PAROLLARNI HIMOYALASHDAGI KOMBINATORIKA ROLI

Mualliflar: ***Rahmatov Abbosbek***
Jabborov Behzod
Tashkilot: Farg‘ona davlat texnika universiteti Ijtimoiy fanlar va sport kafedrasi asistenti. II bosqich 55 23 suniy intlekt yo’nalishi

KIRISH

Bugungi raqamli davrda axborot xavfsizligi eng muhim masalalardan biriga aylandi. Har bir foydalanuvchi o‘zining shaxsiy ma’lumotlari, moliyaviy axboroti, ijtimoiy tarmoqlardagi hisoblari va elektron tizimlarga kirish huquqini parol yordamida himoya qiladi. Parollar – inson va tizim o‘rtasidagi birinchi xavfsizlik darvozasi bo‘lib, ularning kuchliligi va murakkabligi axborot xavfsizligi darajasini belgilab beradi.

Biroq, ko‘pchilik foydalanuvchilar hali ham oddiy, tez yodda qoladigan parollardan foydalanadi. Bu esa parolni “brutfors” (brute-force) yoki “lug‘at” (dictionary attack) kabi avtomatlashtirilgan hujumlarga nisbatan zaif qiladi. Aynan shu nuqtada kombinatorika – matematik tarmoq sifatida – parollar himoyasida beqiyos ahamiyat kasb etadi.

Kombinatorika parolning barcha mumkin bo‘lgan kombinatsiyalarini tahlil qilish, ularning sonini aniqlash, ehtimollik asosida xavfsizlik darajasini baholash imkonini beradi. Masalan, 8 belgili parolda 26 ta lotin harfi, 10 ta raqam va 10 ta maxsus belgidan foydalanilsa, ularning umumiy kombinatsiyalar soni milliardlab natijalarni beradi. Shu bois, kombinatorika nafaqat parol yaratishda, balki kriptografik tizimlarni loyihalashda ham asosiy matematik tayanch hisoblanadi.

Mazkur maqolada parol xavfsizligida kombinatorika nazariyasining o‘rni, uning amaliy qo‘llanilishi, hisoblash modellari va himoya samaradorligini oshirishdagi matematik yondashuvlar tahlil qilinadi.

В современном цифровом обществе безопасность информации является одной из ключевых задач. Почти каждый пользователь защищает свои данные с помощью пароля, который служит главным инструментом контроля доступа. Надёжность и устойчивость пароля определяют уровень защиты персональной информации.

Однако слабые и легко угадываемые пароли остаются самой частой причиной взломов. В этой связи комбинаторика, как раздел математики, играет решающую роль в оценке стойкости паролей и моделировании атак. Комбинаторные методы позволяют рассчитать количество возможных

комбинаций символов, определить сложность перебора и оценить вероятность успешного взлома.

Настоящая статья посвящена анализу роли комбинаторики в обеспечении защиты паролей, исследованию математических закономерностей построения безопасных комбинаций и применению данных принципов в современных криптографических системах.

In today's digital era, information security has become a critical concern. Every user relies on passwords to protect personal and professional data from unauthorized access. The strength of a password is directly related to its complexity and randomness, which determine the overall level of security.

However, many users still use simple and predictable passwords that can be easily cracked using brute-force or dictionary attacks. This is where combinatorics, as a branch of mathematics, plays a fundamental role in password protection.

Combinatorics allows us to calculate the number of possible password combinations, analyze their resistance to guessing, and model the probability of cracking attempts. Therefore, understanding the mathematical basis of combinatorial analysis helps in designing stronger passwords and more resilient cryptographic systems.

This paper explores the significance of combinatorics in password security, its computational aspects, and its role in enhancing the overall robustness of authentication systems.

ASOSIY QISM

1. Parollar va ularning axborot xavfsizligidagi o‘rni

Axborot xavfsizligi bugungi kunda har bir davlat, tashkilot va shaxs uchun eng muhim yo‘nalishlardan biriga aylangan. Raqamli texnologiyalar hayotimizning barcha jabhalariga kirib kelgani sari, har bir foydalanuvchi o‘z shaxsiy ma’lumotlarini himoya qilish zaruriyatiga duch kelmoqda. Bu himoyaning eng oddiy, lekin eng muhim vositalaridan biri — parol hisoblanadi.

1.1. Parol tushunchasi va uning vazifasi

Parol — bu ma’lum bir tizim, dastur yoki ma’lumotlar bazasiga kirish uchun mo‘ljallangan maxfiy belgilar ketma-ketligidir. Parol foydalanuvchini autentifikatsiya qilish (ya’ni, uning haqiqiyligini tekshirish) jarayonida ishlatiladi. U axborot tizimining “birinchi himoya liniyasi” bo‘lib, foydalanuvchini tanib olish hamda begonalarning kirishiga to‘sqinlik qilish uchun xizmat qiladi.

Shunday bo‘lsa-da, parolning samarali himoya vositasi sifatidagi qiymati uning murakkabligi va tasodifiyligi bilan belgilanadi. Juda oddiy yoki qisqa parollarni zamonaviy dasturlar soniyalar ichida aniqlab olishi mumkin. Shuning uchun parol

tanlashda faqat inson yodida qolish qulayligi emas, balki matematik jihatdan murakkablik darajasi ham muhim o‘rin tutadi.

1.2. Parol turlarining rivojlanish bosqichlari

Dastlabki elektron tizimlarda parollar oddiy matn shaklida saqlanar edi. Bunday holatda tizimga kirgan kishi parolni osongina ko‘rishi yoki nusxalab olishi mumkin edi. Keyinchalik parollarni xeshlash (hashing) texnologiyasi joriy etildi — bu usulda parol matematik funksiya orqali kodga aylantirilib saqlanadi. Bunday kodni orqaga qaytarish deyarli imkonsiz.

Bugungi kunda parollarni himoyalashning quyidagi turlari keng qo‘llaniladi:

• Oddiy parollar: foydalanuvchi tomonidan yaratilgan, ko‘pincha qisqa va osongina taxmin qilinadigan parollar.

• Murakkab parollar: katta va kichik harflar, raqamlar hamda maxsus belgilar kombinatsiyasidan iborat bo‘lgan parollar.

• Ko‘p bosqichli autentifikatsiya tizimlari (MFA): paroldan tashqari qo‘shimcha tekshiruv (SMS kodi, biometrik ma’lumot, e-mail tasdiqlash va boshqalar) talab qilinadigan tizimlar.

Shu tarzda parol texnologiyasi oddiy matndan tortib to murakkab kriptografik tizimlargacha rivojlanib bormoqda.

1.3. Parol zaifliklarining asosiy sabablari

Parol xavfsizligiga tahdid soluvchi asosiy omillar quyidagilardan iborat:

1. Oddiy parollardan foydalanish: “123456”, “password”, “qwerty” kabi parollar eng tez buziladiganlardandir.

2. Parolni bir necha joyda takrorlash: foydalanuvchi bir paroldan bir nechta sayt yoki tizimda foydalansa, bitta tizimdagi buzilish barcha hisoblarni xavf ostiga qo‘yadi.

3.Parolni ochiq joyda saqlash: qog‘ozda, telefon bloknotida yoki elektron faylda parolni saqlash xavfli.

4.Ijtimoiy muhandislik (social engineering): foydalanuvchini aldash orqali parolni aniqlash usuli.

5. Avtomatlashtirilgan hujumlar: brutfors (barcha kombinatsiyalarni ketma-ket sinash) yoki lug‘at hujumlari (tayyor parollar ro‘yxati orqali tekshirish).

Shuning uchun zamonaviy xavfsizlik tizimlari parol tanlashda kombinatorika va ehtimollik nazariyalariga asoslangan tavsiyalarni ishlab chiqadi.

1.4. Parol uzunligi va murakkabligining matematik asoslari

Parolning xavfsizlik darajasi uning uzunligi va belgi turining xilma-xilligiga bog‘liq. Kombinatorik nuqtayi nazardan, parolning barcha mumkin bo‘lgan kombinatsiyalar soni quyidagicha aniqlanadi:

bu yerda:

• k — ishlatiladigan belgilar soni (masalan, 26 harf, 10 raqam va 10 maxsus belgidan jami 46 ta),

• n — paroldagi belgilar soni.

Masalan, agar foydalanuvchi 8 belgidan iborat parol tanlasa va 46 xil belgidan foydalanish imkoniyati bo‘lsa, umumiy kombinatsiyalar soni:

ya’ni 22 trillion kombinatsiya bo‘ladi.

Bu shuni anglatadiki, har bir qo‘shimcha belgi parolning buzilish ehtimolini geometrik darajada kamaytiradi. Shu bois, kombinatorika parol xavfsizligini hisoblashda asosiy ilmiy vosita sifatida qo‘llaniladi.

1.5. Axborot tizimlarida parol xavfsizligini ta’minlashda kombinatorikaning o‘rni

Kombinatorika parolni tanlash, tekshirish va himoya qilishda quyidagi asosiy yo‘nalishlarda qo‘llaniladi:

•Parol uchun belgilar to‘plamini kengaytirish orqali kombinatsiyalar sonini ko‘paytirish;

•Minimal uzunlikni belgilash orqali parol xavfsizligini normativlashtirish;

•Parol generatorlarini matematik algoritmlar asosida ishlab chiqish;

•Parollarni tekshirish tizimlarida ehtimollik modellarini joriy etish.

Natijada kombinatorika nafaqat nazariy jihatdan, balki amaliy xavfsizlik tizimlarini loyihalashda ham muhim o‘rin tutadi.

2. Kombinatorika nazariyasi va uning asosiy tushunchalari

Kombinatorika – matematikaning elementlar to‘plamidan ma’lum shartlar asosida tuziladigan tartiblar, joylashuvlar va tanlovlar sonini o‘rganadigan bo‘limidir. U, aslida, “nechta turli imkoniyat mavjud?” degan savolga javob beradi. Aynan shu savol parollar himoyasida ham markaziy o‘rinda turadi. Chunki har bir parol – bu belgilar to‘plamidan hosil qilingan muayyan kombinatsiyadir.

Kombinatorika asosan uchta asosiy operatsiyaga tayanadi:

1.Joylashtirishlar (permutatsiyalar)

2.Tanlovlar (kombinatsiyalar)

3.Qaytarilgan joylashtirish va tanlovlar

Har bir operatsiya turli xil parol tizimlarida qo‘llaniladi, chunki parol belgilarining tartibi, takrorlanishi va uzunligi xavfsizlik darajasini belgilaydi.

2.1. Joylashtirishlar (permutatsiyalar)

Agar n ta turli belgi mavjud bo‘lsa, ularning barchasidan iborat barcha tartiblar soni quyidagicha aniqlanadi:

Bu yerda “!” faktorial belgisini bildiradi, ya’ni

.Masalan, 5 xil belgidan (masalan, A, B, C, D, E) iborat parol hosil qilinsa, barcha turli joylashuvlar soni:

Bu shuni ko‘rsatadiki, belgilar soni ko‘paygan sari kombinatsiyalar soni geometrik emas, balki faktorial o‘sishda ortadi. Shu sababli, har bir qo‘shimcha belgi parol tizimining mustahkamligini keskin oshiradi.

Axborot xavfsizligida joylashtirishlar, odatda, belgilar tartibi muhim bo‘lgan holatlar uchun qo‘llaniladi. Masalan, “abc” va “cba” – belgilar bir xil bo‘lsa-da, joylashuvi turlicha bo‘lgani sababli ikki xil parol sifatida qabul qilinadi.

2.2. Tanlovlar (kombinatsiyalar)

Kombinatsiyalar belgilar tartibi ahamiyatsiz bo‘lgan holatlar uchun ishlatiladi. Ularning soni quyidagicha aniqlanadi:

bu yerda:

•n — mavjud belgilar soni,

• r — tanlangan belgilar soni.

Masalan, foydalanuvchi 10 xil belgidan 4 tasini tanlab parol hosil qilsa (tartib ahamiyatsiz bo‘lsa), kombinatsiyalar soni:

Bu yondashuv ko‘proq kriptografik kalitlarni yaratishda, ya’ni belgilarni tanlashda, lekin ularning tartibini hisobga olmagan holda qo‘llaniladi.

Kombinatsiyalar parol tizimlarining umumiy murakkablik darajasini baholashda, shuningdek ehtimollikni hisoblashda keng qo‘llaniladi.

2.3. Qaytarilgan joylashtirishlar

Parol tizimlarida eng ko‘p uchraydigan holat – bu belgilar takrorlanishiga ruxsat berilgan joylashtirishdir. Chunki foydalanuvchi parolda bir belgidan bir necha marta foydalanishi mumkin (masalan, “AAB5##”).

Bunday holatda barcha mumkin bo‘lgan kombinatsiyalar soni quyidagicha bo‘ladi:

bu yerda:

•n — belgilar to‘plami hajmi (masalan, 62: A–Z, a–z, 0–9),

•r — parol uzunligi.

Masalan, 62 belgidan 8 belgili parol hosil qilinsa:

ya’ni 218 trillion kombinatsiya.

Agar tizim sekundiga 1 milliard (10^9) sinov amalga oshira olsa, barcha kombinatsiyalarni sinab chiqish uchun taxminan 2,5 kun kerak bo‘ladi. Shu sababli, parol uzunligini 8 dan 10 belgigacha oshirish orqali sinov muddati yillar darajasigacha cho‘ziladi. Bu kombinatorikaning amaliy kuchini yaqqol namoyon etadi.

2.4. Kombinatorika va ehtimollikning parol xavfsizligidagi o‘zaro bog‘liqligi

Kombinatorika yordamida faqat kombinatsiyalar soni emas, balki parolni to‘g‘ri topish ehtimoli ham aniqlanadi. Agar foydalanuvchi tomonidan yaratilgan parol tasodifiy bo‘lsa, uni bir urinishda to‘g‘ri topish ehtimoli:

Masalan, 62 belgili tizimda 8 belgidan iborat parol uchun:

ya’ni ehtimol deyarli nolga teng. Bu natija har bir belgining ahamiyatini va kombinatorikaning himoya darajasini matematik asosda isbotlaydi.

Parolni to‘g‘ri topish ehtimoli shunchalik kichik bo‘lsa, tizimning himoya darajasi shunchalik yuqori bo‘ladi. Shu sababli, kombinatorika yordamida xavfsizlik siyosatlari, parol generatorlari va foydalanuvchi tavsiyalari ishlab chiqiladi.

2.5. Kombinatorikaning kriptografiyadagi ahamiyati

Kombinatorika nafaqat oddiy parollarda, balki butun kriptografik algoritmlarning matematik asosi sifatida ishlaydi. Masalan:

• RSA algoritmi – katta tub sonlarni kombinatorik tanlash orqali kalit yaratadi.

• AES (Advanced Encryption Standard) – kombinatorik o‘zgartirishlar va permutatsiyalar asosida ma’lumotni shifrlaydi.

• Hash funksiyalar – belgilarni kombinatsion tarzda o‘zgartirib, bir tomonlama shifrlashni ta’minlaydi.

Bu misollar kombinatorikaning parol himoyasidan chiqib, butun axborot xavfsizligi infratuzilmasining tayanchiga aylanganini ko‘rsatadi.

Xulosa (bo‘lim yakuni uchun)

Demak, kombinatorika – parol tizimlarining nazariy poydevori bo‘lib, u parol uzunligi, belgi turi va tartibga oid barcha matematik hisob-kitoblarni asoslaydi. Kombinatorika yordamida har bir parolning murakkablik darajasi, ehtimollik tahlili va brutfors hujumlariga bardoshliligi oldindan baholanishi mumkin.

Shu bois, kombinatorika nafaqat matematik nazariya sifatida, balki axborot xavfsizligi amaliyotida ham muhim rol o‘ynaydi.

3. Parol tanlashdagi ehtimollik va kombinatsiyalar sonini hisoblash

Har qanday parol tizimi matematik nuqtayi nazardan belgilar to‘plamidan tashkil topgan kombinatorik modeldir. Parolning kuchi — bu uning ko‘p sonli kombinatsiyalar orasida tasodifiy joylashuvi bilan belgilanadi. Shuning uchun kombinatorika yordamida parol tanlash jarayonini matematik tarzda tahlil qilish mumkin.

3.1. Parol murakkabligini belgilovchi omillar

Parolning himoya darajasini aniqlovchi uchta asosiy omil mavjud:

1.Parol uzunligi (n): belgilar soni qanchalik ko‘p bo‘lsa, kombinatsiyalar soni shunchalik tez o‘sadi.

2.Belgi to‘plami hajmi (k): ishlatiladigan belgilar (harflar, raqamlar, maxsus belgilar) ko‘pligi xavfsizlikni oshiradi.

3.Parolning tasodifiyligi: belgilarni inson mantiqiga asoslanmagan holda joylashtirish eng ishonchli natijani beradi.

Kombinatorika nuqtayi nazaridan parol kuchi (K) quyidagicha aniqlanadi:

Bu formula parolni buzish uchun kerak bo‘ladigan sinovlar (brutfors urinishlar) sonini bildiradi.

3.2. Misol: oddiy va murakkab parollarni solishtirish

Quyidagi jadvalda turli belgilar to‘plamlaridan tuzilgan parollarning umumiy kombinatsiyalar soni ko‘rsatilgan:

Parol turi
Belgilar to‘plami (k)
Uzunlik (n)
Umumiy kombinatsiyalar soni
Taxminiy buzish vaqti*
Faqat raqamli
10
6
$10^6 = 1\ 000\ 000$
≈ 0.001 sekund
Kichik harflar
26
6
$26^6 = 308\ 915\ 776$
≈ 0.3 sekund
Harflar + raqamlar
36
8
$36^8 = 2.8\times10^{12}$
≈ 45 minut
Harflar + raqamlar + maxsus belgilar
62
10
$62^{10} = 8.4\times10^{17}$
≈ 260 yil
Harflar, raqamlar, belgilar (tasodifiy)
94
12
$94^{12} = 4.7\times10^{23}$
≈ 10^{14} yil
Копировать таблицу

*Hisoblashda sekundiga 10^9 (bir milliard) urinish amalga oshiruvchi zamonaviy superkompyuter qabul qilingan.

Bu misol shuni ko‘rsatadiki, belgilar turini va parol uzunligini oshirish orqali parolni buzish ehtimoli eksponentsial tarzda kamayadi. Kombinatorika esa bu jarayonni matematik asosda tahlil qilish imkonini beradi.

3.3. Ehtimollik asosida xavfsizlik darajasini baholash

Agar foydalanuvchi tasodifiy parol tanlasa, uni bir urinishda to‘g‘ri topish ehtimoli quyidagicha bo‘ladi:

Masalan, agar parol 10 belgidan iborat bo‘lib, 62 turdagi belgidan tanlansa:

ya’ni ehtimol 0.00000000000000000119 atrofida.

Bu shunchalik kichik ehtimolki, amaliy jihatdan bu parolni to‘g‘ri topish imkonsizga yaqin hisoblanadi.

Shu sababli, xavfsizlik siyosatlarini ishlab chiqishda tashkilotlar minimal uzunlik (masalan, 10 belgidan kam bo‘lmasin) va belgilar xilma-xilligini talab qiladi. Bu talablar to‘g‘ridan to‘g‘ri kombinatorika asosida belgilanadi.

3.4. Brutfors hujumining matematik modeli

Brutfors (brute-force) hujumi — bu barcha mumkin bo‘lgan parol kombinatsiyalarini ketma-ket sinab chiqish usulidir. Kombinatorika yordamida bu hujumning vaqt talabini aniqlash mumkin:

bu yerda:

•

k — belgilar to‘plami hajmi,

•

n — parol uzunligi,

•

S — kompyuter sekundiga bajaradigan sinovlar soni.

Masalan, 62 belgidan 8 belgili parol uchun:

Agar parol uzunligi 10 belgi bo‘lsa:

Shunday qilib, har bir qo‘shimcha belgi nafaqat matematik kombinatsiyalar sonini, balki himoya vaqtini ham keskin oshiradi.

3.5. Kombinatorika va inson psixologiyasi o‘rtasidagi bog‘liqlik

Qiziqarli jihati shundaki, ko‘pchilik foydalanuvchilar parollarni matematik tasodifiylikka emas, psixologik yodda saqlash qulayligiga asoslanib tanlaydi. Masalan,

tug‘ilgan yil, ism, “12345”, “qwerty”, “Umar2005” kabi parollar inson uchun oson, lekin kombinatorika nuqtayi nazardan zaif hisoblanadi.

Bu holatda kombinatorika nafaqat matematik hisoblash, balki foydalanuvchi xatti-harakatini modellashtirish uchun ham qo‘llaniladi. Sun’iy intellekt asosidagi “password pattern analyzer” algoritmlari foydalanuvchi psixologik modelini tahlil qilib, qaysi kombinatsiyalar tez topilishini oldindan baholaydi.

3.6. Parol yaratishda kombinatorik strategiyalar

Kombinatorika asosida samarali parollar yaratish uchun quyidagi strategiyalar tavsiya etiladi:

1. Belgilar sonini oshirish: kamida 10–12 belgi.

2. Turli toifali belgilarni aralashtirish: harflar (katta va kichik), raqamlar, belgilar.

3.Tartibsizlikni ta’minlash: belgilar o‘rtasida mantiqiy bog‘lanish bo‘lmasin.

4.Yangi kombinatsiyalar yaratish: parol generatorlaridan foydalanish.

5.Davriy yangilash: bir paroldan uzoq muddat foydalanmaslik.

Bu tamoyillar kombinatorika qonunlariga asoslanadi, ya’ni parollar sonini maksimal darajada ko‘paytirish orqali ularni buzish ehtimolini minimal darajaga tushirish maqsadida qo‘llaniladi.

3.7. Kombinatorik yondashuvlar asosida xavfsizlik siyosati

Ko‘pgina xalqaro tashkilotlar (masalan, ISO/IEC 27001, NIST SP 800-63B) parol siyosatini matematik kombinatsiyalar tahliliga asoslaydi. Ularning umumiy tavsiyalari:

• Parollar kamida 8–10 belgidan iborat bo‘lsin;

• Belgilar to‘plamida kamida 4 xil tur (katta harf, kichik harf, raqam, maxsus belgi) qatnashsin;

• Parollar tasodifiy generator yordamida yaratilgan bo‘lsin;

• Parollarni takror ishlatish taqiqlansin.

Bularning barchasi kombinatorika va ehtimollik nazariyasining real amaliyotdagi qo‘llanilishidir.

Xulosa (bo‘lim yakuni uchun)

Parol tanlashda kombinatorika nafaqat matematik hisob-kitob vositasi, balki xavfsizlik darajasini baholovchi ilmiy modeldir. Parolning har bir belgisi tizimni himoya qiluvchi omilga aylanadi. Belgilar soni, uzunligi va xilma-xilligi oshgani sayin, kombinatsiyalar soni geometrik tarzda ortadi, bu esa parolni buzishni amalda imkonsiz qiladi.

Demak, kombinatorika parollarni tanlash, tekshirish va tahlil qilish jarayonlarida ishonchli matematik poydevor bo‘lib xizmat qiladi.

4. Brutfors hujumlariga qarshi matematik himoya mexanizmlari

Brutfors (brute-force) hujumi — barcha mumkin bo‘lgan parol kombinatsiyalarini ketma-ket sinash orqali to‘g‘ri parolni topishga yo‘naltirilgan algoritmik hujum turidir. Kombinatorika yordamida brutfors hujumining qancha vaqt talab qilishini oldindan baholash mumkin edi (oldingi bo‘limlardagi formulasi). Ammo amaliy tizimlar faqat kombinatsiyalar sonini oshirish bilan cheklanmay, turli matematik va arxitektura-darajadagi mexanizmlardan foydalanib brutfors hujumlarini samarali cheklaydi. Quyida asosiy himoya mexanizmlari, ularning kombinatorik mantiqi va amaliy tavsiyalari keltiriladi.

4.1. Parolni saqlash: xeshlash, solishtirish va solishtirish xarajatlari (cost factor)

Hash + salt — asosiy nazariy poydevor

Parolni oddiy matn (plaintext) shaklida saqlash xatolikdir. Xesh funktsiyasi (one-way hash) parolni bitta yo‘nalishda kodlab beradi — xeshdan asl parolni qaytarish amalda imkonsiz bo‘lishi kerak. Biroq, oddiy tez xeshlar (masalan, MD5 yoki SHA-1 atributilarida oddiy, tez hisoblash uchun mo‘ljallangan variantlar) zamonaviy xususiylashtirilgan apparat yordamida tezda sinovdan o‘tkazilishi mumkin. Shu bois ikki qo‘shimcha chora talab qilinadi:

1. Salt (tuz): har bir foydalanuvchi uchun noyob, tasodifiy qiymat. Salt xesh jarayoniga qo‘shilganda, bir xil parolga ega foydalanuvchilar ham turlicha xeshga ega bo‘ladi va lug‘at/jadval (rainbow table) hujumlari samarasi yo‘qoladi.

Misol formulasi:

2. Cost factor (ishlab chiqarish qiyinchiligi): xeshni hisoblashni qasddan sekinlashtirish — har bir sinovning vaqt yoki xotira xarajatlarini oshirish. Bu brutfors hujumlari uchun samarali to‘siq yaratadi.

Memory-hard va compute-hard xeshlar

• Compute-hard (CPU-bound): masalan, bcrypt — hisoblash xarajatini oshirishga mo‘ljallangan.

• Memory-hard (RAM-bound): scrypt va Argon2 kabi algoritmlar GPU/ASIC/FPGA ustunliklarini kamaytirish uchun katta miqdorda ishlovchi xotirani talab qiladi.

Amaliy tavsiya: parol saqlashda har doim salt bilan birgalikda zamonaviy adaptive hashing (masalan, Argon2 yoki scrypt yoki kamida bcrypt) ishlatilishi kerak; cost parametrlari vaqt o'tishi bilan yangilanib borishi kerak (server kuchiga mos ravishda).

4.2. Key stretching (kalit cho‘zish) va iteratsiyalar

Key stretching — paroldan dastlabki xesh olishni bir nechta iteratsiyalar orqali amalga oshirish. Iteratsiyalar sonini oshirish har bir sinov vaqtini ko‘paytiradi (ya’ni kamayadi), shuning uchun brutfors uchun umumiy vaqt oshadi:

Cost multiplier — iteratsiyalar yoki memory-hard resurslar tufayli pasaygan sinov tezligi.

Misol: agar oddiy hisoblash 10^9 urinish/s bo‘lgan bo‘lsa va xesh cost factor tufayli har bir sinov 100 marta sekinroq bo‘lsa, samarali S ≈ 10^7 urinish/s bo‘ladi — shu bilan parolni buzish vaqti 100 barobar oshadi.

4.3. Salt va Pepper — uniqlik va qo‘shimcha sir (secret)

• Salt — foydalanuvchiga xos, odatda ommaga ma’lum (ya’ni xesh bilan birga saqlanadi) bo‘lib, rainbow table hujumlarini bekor qiladi.

• Pepper — server tomonidan maxfiy saqlanadigan umumiy kalit (masalan, servis darajasidagi sir), xeshga qo‘shiladi, lekin bazada saqlanmaydi. Agar xaker faqat ma’lumotlar bazasini qo‘lga kiritgan bo‘lsa, pepper bo‘lmasa xeshni qayta ishlash qiyinroq bo‘ladi. Pepper ham xavf-xatarlar bilan — uni nima qilsa bo‘ladi? — pepper server yoki HSM (Hardware Security Module) ichida saqlanishi kerak.

Formula (pepper bilan):

4.4. Hisobga olish va tezlikni cheklash: throttle, lockout, progressive delay

Brutforsni tizim resurslari chegaralaridan foydalanib sekinlashtirish mumkin.

•Progressive delay (bosqichma-bosqich kechikish): har bir noto‘g‘ri urinilishdan keyin keyingi urinish uchun kutish vaqtini eksponentsial oshirish (masalan, 1s, 2s, 4s, 8s...). Bu yondashuv automatlashtirilgan hujumlar uchun juda qiyin sharoit yaratadi.

•Account lockout (bloklash): ma’lum miqdordagi xato urinishidan so‘ng hisobni vaqtincha yoki doimiy bloklash. Tavsiya: qattiq bloklashdan ko‘ra, foydalanuvchini bildirish va MFA so‘rash muammolarni kamaytiradi.

•IP-based rate limiting: bir IP manzildan kelayotgan urinishlar sonini cheklash. Lekin hujumchilar ko‘pincha botnet yoki proxy orqali tarqalgan manbalarni foydalanadi — shuning uchun IP-limiting yagona chorasi emas.

• CAPTCHA qo‘shish: avtomatlashtirilgan skriptlarni aniqlash va bloklashda yordam beradi — ayniqsa login endpointlarda.

Amaliy tavsiya: kombinatsiyalangan yondashuv — progressive delay + CAPTCHA + risk-based MFA. Lockout faqat ekzotik holatlar uchun yoki ko‘p xatar kuzatilganda qo‘llansin.

4.5. Parollarni tekshirish: blacklisting va pattern checking

Kombinatorika jihatidan, bir qancha parollar juda tez-tez ishlatiladi (masalan, “123456”, “password”). Bu “cho‘plar” (popular patterns) kombinatorik hisob-kitobni sezilarli darajada kamaytiradi: samarali dan ma’lum tanlangan subset tezroq sinovdan o‘tadi. Shu sababli:

• Blacklisting: eng ko‘p ishlatiladigan va zaif parollar ro‘yxatini qabul qilmaslik.

• Pattern checking: “Ism+year”, “qwerty” kabi naqshlarni aniqlash va rad etish.

• Leaked password check: foydalanuvchi tanlagan parolni ilgari ma’lumotlar bazasidan o‘g‘irlangan parollar ro‘yxatida tekshirish (agar topilsa, parolni rad etish).

Bu yondashuvlar kombinatorik nuqtai nazardan foydalanuvchi erkinligini biroz qisqartirishi mumkin, lekin real himoya samarasi yuqori.

4.6. Ko‘p bosqichli autentifikatsiya (MFA) — kombinatorik himoyaning kengaytirilishi

Parol faqatgina «bir faktor». Kombinatorika bo‘yicha tizim xavfsizligini oshirish uchun qo‘shimcha mustaqil faktorlar qo‘shiladi (narsaga ega bo‘lish — token, nimagadir bilish — parol, yoki kimlikni tasdiqlovchi — biometrik). Agar har bir faktor mustaqil bo‘lsa, umumiy kombinasiyalar va shu orqali hujum muvaffaqiyati ehtimoli kamayadi — rasmiy kombinatorik model quyidagicha:

Agar hujumchi barcha mustaqil faktorlardan o‘tishi kerak bo‘lsa, umumiy muvaffaqiyat ehtimoli barchasining ko‘paytmasi bo‘ladi:

bu yerda

— i-chi faktor bo‘yicha muvaffaqiyat ehtimoli. Parolning o‘zi juda kichik ga ega bo‘lsa ham, MFA yordamida bu ehtimol yanada kichrayadi.

Amaliy tavsiya: muhim tizimlar uchun kamida ikki faktorli autentifikatsiya (parol + OTP / yuborilgan kod / token / biometric) joriy etilsin.

4.7. Honeywords va honeypotlar — pasaytirilgan kombinatorik signal

Honeywords — agar hisobga bir nechta (masalan, N) parol varianti bilan kirishga ruxsat berilgan bo‘lsa, faqat bittasi haqiqiy bo‘lsa, va qolganlari «honeyword» bo‘lsa, buzilganlik holati osongina aniqlanadi. Honeyword tushunchasi kombinatorika orqali ishlaydi: xaker noto‘g‘ri variantni ishlatganda, tizim darhol buzilish signalini beradi.

Honeypot login endpoints — alohida monitoring qilingan soxta login endpointlar. Agar ular orqali urinish bo‘lsa, tizim hujum boshlanganini aniqlaydi.

4.8. Parol menejerlari va tasodifiy generatorlar

Kombinatorika asosida eng ishonchli parollar — tasodifiy generatsiyalangan uzun ketma-ketliklar. Parol menejerlari foydalanuvchiga qiyin lekin eslab qolishning hojati bo‘lmagan kombinatorik jihatdan kuchli parollar yaratishi va saqlashini ta’minlaydi. Tizimlar uchun esa:

• Kompulsoriy random generator tavsiyasi: foydalanuvchi uchun tavsiya etilgan generatorlar yoki avtomatik yaratilgan parollar.

• Entropy hisoblash: parolni qabul qilishdan oldin uning entropiyasini (bitlarda) hisoblab, minimal entropiya talabini qo‘yish.

Entropiya formulasi:

Masalan, 12 ta belgidan iborat parol, k = 94 uchun:

Bu xavfsizlik nuqtai nazaridan juda kuchli hisoblanadi.

4.9. Real dunyo cheklovlari va xavf-menejment: cost vs. usability tradeoff

Himoya choralari — doimo foydalanuvchi qulayligi (usability) bilan muvozanatda bo‘lishi kerak:

• Juda og‘ir cost factor (xeshni juda sekinlatish) server resurslarini va autentifikatsiya tezligini pasaytiradi — bu yomon foydalanuvchi tajribasiga olib keladi.

• Qattiq password policy (har doim katta parol va qoidalar) foydalanuvchilarni parollarni yozib qo‘yishga yoki pattern-ga qaytishga majbur qilishi mumkin.

• Lockout siyosati esa xizmatning xizmat ko‘rsatish qobiliyatini (DoS) zaiflashtirishi mumkin.

Xulosa: kombinatorik himoya mexanizmlarini joriy etishda xavf-menejment yondashuvi qo‘llanilishi kerak — xavf baholash (risk assessment) asosida cost parametrlari, MFA tarkibi va siyosatlar belgilansin.

4.10. Taklif etiladigan amaliy parametrlar va bosqichli chora-tadbirlar (qisqacha)

Quyidagi parametrlar — tavsiya xabarlari sifatida beriladi va tizimingiz kuchiga hamda foydalanuvchi kontekstiga qarab moslashtirilishi kerak.

1. Parollarni saqlash: Argon2 (agar mumkin bo‘lsa) yoki scrypt / bcrypt. Har doim unik salt (kamida 16 bayt) va iloji bo‘lsa pepper (HSM ichida).

2. Cost factor: server yukiga mos ravishda o‘rnatilsin — har bir xesh hisoblash taxminan 100–500 ms bo‘lsa, foydalanuvchi uchun maqbul (login taxminan 100–300 ms).

3. Rate limiting: IP va account-darajasida progressiv kechikish, 5–10 noto‘g‘ri urinilishdan keyin CAPTCHA va MFA chaqirish.

4. Blacklist va leaked password check: yangi parol qabul qilganda tekshirish.

5. MFA: muhim hisoblar uchun majburiy ikki faktor.

6. Parol menejerlari: tashkilot ichida tavsiya qilish va yordam (guruh siyosati).

7. Monitoring: honeypotlar va honeywords joriy etish, anomaliyalarni real-time kuzatish.

Bo‘lim xulosasi

Kombinatorika brutfors hujumining asosiy raqamli o‘lchovlarini beradi — barcha mumkin kombinatsiyalar soni va shu asosida zarur vaqtni hisoblash mumkin. Ammo amaliy himoya kombinatorika bilan bir qatorda tizim-darajadagi mexanizmlar (salt, adaptive hashing, memory-hard funktsiyalar, rate limiting, MFA, honeywords va boshqalar) orqali amalga oshiriladi. Optimal himoya — bu kombinatorikaning matematik printsiplarini amaliy choralarga aylantirish va foydalanuvchi qulayligi bilan muvozanatlashdir.

Xulosa

Ushbu maqolada parollarni himoyalashda kombinatorikaning nazariy va amaliy roli batafsil tahlil qilindi. Kombinatorika parol tizimlarining matematik poydevorini tashkil etib, parol uzunligi, belgi to‘plami va tasodifiylik kabi omillar orqali mumkin bo‘lgan kombinatsiyalar soni va parolni buzish ehtimolini aniq ifodalaydi. Oddiy

formulalar (masalan,) yordamida parol kuchi va uning entropiyasi sonli jihatdan baholanadi; har bir qo‘shimcha belgi yoki belgi turining ko‘payishi himoya muddatini eksponentsial ravishda oshirishini ko‘rsatadi.

Amaliy jihatdan esa kombinatorik hisob-kitoblar brutfors va lug‘at hujumlarining samaradorligini oldindan baholashda muhim vosita hisoblanadi. Biroq yagona matematik yondashuv yetarli emas: tizimlar salt, pepper va adaptive hashing (Argon2, scrypt, bcrypt) kabi usullarni qo‘shib, hisoblarga kirish tezligini oshirib yoki pasaytirib, hamda rate-limiting, progressive delay, blacklisting, honeywords va MFA orqali hujumlarni real dunyoda samarali to‘xtatadi. Shu tariqa kombinatorika nazariyasi va arxitektura-darajadagi himoya mexanizmlari birgalikda axborot xavfsizligini ta’minlaydi.

Amaliy tavsiyalar qisqacha: parol siyosatida minimal uzunlik va turli belgi turlarini talab qilish, parollarni salt bilan birga memory-hard hashing orqali saqlash, leaked-password tekshiruvi va blacklisting joriy etish, muhim hisoblarda MFA majburiy qilish hamda foydalanuvchilarga parol menejerlari va tasodifiy generatorlardan foydalanishni tavsiya etish lozim. Bu choralar kombinatorik jihatdan parollarni yanada ishonchli qiladi va amaliy hujumlarga qarshi samarali himoya ta’minlaydi.

Umuman olganda, kombinatorika — parollar xavfsizligini baholash va oshirish uchun zarur matematik vosita; lekin haqiqiy va bardoshli tizim yaratish uchun uni amaliy kriptografik chora-tadbirlar, foydalanuvchi xatti-harakatlarini inobatga oluvchi siyosatlar va doimiy monitoring bilan uyg‘unlashtirish talab etiladi.