AMERICAN Journal of Public Diplomacy and International Studies
Volume 01, Issue 09, 2023 ISSN (E): 2993-2157

ELECTRONIC DIGITAL SIGNATURE ALGORITHMS BASED ON THE COMPLEXITY OF THE FACTORIZATION PROBLEM

Sharopova Muxayyo Muxtor qizi
Asian International University
Teacher of the "General Technical Sciences" department
mukhayyosharopova4@gmail.com

Annotation: This article shows the concepts of electronic digital signature and the main goals of its use. In addition, the science "Cryptography", which is the basis of electronic signature, and the initial encryption algorithms of this science are presented, showing examples of them. raised Electronic digital signature algorithms based on the complexity of the factorization problem.
Keywords: cryptography, factoring, digital signature, algorithms, electronic document.

Introduction.

Electronic digital signature based on RSA public key encryption algorithm

Each i - user of the system (e_i, d_i)- generates a key pair. For this, by taking sufficiently large p and q -prime numbers (these numbers are kept secret), $n = pq$ -number and the value of the Euler function $\varphi(n) = (p-1)(q-1)$is calculated (this number is also kept secret). Then, $(e_i, \varphi(n)) = 1$the number satisfying the condition, i.e., the number -by the number $\varphi(n)$-which d_i is prime to the number -is e_i calculated by this formula. $e_i d_i = 1 \bmod \varphi(n)$This (e_i; d_i) pair e_i is declared as public key and d_i private key .

Then i -user j to -user sends encrypted data with signature as follows:

1. Encryption rule: $M^{e_j} \bmod n = C$, where M - open information, S - encrypted information;

2. Decoding rule: $C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M$;

3. Calculation of ERI: $H(M)^{d_i} \bmod n = P_i$,

where i -the -user's P_i -signature is calculated by M the -data's $H(M)$ -hash function value;

4. Checking the ERI: $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$, if $H(M) = H(M_1)$(here M_1 -decrypted information), then the electronic document is valid, otherwise it is invalid, because according to the hash function property $M = M_1$, their hash values are also equal

5. Confidential data transfer protocol:

$\left[M \cup H(M)^{d_i}\right]^{e_j} \bmod n = [M \cup P_i]^{e_j} \bmod n = C$;

6. Protocol for receiving confidential transmitted information:

$C^{d_j} \bmod n = \left[M \cup P_i\right]^{e_j d_j} \bmod n = M \cup P_i$, preliminary information in general

may have been changed, therefore $C^{d_j} \bmod n = M_1 \cup P_i$ and the resulting hash value is u by signature this expression $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$, and if the received information has a hash value $H(M_1)$, then $H(M) = H(M_1)$the electronic document is valid, otherwise, it is fake.

ESIGN digital signature algorithm. ESIGN is an ERI algorithm developed by scientists from Japan (NTT, Japan). The tolerance of this algorithm is determined by the complexity of the factorization problem, such as the RSA algorithm.

In the ESIGN algorithm, a pair of large prime numbers p and q serves as a secret key and is determined by the expression n = p^2*q. The pair (n, k) serves as the public key. Here k is a security parameter.

The formation of ERI according to the ESIGN algorithm and its transmission includes the following sequence of steps:

1) M is a hash function for information:

m = H(M); The value of m is in the range from 0 to n-1;

2) a random number x smaller than p*q is generated;

3) a very small integer w is:

w ≡((m - x^k) (mod n))/p*q;

4) ERI S is formed for m using the secret key:

S ≡x+((w/kx^{k-1} (mod p))p*q;

5) information is transmitted through the communication channel M and ERI S.

Using the received information M and ERI S, the receiving party performs the following sequence of steps:

1) The hash function for M information is m = H(M):

S^k for S using public key (n, k). (mod n) is;

3) the number a is equal to or greater than the double of the number of bits divided by 3, much smaller than the integer, and 2 is ^{a};

s^k (mod n) is compared with m and m+2^a:

m = = s^k (mod n);

m+2^a = = s^k (mod n).

If s^k (mod n) is equal to or greater than m and s^k (mod n) is less than m+2^a, then ERI is valid, otherwise invalid. The fact that this algorithm has the ability to perform calculations related to x and k in advance makes it possible to speed up the ERI formation process.

This algorithm is much faster than RSA if it uses keys and signatures of the same size, and has the same security as RSA. ESIGN has received a patent in the USA, Canada, England and several countries.

References:

1. Sharopova, M. M. (2023). RSA VA EL-GAMAL OCHIQ KALITLI SHIFRLASH ALGORITMI ASOSIDA ELEKTRON RAQMLI IMZOLARI. RSA OCHIQ KALITLI SHIFRLASH

ALGORITMI ASOSIDAGI ELEKTRON RAQAMLI IMZO. *Educational Research in Universal Sciences*, *2*(10), 316-319.
2. Jalolov, T. S. (2023). PSIXOLOGIYA YO ‘NALISHIDA TAHSIL OLAYOTGAN TALABALARGA SPSS YORDAMIDA MATEMATIK USULLARNI O ‘RGATISHNING METODIK USULLARI. Educational Research in Universal Sciences, 2(10), 323-326.
3. Jalolov, T. S. (2023). PYTHON INSTRUMENTLARI BILAN KATTA MA’LUMOTLARNI QAYTA ISHLASH. Educational Research in Universal Sciences, 2(10), 320-322.
4. Sadriddinovich, J. T. (2023). Capabilities of SPSS Software in High Volume Data Processing Testing. American Journal of Public Diplomacy and International Studies (2993-2157), 1(9), 82-86.
5. Jalolov, T. S., & Usmonov, A. U. (2021). “AQLLI ISSIQXONA” BOSHQARISH TIZIMINI MODELLASHTIRISH VA TADQIQ QILISH. Экономика и социум, (9 (88)), 74-77.
6. Турсунов, Б. Ж., Гайбуллаев, С. А., & Жумаев, К. К. (2020). Влияние технологических параметров на гликолевую осушку газа. Sciences of Europe, (55-1 (55)), 33-36.
7. Турсунов, Б. Ж., & Алланазаров, Г. О. (2019). Перспективные технологии производства по улучшению качества бензина. Теория и практика современной науки, (3 (45)), 305-308.
8. Турсунов, Б. Д., & Суннатов, Ж. Б. (2017). Совершенствование технологии вторичного дробления безвзрывным методом. Молодой ученый, (13), 97-100.
9. Турсунов, Б. Ж., & Шомуродов, А. Ю. (2021). Перспективный метод утилизации отходов нефтеперерабатывающей промышленности. TA'LIM VA RIVOJLANISH TAHLILI ONLAYN ILMIY JURNALI, 1(6), 239-243.
10. Bakhodir, T., Bakhtiyor, G., & Makhfuza, O. (2021). Oil sludge and their impact on the environment. Universum: технические науки, (6-5 (87)), 69-71.
11. Турсунов, Б. Ж. (2021). АНАЛИЗ МЕТОДОВ УТИЛИЗАЦИИ ОТХОДОВ НЕФТЕПЕРЕРАБАТЫВАЮЩЕЙ ПРОМЫШЛЕННОСТИ. Scientific progress, 2(4), 669-674.
12. Турсунов, Б. Ж., Ботиров, Т. В., Ташпулатов, Д. К., & Хайруллаев, Б. И. (2018). ПЕРСПЕКТИВА ПРИМЕНЕНИЯ ОПТИМАЛЬНОГО ПРОЦЕССА РУДООТДЕЛЕНИЯ В КАРЬЕРЕ МУРУНТАУ. In Инновационные геотехнологии при разработке рудных и нерудных месторождений (pp. 160-164).
13. ТУРСУНОВ, Б., & ТАШПУЛАТОВ, Д. (2018). ЭФФЕКТИВНОСТЬ ПРИМЕНЕНИЯ ПРЕДВАРИТЕЛЬНОГО ОБОГАЩЕНИЯ РУД В КАРЬЕРЕ КАЛЬМАКИР. In Инновационные геотехнологии при разработке рудных и нерудных месторождений (pp. 165-168).
14. Турсунов, Б. Ж., Ботиров, Т. В., Ташпулатов, Д. К., & Хайруллаев, Б. И. (2018). ПЕРСПЕКТИВА ПРИМЕНЕНИЯ ОПТИМАЛЬНОГО ПРОЦЕССА РУДООТДЕЛЕНИЯ В КАРЬЕРЕ МУРУНТАУ. In Инновационные геотехнологии при разработке рудных и нерудных месторождений (pp. 160-164).
15. Axmedova, Z. I. (2023). LMS TIZIMIDA INTERAKTIV ELEMENTLARNI YARATISH T EXNOLOGIYASI. Educational Research in Universal Sciences, 2(10), 368-372.
16. Jurakulov, S. Z. (2023). NUCLEAR ENERGY. *Educational Research in Universal Sciences*, *2*(10), 514-518.
17. Oghly, J. S. Z. (2023). PHYSICO-CHEMICAL PROPERTIES OF POLYMER COMPOSITES. *American Journal of Applied Science and Technology*, *3*(10), 25-33.
18. Zafarjon o'g'li, Z. S. (2023). PHYSICAL-MECHANICAL PROPERTIES OF INTERPOLYMER COMPLEX FILM BASED ON SODIUM CARBOXYMETHYL CELLULOSE AND POLYACRYLAMIDE.
19. Jurakulov Sanjar Zafarjon Oghly. (2023). THE RELATIONSHIP OF PHYSICS AND ART IN ARISTOTLE’S SYSTEM. *International Journal of Pedagogics*, *3*(11), 67–73.
20. Boboqulova, M. X. (2023). STOMATOLOGIK MATERIALLARNING FIZIK-MEXANIK XOSSALARI. *Educational Research in Universal Sciences*, *2*(9), 223-228.

21. qizi Latipova, S. S. (2023). RIMAN-LUIVILL KASR TARTIBLI INTEGRALI VA HOSILASIGA OID AYRIM MASALALARNING ISHLANISHI. *Educational Research in Universal Sciences*, *2*(12), 216-220.
22. qizi Latipova, S. S. (2023). MITTAG–LIFFLER FUNKSIYASI VA UNI HISOBLASH USULLARI. *Educational Research in Universal Sciences*, *2*(9), 238-244.
23. Shahnoza, L. (2023, March). KASR TARTIBLI TENGLAMALARDA MANBA VA BOSHLANG'ICH FUNKSIYANI ANIQLASH BO'YICHA TESKARI MASALALAR. In *" Conference on Universal Science Research 2023"* (Vol. 1, No. 3, pp. 8-10).
24. Муродов, О. Т. (2023). РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕМПЕРАТУРЫ И ВЛАЖНОСТИ В ПРОИЗВОДСТВЕННЫХ КОМНАТ. *GOLDEN BRAIN*, *1*(26), 91-95.
25. Murodov, O. T. R. (2023). ZAMONAVIY TA'LIMDA AXBOROT TEXNOLOGIYALARI VA ULARNI QO 'LLASH USUL VA VOSITALARI. *Educational Research in Universal Sciences*, *2*(10), 481-486.
26. Sharipova, M. P. L. (2023). CAPUTA MA'NOSIDA KASR TARTIBLI HOSILALAR VA UNI HISOBLASH USULLARI. *Educational Research in Universal Sciences*, *2*(9), 360-365.