HARBIY SOHADA AXBOROT XAVFSIZLIGINI TA'MINLASHDA KRIPTOGRAFIYADAN FOYDALANISH

Abduhamidov Azizbek Adilbekovich

Annotatsiya.

Maqola harbiy sohada axborot xavfsizligini ta'minlashda kriptografiyaning ahamiyatini o'rganadi. Kriptografiya, ya'ni ma'lumotlarni shifrlash va himoya qilish texnologiyalari, harbiy operatsiyalar davomida ma'lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasini ta'minlashda muhim rol o'ynaydi. Maqolada simmetrik va asimmetrik kriptografiyaning asosiy turlari, ularning harbiy sohadagi amaliy qo'llanilishi va xavfsiz aloqa tizimlaridagi o'rni ko'rib chiqiladi. Harbiy kuchlar uchun kriptografiyaning afzalliklari va uning zamonaviy kiber tahdidlarga qarshi kurashdagi ahamiyati ta'kidlanadi. Ushbu maqola axborot xavfsizligini ta'minlashda kriptografik texnologiyalarning muhimligini va ularning harbiy sohada qanday qo'llanilishini yoritadi.

Kalit so‘zlar: Kriptografiya, Axborot xavfsizligi, Harbiy soha, Simmetrik kriptografiya, Asimmetrik kriptografiya, Ma'lumotlarni himoya qilish, Aloqa xavfsizligi

KIRISH.

Zamonaviy harbiy operatsiyalar axborot texnologiyalarining rivojlanishi bilan birga keladi. Harbiy kuchlar o'z operatsiyalarini rejalashtirish va amalga oshirishda ma'lumotlarga asoslangan qarorlar qabul qilishadi. Shuning uchun axborot xavfsizligi harbiy sohada muhim ahamiyatga ega bo'lib, bu sohada kriptografiya alohida o'rin tutadi. Kriptografiya, ya'ni ma'lumotlarni shifrlash va himoya qilish texnologiyalari, harbiy axborot xavfsizligini ta'minlashda asosiy vosita sifatida ishlatiladi. Ushbu maqolada kriptografiyaning harbiy sohadagi ahamiyati, uning asosiy turlari va amaliy qo'llanilishi ko'rib chiqiladi. Kriptografiya ikki asosiy turga bo'linadi: simmetrik va asimmetrik kriptografiya.

1. Simmetrik Kriptografiya: Bu usulda ma'lumotlarni shifrlash va ochish uchun bitta kalit ishlatiladi. Simmetrik kriptografiya tezligi bilan ajralib turadi, lekin kalitni almashish jarayoni xavfli bo'lishi mumkin. Agar kalit yovuz shaxsning qo'liga tushsa, ma'lumotlar osonlik bilan o'qilishi mumkin. Harbiy sohada simmetrik kriptografiya tezkor aloqa va qisqa vaqt ichida katta hajmdagi ma'lumotlarni shifrlash uchun ishlatiladi.
2. Asimmetrik Kriptografiya: Bu usulda ikkita kalit ishlatiladi: ochiq kalit va maxfiy kalit. Ochiq kalit ma'lumotlarni shifrlash uchun, maxfiy kalit esa ma'lumotlarni ochish uchun ishlatiladi. Asimmetrik kriptografiya xavfsizroq hisoblanadi, chunki maxfiy

kalit faqat bitta shaxsda bo'ladi. Harbiy sohada bu usul ko'pincha identifikatsiya va autentifikatsiya jarayonlarida qo'llaniladi.

3. Hash-funksiyalar: Bu usullar ma'lumotlarni o'zgartirmasdan ulardan bir xosilani (hash) yaratadi. Hash-funksiyalar ma'lumotlarning yaxlitligini tekshirishda qo'llaniladi. Harbiy tizimlarda hujjatlarning o'zgarishini aniqlash uchun hash-funksiyalar muhim rol o'ynaydi.

1. Ma'lumotlarni Himoya Qilish: Harbiy operatsiyalar davomida uzatiladigan ma'lumotlar, masalan, buyruqlar, razvedka ma'lumotlari va strategik rejalashtirish, yuqori darajada himoya qilinishi kerak. Kriptografiya bu ma'lumotlarni shifrlab, ularni yovuz niyatli shaxslar tomonidan o'qilishidan himoya qiladi. Bu esa harbiy muvaffaqiyatga erishishda muhim omil hisoblanadi.

2. Identifikatsiya va Avtorizatsiya: Harbiy tizimlarda foydalanuvchilarni aniqlash va ularga kirish huquqini berish uchun kriptografik protokollar qo'llaniladi. Bu harbiy tizimlarga ruxsatsiz kirishni oldini oladi va faqat ruxsat etilgan shaxslar tomonidan ma'lumotlarga kirishni ta'minlaydi.

3. Ma'lumotlarning Yaxlitligini Ta'minlash: Kriptografiya yordamida ma'lumotlarning o'zgarishini aniqlash mumkin. Bu harbiy operatsiyalar paytida ma'lumotlarning ishonchliligini ta'minlaydi. Agar ma'lumotlar o'zgartirilsa yoki yo'q qilinsa, bu darhol aniqlanadi va zarur choralar ko'riladi.

4. Xavfsiz Aloqa: Harbiy aloqa tizimlarida kriptografik texnologiyalar qo'llanilib, uzatilayotgan ma'lumotlarning xavfsizligi ta'minlanadi. Bu aloqa kanallarini tinglash yoki manipulyatsiya qilishdan himoya qiladi. Harbiy kuchlar o'zaro aloqa qilishda shifrlangan kanallarni foydalanish orqali ma'lumotlarning xavfsizligini ta'minlaydi.

Kriptografiya harbiy sohada ko'plab amaliy qo'llanishlarga ega: Shifrlangan Aloqa Tizimlari: Harbiy aloqa tizimlarida shifrlash protokollari qo'llanilib, ma'lumotlarning maxfiyligi ta'minlanadi. Misol uchun, radio aloqa tizimlarida shifrlash algoritmlari ishlatiladi.

Hujjatlarni Shifrlash: Harbiy hujjatlar va hisobotlar shifrlanib, faqat ruxsat etilgan shaxslar tomonidan o'qilishi mumkin. Bu hujjatlarning sir saqlanishini ta'minlaydi.

Mobil Qurilmalarda Kriptografiya: Harbiy xodimlar foydalanadigan mobil qurilmalarda kriptografik himoya vositalari o'rnatiladi, bu esa ularga xavfsiz aloqa qilish imkonini beradi.

Tizimlarni Himoya Qilish: Harbiy axborot tizimlari doimiy ravishda kiberhujumlardan himoya qilinishi kerak. Kriptografik algoritmlar tizimlarni himoya qilishda muhim vosita sifatida xizmat qiladi. Harbiy sohada axborot xavfsizligini ta'minlashda kriptografiya muhim vosita hisoblanadi. U nafaqat ma'lumotlarni himoya qilish, balki identifikatsiya, avtorizatsiya va aloqa xavfsizligini ta'minlashda ham qo'llaniladi. Kriptografiyaning zamonaviy usullari harbiy operatsiyalarni yanada

samarali va xavfsiz o'tkazishga yordam beradi. Shu sababli, harbiy tashkilotlar kriptografik texnologiyalarni doimiy ravishda rivojlantirib borishlari zarur. Axborot xavfsizligini ta'minlash orqali harbiy kuchlar o'z operatsiyalarini muvaffaqiyatli amalga oshirish imkoniyatiga ega bo'ladi va strategik maqsadlariga erishishda muhim ustunlikka ega bo'ladi. Zamonaviy urushlar konvensional qurollardan ko‘ra ko‘proq ma’lumotlar maydonida (cyber warfare) olib borilmoqda. Har bir strategik qaror, maxfiy buyruq, raketali tizimlar koordinatalari va harbiy logistika ma’lumotlari raqamli tarmoqlar orqali uzatiladi. Ushbu ma’lumotlarning raqib tomonidan o‘g‘irlanishi, o‘zgartirilishi yoki bloklanishi davlat xavfsizligiga bevosita tahdid soladi. Kriptografiya - harbiy aloqa va ma’lumotlar xavfsizligini ta’minlovchi eng asosiy va mustahkam qalqondir.

1. Harbiy kriptografiyaning asosiy vazifalari

Harbiy sohada kriptografiya shunchaki ma’lumotni shifrlash emas, balki quyidagi to‘rtta strategik ustunlikni ta’minlashga xizmat qiladi:

1. Maxfiylik (Confidentiality): Ma’lumotni faqat ruxsat berilgan shaxslar yoki qurilmalar o‘qiy olishini ta’minlash. Bu dushman maxfiy rejalarni, qo‘shinlar joylashgan joyni va texnik imkoniyatlarni bilib olishining oldini oladi.

2. Butunlik (Integrity): Ma’lumot uzatish jarayonida uning o‘zgartirilmaganligini kafolatlash. Masalan, raketaning maqsadli koordinatalari uzatilayotganda, raqib tomonidan ushbu raqamlar o‘zgartirilib, missiya safsata aylantirilishidan himoya qiladi.

3. Autentifikatsiya (Authentication): Buyruq beruvchi shaxs yoki tizimning haqiqatda kimligini tasdiqlash. Bu "soxta buyruqlar" orqali qo‘shinlarni chalg‘itish (spoofing) xavfini bartaraf etadi.

4. Nafoyatkorlikni inkor etish (Non-repudiation): Buyruq beruvchi yoki ma’lumot yuboruvchi o‘z harakatini inkor eta olmasligini ta’minlash (raqamli imzo orqali).

2. Asosiy kriptografik usullar va texnologiyalar

Harbiy aloqa tizimlarida murakkab ierarxiya mavjud bo‘lib, u turli kriptografik usullarni birlashtiradi:

A. Simmetrik kriptografiya:

Bu usulda shifrlash va shifrdan ochish uchun bitta kalit ishlatiladi. U juda yuqori tezlikka ega, bu esa real vaqt rejimida ishlaydigan harbiy radar tizimlari va aloqa qurilmalari uchun muhimdir. Biroq, kalitlarni xavfsiz tarzda yetkazib berish — eng katta muammo bo‘lib qoladi.

B. Asimmetrik (Ochiq kalitli) kriptografiya:

Bu yerda ikkita kalit: ochiq (public) va yopiq (private) kalitlar ishlatiladi. Bu usul kalitlarni almashish muammosini hal qiladi va raqamli imzolar yaratishda asosiy vositadir. Harbiy tizimlarda tizimga kirish va foydalanuvchilarni tasdiqlash jarayonlarida keng qo‘llaniladi.

C. Kvant kriptografiyasi (Quantum Cryptography):
Kelajak urushlarida eng muhim omil. Kvant taqsimot tizimi (QKD - Quantum Key Distribution) fizika qonunlariga (kvant mexanikasi) asoslanadi. Agar raqib ma'lumotni o'g'irlashga yoki kuzatishga urinib ko'rsa, kvant holati o'zgaradi va bu darhol aniqlanadi. Bu mutlaq xavfsiz aloqa kanalini yaratish imkonini beradi.
3. Harbiy aloqa kanallarini himoya qilish
Kriptografiya nafaqat matnli xabarlarni, balki turli aloqa kanallarini himoya qiladi:
- Radioaloqa: Harbiy radio to'lqinlarini shifrlash orqali dushman radiotaxallusi (SIGINT) va aloqani tinglashini cheklash.
- Satellit aloqasi: Global navigatsiya va strategik boshqaruv tizimlaridagi ma'lumotlarni shifrlash.
- Ma'lumotlarni saqlash (Data-at-rest): Harbiy serverlar, planshetlar va shaxsiy qurilmalardagi ma'lumotlarni fizika orqali qo'lga kiritilsa ham, ularni o'qib bo'lmaydigan holatga keltirish.
4. Zamonaviy tahdidlar va "Kvant qo'rqinch" (Quantum Threat)
Bugungi kunda harbiy kriptografiya uchun eng katta xavf — Kvant Kompyuterlar rivojlanishidir. Hozirda qo'llanilayotgan ko'plab asimmetrik algoritmlar (masalan, RSA) kuchli kvant kompyuterlari tomonidan bir necha soniya ichida buzilishi mumkin. Bu holat harbiy sohada "Post-kvant kriptografiya" (PQC) - kvant kompyuterlari ham buzib bo'lmaydigan matematik algoritmlarni ishlab chiqishga o'tishni talab qilmoqda. Agar davlat o'z kriptografik standartlarini kvant davriga tayyorlamasa, uning barcha yashirin strategiyalari raqib uchun ochiq "kitob"ga aylanib qoladi.
5. Strategik tavsiyalar va xulosalar
Harbiy sohada axborot xavfsizligini ta'minlash uchun quyidagi yo'nalishlarda ishlash zarur:
1. Algoritmlar diversifikatsiyasi: Faqat bitta kriptografik usulga tayanmaslik, tizimlarni bir necha turdagi algoritmlar bilan himoyalash (multilayered defense).
2. Kvantga tayyorgarlik: PQC (Post-quantum cryptography) standartlarini harbiy infratuzilmaga integratsiya qilishni boshlash.
3. O'zaro bog'li tizimlar: Kriptografiyani sun'iy intellekt va blokcheyn texnologiyalari bilan uyg'unlashtirish orqali ma'lumotlar almashinuvining mustahkamligini oshirish.

XULOSA.

Xulosa o'rnida aytish mumkinki, kriptografiya harbiy kuchi tarkibiy qismi bo'lgan strategik quroldir. Raqamli asrda g'alaba faqat maydondagi qurollar bilan emas, balki o'z ma'lumotlarini himoya qila oladigan va raqibning ma'lumotlarini o'qiy oladigan, eng avvalo, kuchli kriptografik tizimga ega bo'lgan davlatlar tomonidan qozoniladi.

FOYDALANILGAN ADABIYOTLAR

1. Abdurahmonov, S. R. (2018). Kriptografiya asoslari va harbiy ilovalar. Toshkent: Fan va Texnologiya. (b. 15–220).
2. Akbarov, J. M. (2020). Harbiy kommunikatsiyalarni himoyalash: simmetrik va assimetrik kripto tizimlar. Toshkent: Harbiy nashr. (b. 45–162).
3. Boltayev, R. T. (2019). Kvantga qarshi kriptografiya: nazariya va amaliyot. Samarqand: Ilmiy Nashr. (b. 78–210).
4. Davronov, A. K. (2017). Axborot xavfsizligi va kriptografik protokollar. Namangan: Universitet Nashriyoti. (b. 30–145).
5. Karimov, O. S. (2021). Kriptografiya va tarmoq xavfsizligi: harbiy tizimlar uchun qo‘llanma. Toshkent: Innovatsiya. (b. 95–240).
6. Murodov, B. A. (2016). Shifrlash algoritmlari: amaliy misollar va testlar. Buxoro: Texnologiya. (b. 12–200).
7. Rasulova, L. N. (2022). Kriptoanaliz va raqamli imzo: harbiy ma’lumotlar integritetini ta’minlash. Toshkent: O‘qituvchi. (b. 50–183)