AXBOROT XAVFSIZLIGI VA UNING TASHKIL ETUVCHILARI. RSA ALGORITMI

Rasulov Islom Jovli o'g'li
Termiz Davlat Universiteti
https://doi.org/10.5281/zenodo.6492280

Annotatsiya: *maqola axborot xavfsizligi tahdidlarining kompyuter tizimlariga ta'siriga bag'ishlangan. Axborotni muhofaza qilishning asosiy xarakteristikalari, tamoyillari, usullari va mexanizmlarini, shuningdek, axborotni muhofaza qilishning keng doiradagi algoritmlari, usullari va mexanizmlarini belgilovchi CS ning tashkiliy-texnologik va inson-mashina xususiyati kabi masalalar ko'rib chiqiladi.*

Kalit so'zlar: *infratuzilma, KS funksionalligi, uzluksizlik, tashkiliy va texnologik echimlar, xavfsizlik quyi tizimi.*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЕЕ ОРГАНИЗАТОРЫ. АЛГОРИТМ RSA

Аннотация: *статья посвящена влиянию угроз информационной безопасности на компьютерные системы. Рассмотрены такие вопросы, как организационно-технологическая и человеко-машинная природа КС, определяющая основные характеристики, принципы, методы и механизмы защиты информации, а также широкий спектр алгоритмов, методов и механизмов защиты информации.*

Ключевые слова: *инфраструктура, функциональность КС, непрерывность, организационно-технологические решения, подсистема безопасности.*

INFORMATION SECURITY AND ITS ORGANIZERS. RSA ALGORITHM

Abstract: *this article investigates the impact of information security threats in computer systems. It discusses such matters as the basic characteristics, principles, methods and mechanisms of information security, as well as organizational, technological and man-machine characters of the nature of CS, defining an extensive set of methods and mechanisms of information security.*

Keywords: *infrastructure, CS functionality, continuity, organizational and technological solutions, security subsystem.*

Global tarmoqlarning paydo bo'lishi sharoitida, raqamli texnologiyalar tez o'sishi hamda aloqa va elektron ma'lumotlar almashinuvi, ko'p foydalanuvchilar, kibermakonda muloqot qilish imkoniyati paydo bo'lib bormoqda. Har kuni biz ko'plab shaxsiy ma'lumotlarimizni almashtiramiz va shu bilan raqamli izimizni qoldiramiz. Biz bir-birimiz bilan bemalol baham ko'radigan ma'lumotni beixtiyor ochiq qoldiramiz va kiber jinoyatchilar uchun himoyalanmagan vaziyatni yuzaga keltiramiz. Hozirgi vaqtda ma'lumotlarni himoya qilish va uni amalga oshirish yo'llarini izlashga, ma'lumotlarning maxfiyligi, zamonaviy kriptografiyaga ehtiyoj va talablar yuzaga kelmoqda.

Kriptografiya - ma'lumotlarning tamoyillari, vositalari va usullarini o'rganadigan bilim sohasi bo'lib axborot mazmunini yashirish va ruxsatsiz foydalanishning oldini olish uchun transformatsiyalashdir. Kriptografiya foydalanuvchilarga xarid qilish va undan foydalanish uchun Internet va boshqa ommaviy axborot vositalaridan foydalanish imkonini beradi. Parollar va boshqa shaxsiy ma'lumotlarning maxfiyligini ta'minlaydi.

Bugungi kunda kriptografiyani ikki toifaga bo'lish mumkin:

1. Simmetrik kalitli kriptografiya.
2. Asimmetrik kriptografiya.

Ikki toifaning bir biridan asosiy farqi shundaki, simmetrik shifrlash algoritmlari a dan foydalanadi yagona kalit asosida, assimetrik shifrlash algoritmlari esa ikki xil, lekin bir-biriga bog'liq ikki xil kalitlardan foydalanadi. Bundan ko'rinadiki assimetrik shifrlash simmetrik shifrlashdan katta afzalliklarga ega. Bu tomonlarning foydalanmasdan bir-biri bilan maxfiy aloqa kanallari muloqot qilish va ma'lumot almashish qobiliyatidir. Ushbu maqolaga alohida e'tibor qaratmoqchiman assimetrik shifrlash uchun eng keng tarqalgan algoritm RSA hisoblanadi.

RSA algoritmining mohiyati quyidagicha.

Misol uchun 512 yoki 1024 bit uzunlikdagi ikkita bog'langan kalit mavjud. Ulardan biri ochiq kalit ikkinchisi esa shaxsiy kalitdir. Agar ochiq kalit shifrlash uchun ishlatilsa, u holda xabar faqatgina shaxsiy kalit yordamida shifrini hal qiling mumkin va aksincha. RSA algoritmi katta butun sonlar bilan ishlardi va parchalash qiyinligiga asoslanadi. Ochiq kalit ikkita raqamdan iborat bo'lib, bu yerda bitta raqam ikkita katta raqamni ko'paytirish orqali asosiy sonlar hisoblanadi. Maxfiy kalit ham bir xil ikkita asosiy sondan olingan. Agar kimdir asl katta raqamni parchalashi mumkin bo'lsa, shaxsiy kalit buziladi. Shuning uchun RSA shifrlashning ishonchliligi butunlay kalitlarning o'lchamiga bog'liq va agar biz

kalitning o'lchamlarini bir necha baravar kattalashtiradigan bo'lsak shifrlash kuchi qonuniga muvofiq yanada ortadi, geometrik progressiya kabi.

Asimmetrik kriptografiya algoritmlarining tuzilishi

RSA algoritmining assimetrik kriptografiya algoritmi sifatida afzalliklari:

1) kalitlarni taqsimlash muammosini hal qiladi;

2) matematik funktsiyalardan foydalanish tufayli hisoblash intensivdir.

RSA algoritmining kamchiliklari:

1) yetarlicha uzun kalitlarni talab qiladi;

2) vaqt talab qiluvchi;

3) kichik simsiz qurilmalar uchun samarasiz;

4) yuqori hisoblash quvvati va tarmoqli kengligi talab qiladi.

Shunday qilib, agar biz ma'lumotni himoya qilishimiz kerak bo'lsa va biz vaqt bilan cheklanmagan bo'lsak va hisoblash resurslari orqali biz RSA algoritmidan xavfsiz foydalanishimiz mumkin. Ma'lumotlarni samarali shifrlash va shifrini ochish kibermakonda xavfsizlikning kalitidir. Ma'lumotni o'qib bo'lmaydigan formatga keltiring va unga faqat bizga kerak bo'lgan foydalanuvchilarga kirishni ta'minlang. Kriptografiya foydalanuvchilarga Internetda muloqot qilish, muhim ma'lumotlarni uzatish, uni maxfiy qoldirishdir. Ammo ma'lumotni kriptografiyaga aylantirish uchun ham foydalanilganligi o'qib bo'lmaydigan format bizni maxfiy ma'lumotlar mavjud bo'lmasligiga to'liq ishonch hosil qilmaydi. Axborotni himoya qilish, kiber buzg'unchilik va ma'lumotlarni qo'lga olish usullarini takomillashtirmoqda. Shuni anglash mumkinki bizda kuchli algoritmlar orqali ma'lumotlardan foydalanish yoki kuchli algoritmlarni ishlab chiqish ehtiyoji paydo bo'ladi.

Adabiyotlar

1. Levin, V.K. Axborot-hisoblash tizimlari va tarmoqlarida axborotni himoya qilish / Dasturlash. N3. 2012. - 90 s

2. Braun, S. Mozaik va Internetga kirish uchun butun dunyo bo'ylab Internet / S. Braun - M.: Mir: Malip: SK Press, 2011. - 234 p.

3. Shaxsiy ma'lumotlarni himoya qilish, ruxsatsiz kirishdan himoya qilish [Elektron resurs]. – URL: http://www.npp-itb.spb.ru/persdan/pdpo.shtml - Kirish rejimi: (kirish sanasi: 17.05.2014);

4. Axborot xavfsizligi [Elektron resurs]. – URL: http://www.itsec.ru/articles2/Inf_security/tak-shto-zhe-takoe - Kirish rejimi: (kirish sanasi: 15.04.2014);

5. Melnikov V. P., Kleimenov S. A., Petrakov A. M. Axborot xavfsizligi va axborotni himoya qilish. M .: Akademiya. 2011. - 589 b.