi qism hisoblanadi:

$$M = \{m_1, m_2, \dots m_i\}$$
$$c_i = m_i \cdot y_B^k \bmod p, i = \overline{1,n}$$

k har safar yangidan tanlangani uchun bir xil xabar turli shifrlangan ko‘rinishlarga ega bo‘ladi.

$$C = (c_0, c_i)$$

A foydalanuvchi B foydalanuvchiga shifrlangan xabarni va imzoni yuboradi:

$$(C, S)$$

Deshifrlash. B foydalanuvchi A foydalanuvchidan shifrlangan xabar va imzoni (C, S) qabul qilib oladi. Bunda, C – shifr matn, S – elektron raqamli imzo.

Matinni qayta tiklash uchun quyidagi formuladan foydalaniladi:

$$m_i = {c_i}^{d_B}\ mod\ n$$

Matinni qayta tiklash uchun quyidagi formuladan foydalaniladi:

$$v = (c_1^{x_B})^{-1}\ mod\ p$$
$$M = c_i \cdot v\ mod\ p$$

B foydalanuvchi matnni qayta tiklaydi va xabar M ga ega bo‘ladi.

Imzoni tekshirish jarayoni(B foydalanuvchi). B foydalanuvchidan xesh qiymatni hisoblaydi:$h' = H(M)$.

Imzo qiymatini imzolovchining ochiq kaliti (e_B, n) yordamida tekshiriladi:

$$h' = S^{e_B}\ mod\ n$$

Ushbu formuladagi h' va xesh qiymatlar taqqoslanadi.

Imzo qiymatini imzolovchining ochiq kaliti (p, g, y_B) yordamida tekshiriladi:

Imzo (r, s) juftligi orqali tekshiriladi. Quyidagi tenglik hisoblanadi:

$$g^{h'} = y^r \cdot r^s\ mod\ p$$

Agar tenglik bajarilsa, imzo haqiqiy deb topiladi.

Imzoning korrektligi. Matinning xesh qiymati hisoblanadi: $h = H(m)$

Imzo: $S_A = h^{d_A}(mod\ n)$

$$h = S_A^{e_A}(mod\ n)$$
$$h = (h^{d_A})^{e_A}\ (mod\ n)$$
$$h = h^{\,d_A e_A}(mod\ n)$$
$$d_A e_A \equiv 1\ (mod\varphi(n_A))$$

Natijada:

$$h = h$$

Imzo: $r = g^k(mod\ p)$

$$s = k^{-1}(h - xr) mod\ (p-1)$$

Tekshirish:

$$g^h = y^r \cdot r^s\ mod\ p$$
$$(g^x)^r \left(g^k\right)^s = y^r \cdot r^s\ mod\ p$$
$$g^{xr+ks} = y^r \cdot r^s\ mod\ p$$
$$ks = h - xr$$

Natijada:

$$g^h = y^r \cdot r^s\ mod\ p$$

Xulosa va takliflar. Ushbu maqolada RSA va El-Gamal algoritmlariga asoslangan elektron raqamli imzo tizimlarining ishlash prinsiplari, matematik asoslari hamda imzoni hosil qilish va tekshirish bosqichlari tahlil qilindi. Tadqiqot davomida RSA algoritmida xavfsizlik katta tub sonlarni koʻpaytuvchilarga ajratish masalasining murakkabligiga, El-Gamal algoritmida esa diskret logarifmlash muammosining hisoblash jihatdan murakkab ekanligiga asoslanishi koʻrsatib berildi.

Shuningdek, algoritmlarning kalitlar bilan ishlash xususiyatlari, hisoblash jarayonlari va kriptografik barqarorligi oʻzaro solishtirildi. Tahlil natijalarida, RSA algoritmi amaliy tizimlarda koʻp qoʻllaniladi, El-Gamal algoritmi esa tasodifiy parametrlardan foydalanganligi sababli ma'lumotlarni ishonchli himoyalash imkonini beradi.

Natijada RSA va El-Gamal algoritmlariga asoslangan elektron raqamli imzo mexanizmlari zamonaviy axborot tizimlarida elektron hujjatlarning ishonchliligi, yaxlitligi va autentifikatsiyasini ta'minlashda muhim kriptografik yechimlardan biri ekanligi aniqlandi.

Foydalanilgan adabiyotlar roʻyxati:

[1]. Liu B., Blancaflor E.B. Data Security and Privacy Protection Scheme Based on EC-ElGamal in Federal Learning, 2025.

[2]. FIPS 186-5 –Digital Signature Standard (DSS). National Institute of Standards and Technology (NIST), 2023. URL: https://csrc.nist.gov/publications/detail/fips/186/5/final

[3]. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие для вузов. Москва, 2005, URL: https://нэб.рф/

[4]. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. Москва, 2002, URL: https://www.schneier.com/books/applied_cryptography/

[5]. Akbarov D.E., Xasanov P.F., Xasanov X.P., Axmedova O.P. Kriptografiyaning matematik asoslari. Toshkent, 2010.

[6]. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, URL: https://link.springer.com/book/10.1007/978-3-642-04101-3

[7]. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson Education, 2017, URL: https://www.pearson.com/

[8]. IEEE Std 1363-2000 – IEEE Standard Specifications for Public-Key Cryptography. IEEE, 2000. URL: https://standards.ieee.org/

[9]. ISO/IEC 18033-2:2006 – Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers. ISO/IEC, 2006. URL: https://www.iso.org/standard/37971.html

Qurbonova Mahzuna Roʻziboyevna (Mirzo Ulugʻbek nomidagi Oʻzbekiston Milliy universitetining "Axborot xavfsizligi" kafedrasi "05.01.02-Tizimli tahlil, boshqaruv va axborotlarni qayta ishlash" mutaxassisligi tayanch doktoranti (PhD); E-mail: mahzuna1214@icloud.com)

OCHIQ KALITLI KRIPTOGRAFIK ALGORITMLARNING XAVFSIZLIK MODELLARI ASOSIDA QIYOSIY BARDOSHLILIK TAHLILI

Annotatsiya. *Maqolada RSA va El-Gamal ochiq kalitli algoritmlari matematik asoslari va zamonaviy xavfsizlik modellari (IND-CPA, IND-CCA) boʻyicha qiyosiy tahlil qilingan. RSAning kichik maxfiy koʻrsatkichga asoslangan zaifligi Wiener hujumi misolida davomli kasrlar usulida isbotlangan, shuningdek, uning determinizm sababli IND-CPA xavfsiz emasligi koʻrsatilgan. El-Gamal uchun DDH farazi asosida IND-CPA xavfsizligi isbotlangan, ammo malleability xususiyati tufayli IND-CCA modellarida zaifligi aniqlangan. Natijalar resurslari cheklangan qurilmalar uchun yengil kriptografik yechimlar zarur-ligini koʻr-satadi.*

Kalit soʻzlar: *RSA; El-Gamal, ochiq kalitli kriptografiya, IND-CPA xavfsizligi, IND-CCA xavfsizligi, Wiener hujumi, DDH farazi, malleability.*

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ МОДЕЛЕЙ БЕЗОПАСНОСТИ

Аннотация. *В статье проведён сравнительный анализ криптографических алгоритмов с открытым ключом RSA и Эль-Гамаль на основе их математических основ и современных моделей безопасности (IND-CPA, IND-CCA). Уязвимость RSA при малом секретном показателе доказана на примере атаки Винера методом цепных дробей, а также показана недостаточность RSA для IND-CPA из-за детерминированности. Для Эль-Гамаль доказана IND-CPA-безопасность на основе предположения DDH, однако выявлена уязвимость в моделях IND-CCA из-за свойства malleability.*