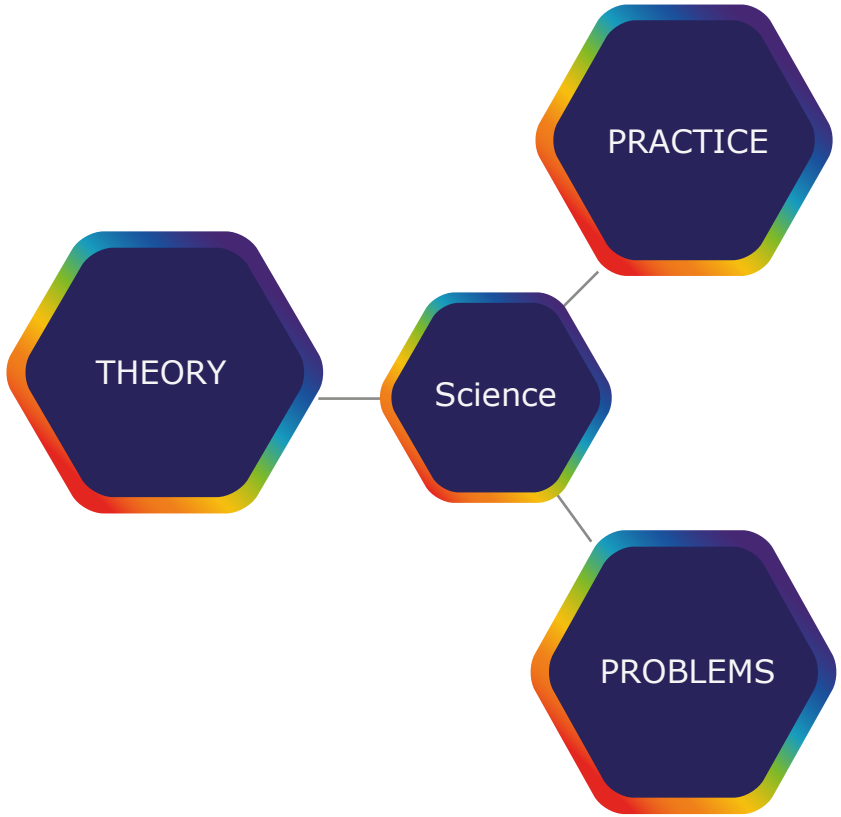
SCOPE ACADEMIC HOUSE

11th International Conference «SCIENCE AND PRACTICE: A NEW LEVEL OF INTEGRATION IN THE MODERN WORLD»

November 30, 2020, Sheffield, UK

Conference Proceedings



SCOPE ACADEMIC HOUSE

B&M PUBLISHING

11th International Conference «SCIENCE AND PRACTICE: A NEW LEVEL OF INTEGRATION IN THE MODERN WORLD»

September, 10 - November, 30, 2020, Sheffield, UK

Conference Proceedings

Scope Academic House
UK, S Yorkshire, Sheffield

B&M Publishing
USA, San Francisco, California

SCOPE ACADEMIC HOUSE

B&M PUBLISHING

11th International Conference
«SCIENCE AND PRACTICE: A NEW LEVEL OF INTEGRATION
IN THE MODERN WORLD»

Science editor: Prof. Robert Draut

Office 1 Velocity tower
10 st. Mary's gate
Sheffield
S Yorkshire
United Kingdom
S1 4LR

Published by B&M Publishing.

ISBN 978-0-9898799-4-2

DOI: http://doi.org/10.15350/UK_6/11

DOI: http://doi.org/10.15350/UK_6/11

CONTENTS

11th International Conference. September, 10 - November, 30, 2020.
UK, S Yorkshire, Sheffield

«SCIENCE AND PRACTICE: A NEW LEVEL OF INTEGRATION IN THE MODERN WORLD» • Conference Proceedings

DOI: http://doi.org/10.15350/UK_6/11

Research Article

METHODS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION

S.M. Imomova[1]
F.N. Safoyeva[2]

[1]Senior lecturer, Department of Information technologies, faculty of physics and mathematics, Bukhara state University, Uzbekistan.
[2]Student, Department of mathematics and software for information systems, faculty of physics and mathematics, Bukhara state University, Uzbekistan.

DOI: http://doi.org/10.15350/UK_6/11.6

Abstract

The article provides information on methods of cryptographic information protection.

Key words: information, information security, cryptography, cryptographic tools, coding and encryption.

Axborotning himoyasi deb, boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta'minlovchi va tashkilot axborot zahiralarining yaxlitliligi, ishonchliligi, foydalanish osonligi va maxfiyligini ta'minlovchi qatiy reglamentlangan dinamik texnologik jarayonga aytiladi.

«Kriptografiya» atamasi dastlab «yashirish, yozuvni berkitib quymoq» ma'nosini bildirgan. Birinchi marta u yozuv paydo bo'lgan davrlardayoq aytib o'tilgan. Hozirgi vaqtda kriptografiya deganda har qanday shakldagi, ya'ni diskda saqlanadigan sonlar ko'rinishida yoki hisoblash tarmoqlarida uzatiladigan xabarlar ko'rinishidagi axborotni yashirish tushuniladi. Kriptografiyani raqamlar bilan kodlanishi mumkin bo'lgan har qanday axborotga nisbatan qo'llash mumkin. Maxfiylikni ta'minlashga qaratilgan kriptografiya kengroq qo'llanilish doirasiga ega. Aniqroq aytganda, kriptografiyada qo'llaniladigan usullarning o'zi axborotni himoyalash bilan bog'liq bo'lgan ko'p jarayonlarda ishlatilishi mumkin. Kriptografiya axborotni muhofaza qilish usullaridan biri hisoblanadi. Kriptografiya axborot (ma'lumotlar)ni o'zgartirish tamoyillari, vositalari va usullarini tadqiq etadi. Bundan maqsad axborot mazmunidan ruxsat etilmagan foydalanishdan muhofazalash va uni buzishni bartaraf qilish. Kriptografiya ma'lumotlarni aloqa kanallari orqali uzatishda yoki saqlashda konfedensiallikni yoki haqiqiylikni ta'minlash usullari bilan shug'ullanadi. Shu bilan birga kriptografiya ma'lumotlarni xabardor bo'lmagan shaxslar uchun tushuna olmaydigan qilish maqsadida o'zgartirish usuli hamdir. Ma'lumotlar xavfsizligi tizimining muhim tarkibiy bo'lagi. Uning mohiyati ma'lumotlarni uzatishdan oldin ma'nosiz belgilar yoki signallar yig'masiga aylantirish va ma'lumotlarni oluvchi qabul qilib olgandan so'ng, ularni dastlabki shakliga qayta tiklashdir. «Kriptografiya» atamasi grek tilidan tarjima qilinganda «yashirish, yozuvni berkitib qo'ymoq» ma'nosini bildiradi. Atamaning ma'nosi kriptografiya kerakli ma'lumotni yashirin saqlash va himoyalash maqsadida qo'llanishini anglatadi. Kriptografiya axborotni himoyalash vositasi, shuning uchun u axborot xavfsizligini ta'minlashning bir tarmog'i hisoblanadi. Ma'lumki, kriptografik vositalar hozirgi vaqtgacha asosan davlat sirlarini himoya qilishga qaratilgan edi, shuning uchun bu vositalar maxsus organlar tomonidan yaratilgan. Bunda yuqori kriptomustahkamlikka ega bo'lgan kriptotizimlar qo'llanilgan, bu esa katta xarajatlarni talab qilgan. Oxirgi yillarda ma'lumotlarni kriptografik o'zgartirishning yangi usullari intensiv ishlab chiqilmoqda, ular an'anaviy qo'llanishiga qaraganda kengroq sohalarga tatbiq etilmoqda. Avtomatlashtirilgan tizimlarda ma'lumotlar himoyasining kriptografik usullari hisoblash texnikasi vositalarida qayta ishlanayotgan yoki har xil turdagi saqlash qurilmalarida saqlanayotgan ma'lumotlarni himoyalashda, shuningdek aloqa liniyalari orqali tizim elementlariga uzatilayotgan ma'lumotlarni himoyalashda qo'llaniladi. Hozirgi vaqtda ko'plab har xil shifrlash usullari ishlab chiqilgan va ularni qo'llashning nazariy va amaliy asoslari yaratilgan.

Kriptografiya sohasidagi oxirgi yutuqlardan biri — raqamli signatura — maxsus xossa bilan axborotni to'ldirish yordamida yaxlitlikni ta'minlovchi usul, bunda axborot uning muallifi bergan ochiq kalit ma'lum bo'lgandagina tekshirilishi mumkin. Ushbu usul maxfiy kalit yordamida yaxlitlik tekshiriladigan ma'lum usullardan ko'proq afzalliklarga ega.

Kriptografiya usullarini qo'llashning ba'zi birlarini ko'rib chiqamiz. Uzatiladigan

DOI: http://doi.org/10.15350/UK_6/11

axborotning ma'nosini yashirish uchun ikki xil o'zgartirishlar qo'llaniladi: **kodlashtirish** va **shifrlash**.

Kodlashtirish uchun tez-tez ishlatiladigan iboralar to'plamini o'z ichiga oluvchi kitob yoki jadvallardan foydalaniladi. Bu iboralardan har biriga, ko'p hollarda, raqamlar to'plami bilan beriladigan ixtiyoriy tanlangan kodli so'z to'g'ri keladi. Axborotni kodlash uchun xuddi shunday kitob yoki jadval talab qilinadi. Kodlashtiruvchi kitob yoki jadval ixtiyoriy kriptografik o'zgartirishga misol bo'ladi. Kodlashtirishning axborot texnologiyasiga mos talablar — qatorli ma'lumotlarni sonli ma'lumotlarga aylantirish va aksincha o'zgartirishlarni bajara bilish. Kodlashtirish kitobini tezkor hamda tashqi xotira qurilmalarida amalga oshirish mumkin, lekin bunday tez va ishonchli kriptografik tizimni muvaffaqiyatli deb bo'lmaydi. Agar bu kitobdan biror marta ruxsatsiz foydalanilsa, kodlarning yangi kitobini yaratish va uni hamma foydalanuvchilarga tarqatish zaruriyati paydo bo'ladi. Kriptografik o'zgartirishning ikkinchi turi **shifrlash** o'z ichiga — boshlang'ich matn belgilarini anglab olish mumkin bo'lmagan shaklga o'zgartirish altoritmlarini qamrab oladi. O'zgartirishlarning bu turi axborot-kommunikatsiyalar texnologiyalariga mos keladi. Bu yerda algoritmni himoyalash muhim ahamiyat kasb etadi. Kriptografik kalitni qo'llab, shifrlash algoritmining o'zida himoyalashga bo'lgan talablarni kamaytarish mumkin. Endi himoyalash ob'ekti sifatada faqat kalit xizmat qiladi. Agar kalitdan nusxa olingan bo'lsa, uni almashtirish mumkin va bu kodlashtiruvchi kitob yoki jadvalni almashtirishdan engildir. Shuning uchun ham kodlashtirish emas, balki shifrlash axborot-kommunikatsiyalar texnologiyalarida keng ko'lamda qo'llanilmoqda.

Sirli (maxfiy) aloqalar sohasi **kriptologiya** deb aytiladi. Ushbu so'z yunoncha «**kripto**» — sirli va **«logus»** — xabar ma'nosini bildiruvchi so'zlardan iborat. Kriptologiya ikki yo'nalish, ya'ni **kriptografiya** va **kriptotahlil**dan iborat. **Kriptografiyaning** vazifasi xabarlarning maxfiyligini va haqiqiyligini ta'minlashdan iborat. **Kriptotahlilning** vazifasi esa kriptograflar tomonidan ishlab chiqilgan himoya tizimini ochishdan iborat.

Hozirgi kunda **kriptotizim**ni ikki sinfga ajratish mumkin:

• simmetriyali bir kalitlilik (maxfiy kalitli);

• asimmetriyali ikki kalitlilik (ochiq kalitli).

Simmetriyali tizimlarda quyidagi ikkita muammo mavjud:

1) Axborot almashuvida ishtiroq etuvchilar qanday yo'l bilan maxfiy kalitni bir-birlariga uzatishlari mumkin?

2) Jo'natilgan xabarning haqiqiyligini qanday aniqlasa bo'ladi?

Ushbu muammolarning yechimi ochiq kalitli tizimlarda o'z aksini topdi.

Ochiq kalitli asimmetriyali tizimda ikkita kalit qo'llaniladi. Biridan ikkinchisini hisoblash usullari bilan aniqlab bo'lmaydi.

Birinchi kalit axborot jo'natuvchi tomonidan shifrlashda ishlatilsa, ikkinchisi axborotni qabul qiluvchi tomonidan axborotni tiklashda qo'llaniladi va u sir saqlanishi lozim. Ushbu usul bilan axborotning maxfiyligini ta'minlash mumkin. Agar birinchi kalit sirli bo'lsa, u holda uni elektron imzo sifatida qo'llash mumkin va bu usul bilan axborotni autentifikatsiyalash, ya'ni axborotning yaxlitligini ta'minlash imkoni paydo bo'ladi.

References:

С.К.Ганиев, М.М. Каримов,К.А.Ташев. Ахборот хавфсизлиги. Тошкент. Дарслик. 2017.
Имомова Ш.М. Использование электронной цифровой подписи // БУХОРО ДАВЛАТ УНИВЕРСИТЕТИ ИЛМИЙ АХБОРОТИ. 2018. №4.С62.
Бердиева С.М., Имомова Ш.М. Использование инновационных технологий на уроках информатики// Наука, техника и образование. 2018.10 (51).С. 28-31.