ENG XAVFSIZ SHIFRLASH ALGORITMLARI.

Doniyor Kuvondikovich Ibadullayev
O'zMU Amaliy matematika va Intelektual texnologiyalar fakulteti "Kriptografiya va kriptoanaliz" yo'nalishi II kurs magistranti
ibadullaev.d@gmail.com

Muzaffar Nematjon o'g'li Atajonov
O'zMU Amaliy matematika va Intelektual texnologiyalar fakulteti "Kriptografiya va kriptoanaliz" yo'nalishi I kurs magistranti
muzaffar_9127@mail.ru

ANNOTATSIYA

Mazkur ish kriptografiyaning muhim vazifalaridan biri - elektron raqamli imzoga bag‟ishlangan. Elektron raqamli imzo (ERI) biror hujjatning muallifini bir qiymatli o‟rnatish uchun zarur. ERI biror hujjat yoki shartnomaning haqiqiyligini ta‟minlovchi oddiy imzoning analogidir. Ushbu ishda RSA, ElGamal va DSA algoritmlarining afzalliklari va kamchiliklari qarab chiqilgan.

Kalit so‘zlar: shifrlash algoritmlari, elektron raqamli imzo, RSA, ElGamal, DSA.

ABSTRACT

This paper deals with one of the most important tasks of cryptography - the electronic digital signature. Electronic digital signature (EDS) is needed to uniquely establish the author of any document. EDS is the analog of a common signature that authenticates any document or contract. In this paper we look at the advantages and disadvantages of the algorithms RSA, ElGamal and DSA.

Keywords: encryption algorithms, electronic digital signature, RSA, ElGamal,DSA.

KIRISH

Shifrlash mashhur so'zga aylandi. Biz har doim shifrlash oraqali bizni tinglash va kuzatuvdan qanday himoya qilishini eshitamiz. Ko'pgina Internet foydalanuvchilari ulanishni himoya qilish uchun shifrlangan ilovalar, elektron pochta, tezkor xabarlar yoki VPN-lardan foydalanadilar. Shu bilan birga, hukumatlarning shifrlangan xizmatlar haqida o‘z g‘oyalari bor – ular favqulodda vaziyatlarda turli akkauntlarga to‘liq kirishni

istashadi. Va shuning uchun ular qonun orqali shifrlangan xizmatlarga orqa eshiklarni taqdim qilishni talab qilmoqdalar. Tabiiyki, ushbu yangi qonunlar ommaviy axborot vositalarining katta e'tiborini tortmoqda va shifrlashni diqqat markaziga qo'ymoqda.

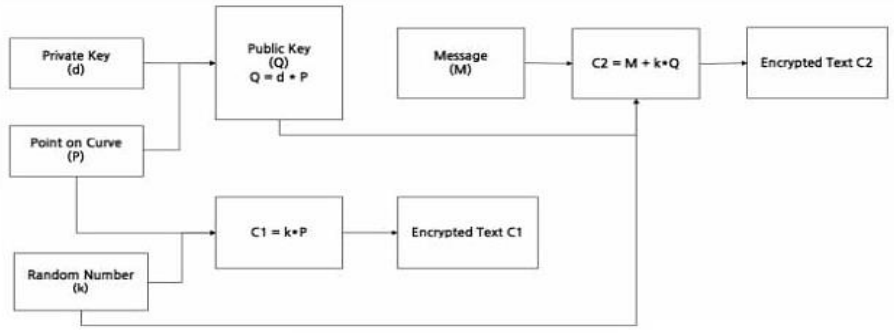
ADABIYOTLAR TAHLILI VA METODOLOGIYA

Internetda hamma joyda biz shifrlashni ko'rsatadigan juda ko'p tasodifiy harflar va raqamlarga duch kelishimiz mumkin - **ECC** , **XChacha 20**, **AES -256**, **RC 6**, **2 DES** , **QUAD** yoki **DSA** . Ammo agar siz maxfiyligingiz va xavfsizligingiz haqida qayg'uradigan oddiy foydalanuvchi bo'lsangiz, bu qisqartmalarning barchasini hazm qilish qiyin bo'ladi. Umid qilamanki, quyida keltirilgan tushuntirishlar ularni yaxshiroq tushunishingizga yordam beradi.

Bir nechta shifrlash algoritmlari mavjud. Shuning uchun ularning eng keng tarqalgan va ishonchli bo’lganlarini ko'rib chiqishni avzal ko’rdik.

ECC – SHIFRLASH ALGORITMI

Bu keyingi avlod assimetrik shifrlash algoritmidir. Bundan tashqari, u shifrlash kalitlarini yaratish va xavfsiz ma'lumotlarni uzatish uchun xavfsiz ulanishlarni yaratish uchun ishlatiladi. ECC RSA yoki DSA ga qaraganda ancha tez va xavfsizroq. U RSA ga qaraganda qisqaroq kalitlardan foydalanadi, ularni sindirish juda qiyin. Misol uchun, 512-bitli ECC kaliti 15360-bitli RSA kaliti kabi xavfsizdir, lekin u ancha qisqaroq bo'lgani uchun uni ishlab chiqarish uchun ishlov berish quvvatini sezilarli darajada kam sarflaydi. ECC RSA kabi ishlatilmaydi, chunki u nisbatan yangi va RSAni amalga oshirish osonroq.



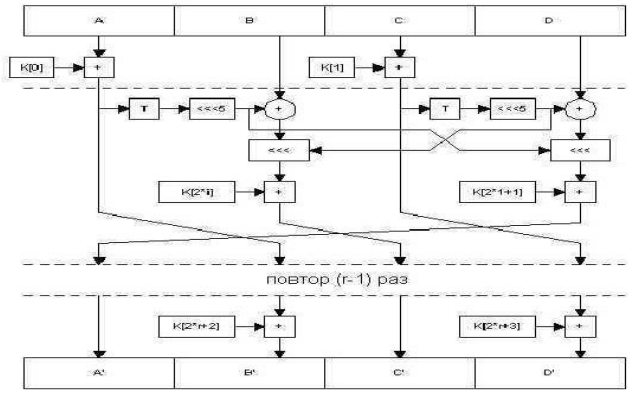
XCHACHA 20 – SHIFRLASH ALGORITMI

Bu Daniel Bernshteyn tomonidan ishlab chiqilgan simmetrik shifrlash algoritmidir. ECC singari , u nisbatan yangi, lekin allaqachon o'zini juda xavfsiz, ishonchli va tezkor algoritm ekanligini isbotlagan. ChaCha - oqim shifridir, ya'ni u ma'lumotlar kelishi bilan bitma-bit shifrlaydi. Shu sababli, ChaCha har qanday blokli shifrga qaraganda ancha tezroq

va apparat yoki katta hisoblash quvvatini talab qilmaydi. Ayrim blokli shifrlardan farqli o'laroq, ChaCha vaqti hujumlariga duchor bo'lmasligining sababi ham shu .

NATIJALAR

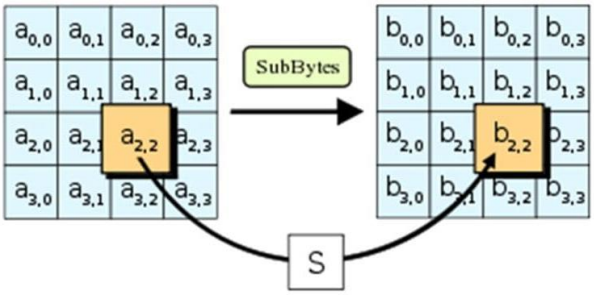
Rc 6 (oldingi versiyalari - rc 4 va rc 5) - shifrlash algoritmi



Bu simmetrik (shaxsiy kalit) shifrlash algoritmidir. Shifrlangan ma'lumotlarni oluvchi unga faqat jo'natuvchi tomonidan ulashilgan shaxsiy kalit bilan kirishi mumkin. RC 6 umumiy foydalanish uchun mo'ljallanmagan va shifrlanishi mumkin bo'lgan ma'lumotlar miqdori bo'yicha cheklovlar mavjud. RC 6 ni buzish mumkin bo'lgan darajada zaiflashtiradigan ma'lum hujumlar yo'q .

AES – SHIFRLASH ALGORITMI

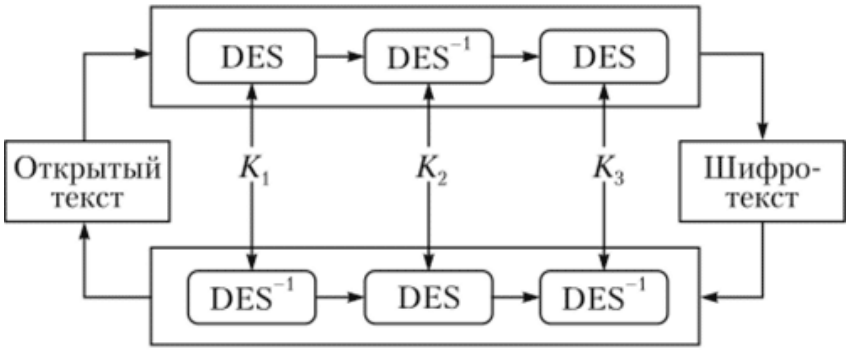
Bu bir vaqtning o'zida bitta qattiq o'lchamdagi blokdagi ma'lumotlarni shifrlaydigan yana bir nosimmetrik algoritm. AES turli uzunlikdagi kalitlarga ega bo'lishi mumkin, masalan, AES -128, AES -192 yoki AES -256. 128-bitli algoritm samarali va xavfsiz bo'lsa-da, shifrlash xizmatlari maksimal xavfsizlik uchun AES -192 dan ko'proq foydalanadi.

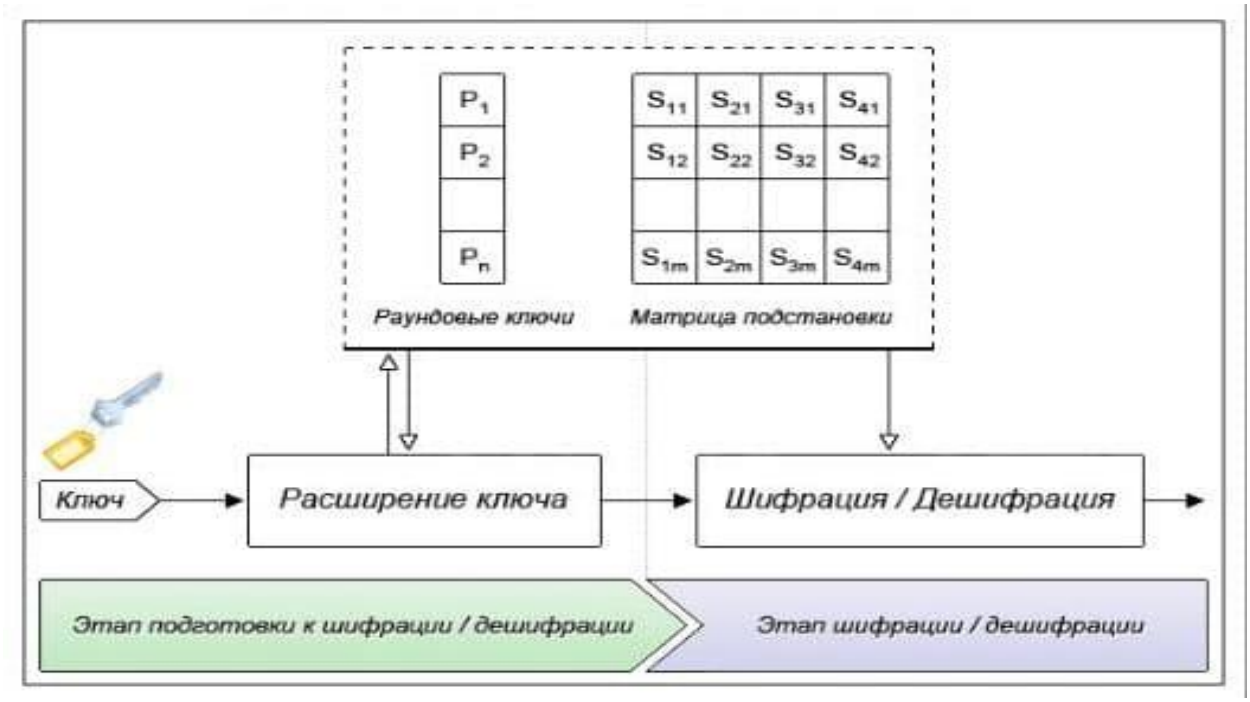


UCHLANGAN DES - SHIFRLASH ALGORITMI

Bu moliyaviy xizmatlar tomonidan keng qo'llaniladigan ma'lumotlarni shifrlash standartining yangi versiyasidir. Ushbu

algoritm 56 bitli kalitdan foydalanadi, lekin ma'lumotlarni uch marta shifrlaydi va uni 168 bitli kalitga aylantiradi. Biroq, ba'zi ekspertlarning ta'kidlashicha, bu 112 bitli kalitga o'xshaydi. Uch tomonlama shifrlash jarayoni boshqa algoritmlarga qaraganda ancha sekinroq qiladi. Bundan tashqari, u qisqaroq ma'lumotlar bloklaridan foydalanganligi sababli, ma'lumotlarni parolini ochish va sizib chiqish osonroq bo'lishi mumkin. Zamonaviy va tezroq texnologiyalar paydo bo'lishi bilan DES texnologiyasi bosqichma-bosqich to'xtatilmoqda.

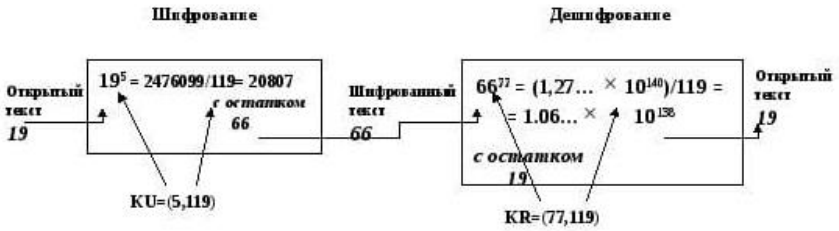




U 1993 yilda o'sha paytda mashhur bo'lgan boshqa shifrlash algoritmlariga tez, litsenziyasiz alternativ sifatida taqdim etilgan. Ko'pgina kriptograflar hali ham ushbu algoritmni o'rganishmoqda va uning xakerlikdan himoyalanganligini tasdiqlashga harakat qilmoqdalar.

MUHOKAMA

Rsa – shifrlash algoritmi

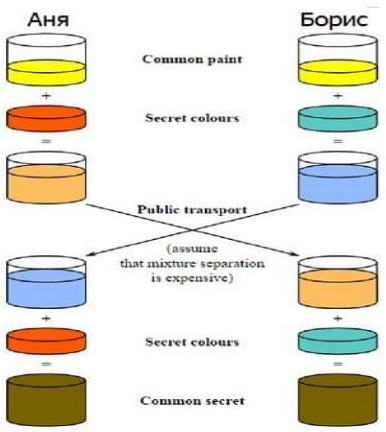


В примере **ключи** вычисляются следующим образом:

1. Выбираются два простых числа: p = 7 и q = 17.
2. Вычисляется $n = pq = 7 \times 17 = 119$
3. Вычисляется $\phi(n) = (p - 1)(q - 1) = 96$.
4. Выбирается e, взаимно простое с $\phi(n) = 96$ и меньшее, чем $\phi(n)$; в данном случае – e = 5.
5. Определяется такое d, что de = 1 (mod 96) и d < 96. Соответствующим значением будет d = 77, так как $77 \times 5 = 385 = 4 \times 96 + 1$.
6. В результате получаются открытый ключ KU = {5,119} и личный ключ KR={77,119}.

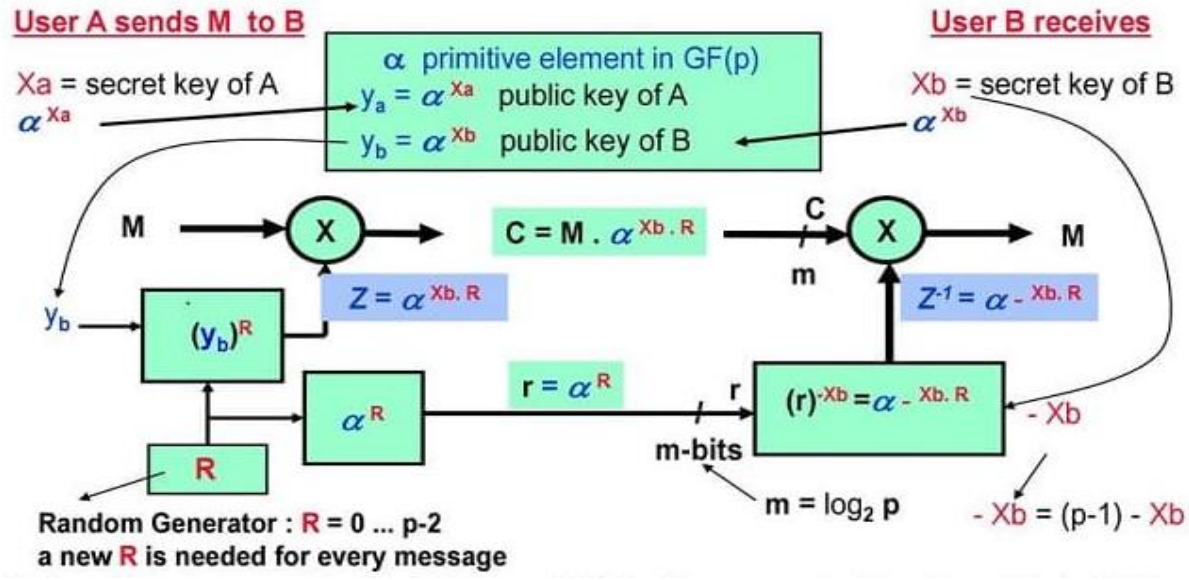
foyda ...a kalitdan ...un, shaxsiy kalit ...ernet orqali o'tadi ...u kalitlarni boshqa algoritm bilan shifrlash uchun ishlatiladi, ayniqsa shaxsiy kalitingizni baham ko'rishingiz kerak bo'lganda. Ma'lum qilinishicha, 768-bitli RSA kaliti buzilgan, ammo hozirda RSA kalitlarining aksariyati 2048-bit va 4096-bit. Bu shifrlash uchun xavfsizroq qiladi, lekin u juda sekin.

DIFFIE HELLMAN - SHIFRLASH ALGORITMI



Bu ommaviy kanal orqali kalitlarni xavfsiz almashish uchun birinchi protokollardan biridir. RSA singari, Diffie-Hellman ham katta tub sonlarning o'ta murakkabligiga tayanadi. U odatda SSL, SSH, PGP va boshqa PKI (Ochiq kalitlar infratuzilmasi) tizimlari uchun ishlatiladi. Shunday qilib, har safar URL manzili yonida qulf belgisi bo'lgan veb-saytga tashrif buyurganingizda, bu sizning qurilmangiz Diffie-Hellmandan foydalanayotganini bildiradi.

EL-GAMAL - SHIFRLASH ALGORITMI



Bu 1984 yilda Taher El-Gamal tomonidan yaratilgan ochiq kalitli shifrlash algoritmidir. Bu Diffie-Hellmanning soddalashtirilgan algoritmi bo'lib, ikkinchi tomonning faol ishtirokisiz bir yo'nalishda shifrlash imkonini beradi. Ushbu algoritmning asosiy kamchiligi shundaki, shifrlangan matn oddiy matndan ikki baravar uzun. Va eng katta afzalligi shundaki, bir xil matn har safar shifrlanganda boshqa shifrlangan matn yaratadi. Bu juda xavfsiz shifrlash usuli ekanligi bir necha bor isbotlangan.

XULOSA.

Aksariyat kiberxavfsizlik bo'yicha mutaxassislar sizga ko'p narsa har bir algoritm qayerda va qanday ishlatilishiga bog'liqligini aytadi. Har bir shifrlash usuli o'zining ijobiy va salbiy tomonlariga ega. Shuning uchun ko'p hollarda assimetrik shifrlash simmetrik shifrlash bilan birgalikda qo'llanilishi kerak.

AES hozirda ko'plab shifrlash xizmatlarida qo'llaniladigan eng mashhur simmetrik algoritmdir. Shuningdek, u ko'plab mamlakatlarda standart sifatida tan olingan. Biroq, ko'proq texnologiya gigantlari **ChaCha** kabi yangi algoritmlardan foydalanishni avzal ko’radilar.

Ammo simmetrik shifrlashning kamchiliklari bor - shaxsiy kalit qabul qiluvchiga yuborilishi kerak. Bu yerda assimetrik algoritmlar o'ynaydi. Shu sababli, bugungi kunga kelib, xavfsizlik va xotirjamlik bo’lishi uchun **ECC** ni **ChaCha** bilan birgalikda ishlatish yaxshiroq bo'ladi .

REFERENCES

1. Kuralov, Y. A., Makhmudova, D. M., (2020). METHODOLOGY OF DEVELOPING CREATIVE COMPETENCE IN STUDENTS WITH PROBLEMATIC EDUCATION. European Journal of Research and Reflection in Educational Sciences Vol. 8 No. 4, 2020, Part IIISSN 2056-5852, 142-146.
2. Akhmedov, B. A., Majidov, J. M., Narimbetova, Z. A., Kuralov, Yu. A. (2020). Active interactive and distance forms of the cluster method of learning in development of higher education. Экономика и социум, 12(79), 805-808.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М., 2002 – 816 с.
5. Жўраева, Н. В., Султанов, Р. О., Абдуллаева, С. А., Рахимжонова, В. А. (2020). Systematization of word combinations in the uzbek language. Наука и Мир, 2(6), 6568.
6. Sultanov R. O., Yusupov M. R. (2020). Ta'limda matematika fanini o'qitishdagi muammolar va ularning yechimida axborot kommunikatsiya texnologiyalarining ahamiyati. O`zMU xabarlari, 2(1/2/1), 144-147.
7. Султанов, Р. О. (2020). Idea блокли шифрлаш алгоритмини такомиллаштириш методлари. Academic Research in Educational Sciences, 1(3), 397-404.
8. Kamolov, E. R., Raximov, S. M., Sultanov, R. O., Maxmudov, M.A., (2021). Innovative method of developing creative thinking of students. Экономика и социум, 1(80).
9. Хуррамов, А. Ж., Комолов, Э. Р., Разработка алгоритма управления с учетом трудноформализуемой информации // Academic research in educational sciences, (2020). Volume 01, Issue 03, -pp: 240-247.
10. Khurramov, A. J., Makhmudova, D. M., Improvement of Technique of Designing and Teaching Learning Process in the course “Methods of Teaching Mathematics”. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019. Volume-9 Issue-2, pp: 5244-5249.