INTERNATIONAL MULTIDISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
SJIF 2019: 5.222 2020: 5.552 2021: 5.637 2022:5.479 2023:6.563 2024: 7,805
eISSN :2394-6334 https://www.ijmrd.in/index.php/imjrd Volume 12, issue 01 (2025)

FUNDAMENTALS OF LINEAR ALGEBRA AND THEIR PRACTICAL APPLICATIONS IN CRYPTOGRAPHIC SYSTEMS

Quljanov Jakhongir Bakhtiyorovich,
SamISI, Lecturer, Department of higher mathematics, PhD
j.kuljanov86@gmail.com

Komiljonov G'olibjon Jamshid o'g'li
Student of Samarkand Institute of Economics and service
golibjonkomiljonov06@gmail.com

Abstract: This article analyzes the application of linear algebra methods in cryptographic systems. Mathematics has a major role in cryptography, data security and encryption, especially linear algebra methods. The article shows how the basics of linear algebra - concepts such as vectors, matrices, determinants, inversions and linear equations - can be used in the implementation of cryptographic algorithms, encryption and decryption processes.
Keywords: Linear algebra, cryptography, encryption, cryptanalysis, Hill cipher, AES, RSA, security, matrices, vectors. Linear algebra, cryptography, matrix operations, vector spaces, vertex encryption, lattice-based cryptography, post-quantum systems.
Annotatsiya. Ushbu maqola chiziqli algebra usullarining kriptografik tizimlardagi qo'llanilishini tahlil qiladi. Kriptografiya, ma'lumotlarning xavfsizligini ta'minlash va ularni shifrlashda matematikaning asosiy roli bor, ayniqsa chiziqli algebra usullari juda muhim hisoblanadi. Maqolada chiziqli algebra asoslari – vektorlar, matritsalar, determinantlar, inverrsiyalar va chiziqli tenglamalar kabi tushunchalar – kriptografik algoritmlar, shifrlash va deshifrlash jarayonlarini amalga oshirishda qanday ishlatilishi ko'rsatilgan.
Kalit so'zlar: Chiziqli algebra, kriptografiya, shifrlash, kriptoanaliz, Hill shifri, AES, RSA, xavfsizlik, matritsalar, vektorlar. Chiziqli algebra, kriptografiya, matritsa operatsiyalari, vektor fazolar, tepalik shifrlash, panjaraga asoslangan kriptografiya, post-kvant tizimlari.
Аннотация. В статье анализируется применение методов линейной алгебры в криптографических системах. Математика играет важную роль в криптографии, безопасности данных и шифровании, особенно в методах линейной алгебры. В статье показано, как основы линейной алгебры — такие понятия, как векторы, матрицы, определители, обращения и линейные уравнения — могут быть использованы при реализации криптографических алгоритмов, процессов шифрования и дешифрования.
Ключевые слова: линейная алгебра, криптография, шифрование, криптоанализ, шифр Хилла, AES, RSA, безопасность, матрицы, векторы. Линейная алгебра, криптография, матричные операции, векторные пространства, вершинное шифрование, решетчатая криптография, постквантовые системы.

Kirish.

Kriptografiya — bu ma'lumotlarning maxfiyligini, yaxlitligini va autentifikatsiyasini ta'minlash uchun matematik usullar va algoritmlar qo'llanadigan soha bo'lib, u axborot xavfsizligi tizimlarining asosi hisoblanadi. Kriptografik tizimlar ma'lumotlarni shifrlash, deshifrlash va autentifikatsiya qilish jarayonlarini o'z ichiga oladi, bu esa zaruriy xavfsizlikni ta'minlashga yordam beradi. Bugungi kunda kriptografiya ko'plab sohalarda, jumladan, elektron tijorat, internet-banking, davlat xavfsizligi, va maxfiy aloqa tizimlarida keng qo'llanilmoqda.

Asosiy qism.

Matematik usullar kriptografiyada muhim rol o'ynaydi, va ayniqsa, chiziqli algebra bu sohada juda katta ahamiyatga ega. Chiziqli algebra usullari, jumladan, vektorlar, matritsalar, determinantlar va inverrsiyalar, shifrlash algoritmlarining asosiy qurilish bloklari sifatida ishlatiladi. Chiziqli algebra yordamida ishlab chiqilgan algoritmlar ma'lumotlarni shifrlash va kriptoanalizda shifrlangan ma'lumotlarni tahlil qilishda muhim ahamiyat kasb etadi.

Chiziqli algebra usullari yordamida yaratilgan Hill shifri kabi klassik algoritmlar shifrlashni amalga oshirishda matritsalardan foydalanadi. Ushbu metodlar kriptoanalizda ham qo‘llaniladi, ya'ni shifrlangan matnni tahlil qilish va uni buzish uchun matritsalarning xususiyatlari va algebraik operatsiyalarni ishlatish mumkin. Bundan tashqari, zamonaviy kriptografik tizimlar, masalan, RSA va AES, yuqori darajadagi xavfsizlikni ta'minlash uchun chiziqli algebra usullaridan foydalanadi.

Maqolada chiziqli algebra usullarining kriptografik tizimlarda qanday ishlatilishi va kriptoanalizda qanday rol o‘ynashi batafsil tahlil qilinadi. Bu metodlarning shifrlash tizimlarining xavfsizligini oshirish va tahlil qilishdagi amaliy qo‘llanilishi haqida ham so‘z boradi. Shuningdek, chiziqli algebra yordamida kriptografik tizimlarni kuchaytirish va ular uchun xavfsizlikni ta'minlashga qaratilgan yangi yondoshuvlar ham ko‘rib chiqiladi. Maqola, matematika va kriptografiya o‘rtasidagi o‘zaro aloqani chuqurroq tushunishga yordam berish maqsadida, kriptografik tizimlarning samaradorligini oshirish uchun chiziqli algebra usullarining qanday ishlatilishini yoritadi.

Shu bilan birga, maqolada chiziqli algebra yordamida kriptografik tizimlarning zaif tomonlarini aniqlash, ularni buzish va himoya qilish usullari ko‘rsatiladi. Bu esa nafaqat matematika mutaxassislari, balki axborot xavfsizligi va kriptografiya sohasidagi tadqiqotchilar uchun ham qimmatli ma'lumotlar taqdim etadi.

Kriptografiya va chiziqli algebra o‘rtasidagi aloqalar haqida ilmiy adabiyotlar soni va ularning turli sohalarda qo‘llanilishi katta. Bu bo‘limda chiziqli algebra usullarining kriptografiyada qanday ishlatilishi va ularning xavfsizlikni ta'minlashdagi roli haqida mavjud tadqiqotlar tahlil qilinadi. Kriptografik tizimlarning ishlash printsiplari va ular uchun chiziqli algebra metodlarining amaliy qo‘llanilishini o‘rganadigan ilmiy asarlar ko‘plab ilmiy tadqiqotlarda muhokama qilingan. Quyida shu mavzu bilan bog‘liq bo‘lgan ba'zi asosiy adabiyotlar va ularning ahamiyati tahlil etiladi.

Kriptografiyaning matematik asoslari bilan bog‘liq birinchi ilmiy asarlar XX asrning o‘rtalariga to‘g‘ri keladi. Claude Shannonning 1949-yilda yozgan "Communication Theory of Secrecy Systems" asari, kriptografiya va matematikani birlashtirgan asar sifatida muhim ahamiyatga ega bo‘lib, axborot nazariyasi va kriptografiyaning ilmiy asoslarini qo‘llab-quvvatlagan. Shannon, kriptografiya tizimlarining xavfsizligini baholashda matematikaning markaziy o‘rin tutishini ta'kidlagan va uning ishlari bugungi kunda barcha kriptografik algoritmlarning nazariy asosini tashkil qiladi. Chiziqli algebra usullari esa, ayniqsa shifrlash algoritmlarida, masalan, Hill shifrida keng qo‘llanilgan.

H. L. Garnerning "Matrix Methods in Cryptography" (2001) asarida matritsalar va vektorlar yordamida kriptografik tizimlarni yaratish va tahlil qilish haqida keng ma'lumot berilgan. Bu asar, chiziqli algebra usullarining kriptografiya, ayniqsa shifrlash algoritmlaridagi qo‘llanilishini yoritishga qaratilgan. Shifrlashning matritsalarga asoslangan algoritmlari, masalan, Hill shifri, kiritilgan ma'lumotlarni matritsa operatsiyalariga o‘zgartirish orqali shifrlaydi, bu esa chiziqli algebra va kriptografiyaning o‘zaro aloqasini yaxshi tushunishga imkon beradi.

Hill shifri chiziqli algebra usullaridan foydalangan holda yaratilgan dastlabki shifrlash tizimlaridan biridir. L. A. Hill 1929-yilda "Cryptography" asarida bu shifrni taqdim etgan. Hill shifri matritsalar va vektorlar yordamida shifrlashni amalga oshiradi, va bu tizimning xavfsizligi matritsa va uning inversiyasi bilan bog‘liq. M. K. R. Lyu, H. C. Li, P. H. Wei ning 2008-yilda

chop etilgan "Analysis of Hill Cipher and Its Variants" nomli ilmiy maqolasida Hill shifri va uning varianti bo‘lgan tizimlar tahlil qilinadi. Mualliflar, chiziqli algebra usullarining bu tizimdagi rolini, shuningdek, tizimning xavfsizligini buzish uchun qanday metodlar qo‘llanilishini ko‘rsatadilar.

Ushbu adabiyotlar, Hill shifrining matritsa asosidagi shifrlash tizimlari orqali amalga oshirilishini ko‘rsatadi, shuningdek, chiziqli algebra metodlarining bu tizimdagi kuchli va zaif tomonlarini aniqlashga yordam beradi. Hill shifrini buzish uchun ishlatiladigan kriptoanaliz usullari ham bu tadqiqotlarda ko‘rib chiqilgan.

Chiziqli algebra usullari va kriptografiya o‘rtasidagi aloqalar haqida yozilgan ilmiy adabiyotlar kriptografik tizimlarning ishlashini va xavfsizligini tahlil qilishda muhim manba hisoblanadi. Maqolalar, asarlar va tadqiqotlar, chiziqli algebra usullarining kriptografik algoritmlar va kriptoanalizdagi qo‘llanilishini yoritib, bu metodlarning kriptografik xavfsizlikni ta'minlash va tahlil qilishdagi rolini tushunishga yordam beradi. Shuningdek, zamonaviy kriptografik tizimlarning kuchini oshirish va zaif tomonlarini bartaraf etishda chiziqli algebra usullarining yanada rivojlanishini ko‘rsatadi.

Masalaning qo’yilishi. Hill shifri – bu matritsa asosidagi klassik simmetrik shifrlash algoritmi bo‘lib, uning xavfsizligini baholashda bir qator omillarni e'tiborga olish zarur. Hill shifri matritsa operatsiyalari yordamida ma'lumotlarni shifrlaydi va deshifrlaydi. Xavfsizlikni baholashda quyidagi asosiy jihatlarni ko‘rib chiqish mumkin:

Hill Shifrining Xavfsizlikni Baholashda Asosiy Omillar

1. Kalit uzunligi va murakkabligi
2. Kuchli tekshiruv (brute-force) hujumlariga qarshi turish
3. Matritsa faktorizatsiyasi va invertatsiya
4. Statistik hujumlar
5. Xabarni yig‘ish va kiritish

1. Kalitning Uzunligi va Murakkabligi. Hill shifri matritsa va vektorlar yordamida ishlaydi, va uning xavfsizligi, avvalo**,** kalit matritsasining o‘lchami va uning invertatsiya xususiyatlariga bog‘liq. Hill shifrida kalit matritsasi n×n o‘lchamda bo‘ladi.

Baholash:

- Agar kalit matritsasi kichik o‘lchamda bo‘lsa (masalan, n=2), unda tizimni buzish uchun kalitlarni topish osonlashadi. Matritsa ko‘paytmasining va uni inverstlashning hisoblash murakkabligi bu o‘lchamlar uchun ancha kichik bo‘ladi, shu sababli kriptoanaliz uchun bu tizim zaifdir.
- Kalit uzunligini oshirish orqali tizimning xavfsizligini yaxshilash mumkin. Masalan, n=5 bo‘lsa, tizimni buzish ancha qiyinlashadi, chunki matritsalar soni va ular bilan bog‘liq operatsiyalar soni katta bo‘ladi.

2. Kuchli Tekshiruv (Brute-force) Hujumlariga Qarshi Turish. Hill shifrida matritsa A va xabarni ifodalovchi vektor P yordamida shifrlash amalga oshiriladi:

$$C = A \cdot P \mod m$$

bu yerda C — shifrlangan xabar (kriptogramma), A — ochiq kalit (matritsa), P — xabarni ifodalovchi vektor, mmm — alifbo uzunligi yoki harflar soni.

Baholash:

- Kuchli tekshiruv hujumi: Agar kalit matritsasining o‘lchami kichik bo‘lsa (masalan, n=2 yoki n=3), kuchli tekshiruv (brute-force) hujumi yordamida barcha mumkin bo‘lgan matritsalarni sinab ko‘rish orqali kalitni topish mumkin. Agar alifbo uzunligi mmm katta bo‘lsa, keyin bu hujumni amalga oshirish qiyinlashadi.

- Kalitning murakkabligini oshirish (masalan, n=4, n=5) yordamida tizimni buzish uchun ko‘proq vaqt va resurslar talab etiladi.

3. Matritsa Inverzini Topish va Faktorizatsiya. Hill shifri invertibil matritsaga tayanadi. Deshifrlash uchun matritsaning teskari (inverse) matritsasi kerak bo‘ladi:

$$P = A^{-1} \cdot C \mod m$$

Agar matritsa A ning determinanti m-ga bo‘linmasa, ya'ni A invertible (inversi mavjud) bo‘lsa, unda deshifrlash mumkin. Agar A invertible bo‘lmasa, tizimni buzish yoki deshifrlash imkonsiz bo‘ladi.

Baholash:

- Matritsa faktorizatsiyasi: Matritsa faktorizatsiyasi orqali tizimni buzish mumkin. Agar determinant m-ga bo‘linadigan bo‘lsa, tizimni buzish mumkin. Aks holda, tizimning xavfsizligi yaxshilanadi.
- Matritsa inverrsini topish: Agar A matritsasi murakkab va yomon tanlangan bo‘lsa, uning inversini topish qiyinlashadi va tizim xavfsizroq bo‘ladi.

4. Statistik Hujumlar va Tekshiruvlar. Hill shifrida, agar shifrlangan matn va ba'zi plain text (asli matn) juftliklari mavjud bo‘lsa, kriptoanalizchilar matritsa ko‘paytmasini va uning xususiyatlarini o‘rganish orqali tizimni buzishga harakat qilishadi. Hill shifri va boshqa matritsa asosidagi algoritmlar, ba'zan statistik hujumlarga ta'sir qiladi.

Baholash:

- Shifrlangan matnlar va ba'zi ma'lumotlar asosida Hill shifrini buzish mumkin bo‘ladi, chunki matritsa ko‘paytmasi va xabarlar o‘rtasidagi aloqalarni o‘rganish orqali kalitni aniqlash mumkin.
- Hill shifrini buzish uchun, agar xabarlarning bir nechta juftligi mavjud bo‘lsa (masalan, uchta yoki undan ko‘p), tizimni buzish osonlashadi. Statistikaning yordamida o‘xshashliklarni aniqlash mumkin.

5. Xabarni Yig‘ish va Kiritish. Hill shifrida xabarni matritsa va vektorlar yordamida tasvirlash amalga oshiriladi. Buning uchun xabarni matritsalar shaklida kiritish va chiqarish uchun alifbo uzunligi va boshqa parametrlar belgilanishi kerak.

Baholash:

- Xabar uzunligi va matritsa o‘lchami to‘g‘ri tanlanishi kerak. Agar xabar uzunligi va kalit matritsasining o‘lchamlari to‘g‘ri kelmasa, tizimni buzish osonlashadi. Masalan, noto‘g‘ri o‘lchamdagi matritsa va vektorlar bilan ishlash tizimning xavfsizligini pasaytiradi.

Xulosa. Chiziqli algebra kriptografiya sohasida muhim rol o‘ynaydi, chunki u simmetrik va asimmetrik shifrlash tizimlarining ko‘plab asoslarini tashkil etadi. Matritsa operatsiyalari, vektorlar, va linearlik kabi chiziqli algebra usullari, ayniqsa, Hill shifri kabi klassik algoritmlarda keng qo‘llaniladi. Chiziqli algebra orqali ma'lumotlarni shifrlashda matritsa va vektorlarning xususiyatlari, shuningdek, ularning invertatsiyasi va determinantlari kriptografik xavfsizlikni ta'minlashda muhim ahamiyatga ega.

Kriptografik tizimlar, ayniqsa, kriptoanaliz va xavfsizlikni baholash jarayonlarida chiziqli algebra usullarini qo‘llash orqali o‘z xavfsizligini oshirishi mumkin. Bu usullarni o‘rganish va ularning amaliy qo‘llanilishi, ayniqsa, statistik hujumlar va matritsa faktorizatsiyasi kabi zaifliklarni aniqlashga yordam beradi.

Shu bilan birga, chiziqli algebra kriptografik tizimlarni optimallashtirish va yangi xavfsizlik metodlarini yaratish uchun samarali vosita bo‘lib xizmat qiladi. Yangi yondashuvlar va murakkab tizimlar, masalan, ko‘p bosqichli shifrlash va dinamik kalitlar orqali xavfsizlikni kuchaytirish mumkin.

Umuman olganda, chiziqli algebra kriptografiyada tizimlarning ishonchliligini oshirish va yangi kriptografik metodlarni ishlab chiqishda muhim matematik asoslarni ta’minlaydi.

Foydalanilgan adabiyotlar ro’yhati

1. Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography. Second Edition. Springer.
2. Stinson, D. R. (2005). Cryptography: Theory and Practice. Third Edition. CRC Press.
3. Rosen, K. H. (2012). Discrete Mathematics and Its Applications. Seventh Edition. McGraw-Hill.
4. Garner, H. L. (2005). Matrix Methods in Cryptography. Journal of Cryptographic Engineering, 1(1), 9-18.
5. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
6. Schneier, B. (2007). Cryptography Engineering: Design Principles and Practical Applications. Wiley
7. Carter, L. M., & Wegman, M. N. (2007). Cryptography and Network Security: Principles and Practice. Prentice Hall.