

## **6 - AMALIY MASHG'ULOT. MA'LUMOTLAR YAXLITLIGINI TA'MINLASH YO'LLARI.**

**Ishdan maqsad:** Talabalarda ma'lumotlar yaxlitligini ta'minlash yo'llari bo'yicha bilim va ko'nikmalarini oshirish.

**Nazariy qism:** Ma'lumotlar yaxlitligi axborot xavfsizligining asosiy jihati bo'lib, ma'lumotlar butun hayoti davomida to'g'ri va buzilmasligini ta'minlaydi. Ma'lumotlar yaxlitligini ta'minlashning asosiy usullariga xeshlash, raqamli imzolar, nazorat summalari, ro'yxatga olish auditi, kriptografik ma'lumotlarni saqlash va zahira nusxalari kiradi. Ushbu ma'ruzada biz grafik nazariyasining asosiy tushunchalarini va ularning ma'lumotlar yaxlitligi texnikasi bilan qanday bog'liqligini ham ko'rib chiqamiz.

Ma'lumotlar yaxlitligi texnikasi quyidagilardan iborat:

### **1. Xeshlash**

Hashing - ma'lumotlar yaxlitligini ta'minlashning eng keng tarqalgan usullaridan biri. Bu jarayon o'zboshimchalik bilan uzun ma'lumotlarni xesh-kod deb ataladigan qattiq uzunlikdagi qatorga aylantiradi. Ma'lumotlarning kichik o'zgarishi ham xesh kodida sezilarli o'zgarishlarga olib keladi. Bu xeshni ma'lumotlardagi eng kichik o'zgarishlarni ham aniqlash uchun ideal usulga aylantiradi.

### **2. Elektron raqamli imzolar**

Raqamli imzolar autentifikatsiya va ma'lumotlar yaxlitligi uchun ishlatiladi. Imzo shaxsiy kalitni xabar xeshiga qo'llash orqali yaratiladi va natijada imzo mos keladigan ochiq kalit yordamida tekshirilishi mumkin. Imzo yaratilgandan keyin ma'lumotlarga kiritilgan har qanday o'zgarishlar imzoni bekor qiladi, bu esa qalbakilashtirish va o'zgarishlarni aniqlash imkonini beradi.

### **3. Tekshirish summalari**

Tekshirish summalari ma'lum bir algoritm yordamida ma'lumotlar tarkibidan hisoblangan raqamli qiymatlardir. Ular keyingi yaxlitlikni tekshirish uchun ma'lumotlarga yoki uning qismlariga qo'shiladi. Agar ma'lumotlarni tekshirish summasi hisoblangan qiymatga mos kelmasa, bu ma'lumotlarda xatolar yoki o'zgarishlar mavjudligini ko'rsatadi.

### **4. Ro'yxatga olish auditi**

Audit jurnali keyinchalik tahlil qilish va yaxlitlikni tekshirish uchun barcha ma'lumotlar operatsiyalarini yozib olishni o'z ichiga oladi. Bu ma'lumotlarning yaxlitligiga ta'sir qilishi mumkin bo'lgan har qanday ruxsatsiz harakatlar yoki xatolarni aniqlash imkonini beradi. Audit jurnallaridan ma'lumotlar buzilgan yoki yo'qolgan bo'lsa, ularni tiklash uchun ham foydalanish mumkin.

## ***5. Kriptografik ma'lumotlarni saqlash***

Kriptografik ma'lumotlar do'konlari ma'lumotlarni ruxsatsiz kirish va o'zgarishlardan himoya qilish uchun shifrlash mexanizmlaridan foydalanadi. Ma'lumotlar shifrlangan shaklda saqlanadi, bu esa tegishli kirish kalitlarisiz foydalanishga yaroqsiz holga keltiradi. Bu ruxsatsiz o'zgartirishlarning oldini olish orqali ma'lumotlarning yaxlitligini ta'minlaydi.

## ***6. Ma'lumotlarning zahira nusxalari***

Ma'lumotlarning zaxira nusxalari - bu shikastlangan yoki yo'qolgan ma'lumotlarni qayta tiklashga imkon beruvchi muhim yaxlitlik usuli. Zaxira nusxalarini muntazam ravishda yaratish va saqlash qimmatli ma'lumotlarning yo'qolishining oldini olishga yordam beradi va kerak bo'lganda ma'lumotlarni qayta tiklashni ta'minlaydi.

Grafiklar nazariyasining asosiy tushunchalari quyidagilar:

### ***1. Grafiklar***

Grafiklar turli stsenariylarni va ob'ektlar orasidagi munosabatlarni modellashtirish uchun ishlatiladigan muhim matematik tushunchadir. Grafik - bu uchlari va qirralari to'plamidan tashkil topgan mavhum ma'lumotlar strukturasi. Cho'qqilar ob'ektlarni, qirralar esa bu ob'ektlar orasidagi bog'lanishlarni ifodalaydi.

### ***2. Cho'qqilar va qirralar***

Grafikning uchlari bir-biriga bog'lanishi mumkin bo'lgan alohida ob'ektlar yoki elementlarni ifodalaydi. Qirralarning o'zlari uchlari orasidagi bog'lanishlarni ifodalaydi. Qirralar ma'lum bir yo'nalishga ega bo'lishiga qarab yo'naltirilgan yoki yo'naltirilmagan bo'lishi mumkin.

### ***3. Yo'naltirilgan va yo'naltirilmagan grafiklar.***

Yo'naltirilgan grafiklar qirralarning ma'lum bir yo'nalishga ega bo'lishi bilan ajralib turadi. Bu cho'qqilar orasidagi aloqa faqat bitta yo'nalishda borishini anglatadi. Yo'naltirilmagan grafiklarda qirralarning yo'nalishi yo'q va cho'qqilar orasidagi bog'lanish ikki tomonlama hisoblanadi.

### ***4. Yo'l va siklik grafiklar.***

Yo'l grafigi - bu bir cho'qqidan ikkinchisiga yo'l bo'lgan grafik. Bu shuni anglatadiki, siz grafikning chetlari bo'ylab harakatlanish orqali bir cho'qqidan ikkinchisiga o'tishingiz mumkin. Tsiklik grafik esa tsikllarni, ya'ni boshlang'ich va oxiri bir xil bo'lgan cho'qqilar ketma-ketligini o'z ichiga oladi.

## ***Amaliy qism:***

### ***1. Ma'lumotlarni shifrlash:***

***Vazifa:*** Oddiy harflarni almashtirish (Sezar shifrlash) yordamida maxfiy xabarni shifrlang.

**Yechim:** Xabardagi har bir harfni alifbodagi boshqa harf bilan ma'lum bir qator pozitsiyalar bilan almashtiring. Harflarni bir xil masofaga qarama-qarshi yo'nalishda siljitish orqali xabarni hal qiling.

## **2. Ma'lumotlarni xeshlash:**

**Vazifa:** Ixtiyoriy matnli hujjat uchun xesh summasini hisoblang.

**Yechim:** Noyob xesh kodini olish uchun siz tanlagan xesh algoritmini (MD5 yoki SHA-256 kabi) hujjat tarkibiga qo'llang.

## **3. Raqamli imzolar:**

**Vazifa:** Ismingiz va sanangizdan iborat raqamli imzo yordamida xat uchun imzo yarating.

**Yechim:** Maktub mazmuniga ismingiz va sanangizni qo'shing, so'ng xabarga o'z imzongiz bilan imzo qo'ying.

## **4. Tekshiruv summolari:**

**Vazifa:** Har qanday o'zgarishlarni aniqlash uchun har safar nazorat summasini tekshirib, hujjat faylini tarmoq orqali o'tkazing.

**Yechim:** Yuborishdan oldin faylning nazorat summasini hisoblang, so'ngra faylni ham, nazorat summasini ham o'tkazing. Qabul qiluvchi faylni olgandan keyin nazorat summasini tekshirishi kerak.

## **5. Tranzaksiyalar va jurnallar:**

**Vazifa:** Mumkin bo'lgan muammolarni va operatsiyani orqaga qaytarishni hisobga olgan holda, do'konda mahsulot sotib olayotganda tranzaksiyani simulyatsiya qiling.

**Yechim:** Tovarni tanlashdan boshlab, uni savatga qo'shishdan, to'lov jarayonidan va mahsulotni qabul qilishgacha bo'lgan barcha bosqichlarini yozib oling. Muammo yuzaga kelsa, tizimni asl holatiga qaytarish uchun orqaga qaytarishni bajaring.

## **6. Grafik yaratish:**

**Vazifa:** Oila a'zolaringiz o'rtasidagi oilaviy munosabatlarni ko'rsatadigan oilaviy munosabatlar grafigini chizing.

**Yechim:** Qog'ozda yoki matn protsessorida har bir oila a'zosi uchun doiralar chizib, ularni ota-onalar va avlodlarga ishora qiluvchi o'qlar bilan bog'lang.

## **7. Yo'l topish:**

**Vazifa:** Bir nechta ko'chalardan o'tib, uyingizdan eng yaqin do'kongacha bo'lgan eng qisqa yo'lni toping.

**Yechim:** Hududingiz xaritasini o'rganing va burilishlar soni va masofani minimallashtirib, eng yaxshi marshrutni aniqlang.

## **8.To'g'riining darajasini aniqlash:**

**Vazifa:** Ijtimoiy tarmoqdagi har bir do'stingizning do'stlari sonini aniqlang.

**Yechim:** Yuqori darajani aniqlash uchun har bir do'stingizning profilini ko'rib chiqing va ularning do'stlari sonini hisoblang.

## **9.Grafik ulanishini tekshirish:**

**Vazifa:** Sayohat ro'yxatidagi har bir shaharga pul o'tkazmasdan borish mumkinligini tekshiring.

**Yechim:** Ro'yxatdagi barcha shaharlar orasidagi yo'nalishlarni o'rganing va har bir shaharga boshqa shaharlar orqali o'tmasdan yetib borish mumkinligiga ishonch hosil qiling.

## **10.Daraxt qurish:**

**Vazifa:** Sinfingiz a'zolari o'rtasidagi aloqalarni ko'rsatuvchi daraxt chizing.

**Yechim:** Har bir sinf a'zosi uchun doiralardan foydalaning va kim kim bilan bog'liqligini ko'rsatish uchun ularni chiziqlar bilan bog'lang. Faqat davrlarsiz daraxt hosil qiladigan ulanishlarni belgilang.

Ushbu amaliy mashqlar va misollar sizga dasturlash tillaridan foydalanmasdan ma'lumotlar yaxlitligi texnikasi va asosiy grafik nazariyasi tushunchalarini yaxshiroq tushunishga va qo'llashga yordam beradi.

### **Mustaqil bajarish uchun topshiriqlar**

1. Ma'lumotlar yaxlitligi nima va u nima uchun axborot xavfsizligi uchun muhim?
2. Ma'lumotlar yaxlitligini ta'minlashning qanday usullarini bilasiz?
3. Ma'lumotlarni shifrlash jarayoni qanday ishlaydi va shifrlashning qanday turlari mavjud?
4. Ma'lumotlarni xeshlash nima va eng keng tarqalgan xeshlash algoritmlari qanday?
5. Ma'lumotlar yaxlitligi va autentifikatsiyasini ta'minlash uchun raqamli imzolardan qanday foydalanish mumkin?
6. Axborotni tarmoq orqali uzatishda ma'lumotlar yaxlitligini nazorat qilishning qanday usullaridan foydalaniladi?
7. Ma'lumotlar bazalari kontekstidagi tranzaktsiyalar nima va ular ma'lumotlar yaxlitligini ta'minlashga qanday yordam beradi?

8. Yo'naltirilgan va yo'naltirilmagan grafiklarning farqi nimada?
9. Grafiklar nazariyasi qanday asosiy tushunchalarni o'z ichiga oladi?
10. Grafikda cho'qqining darajasi qanday aniqlanadi?
11. Grafikdagi eng qisqa yo'lni topish uchun qanday algoritmlardan foydalaniladi?
12. Grafikning barcha uchlarini kesib o'tmasdan uning bog'lanishini qanday tekshirish mumkin?
13. Grafiklarni tasvirlashning qanday usullari mavjud?
14. Berilgan grafik uchun minimal kenglikdagi daraxt qanday quriladi?
15. Axborot texnologiyalari va ma'lumotlar fanida grafiklar nazariyasining qanday qo'llanilishini topishingiz mumkin?