KOMPYUTER TIZIMLARIDA KRIPTOGRAFIK SHIFRLAR

Ilmiy rahbar: i.f.d., PhD ***F.T.Jumayev***

Kompyuter tizimlari va ularning dasturiy ta'minoti

yo'nalishi magistranti ***Ikromov Husniddin Abduvoid o'g'li***

Annotatsiya: Ushbu maqolada Kompyuter tizimlarida kriptografik shifrlar bayon qilingan bo'lib, ochiq kalitli kriptotizimlar haqida ma'lumot berilgan.

Kalit so'zlar: kriptotizim, ochiq kalitli kriptotizim, kriptografiyaning bosh amaliy masalasi, Kalitlarni taqsimlash protokoli, ANSI X9.17 generatori, FIPS-186 generatori, Yarrow-160 generatori.

Maxfiy yo'lli bir tomonlama funksiyaga asoslangan ochiq kalitli kriptotizimlar o'z mohiyatiga ko'ra undan foydalanishning alohida protokolini talab etadi. Bu alohida tartib va qoidalarga ko'ra, tizimning foydalanuvchilari va tizim foydalanuvchilarigagina ochiq bo'lgan ochiq ma'lumotlar to'plamining (kitobining) administratori (saqlovchisi) birgalikda shu tizimda uzatiladigan ma'lumotlarning maxfiyligini ta'minlaydilar. Ochiq kalitli kriptotizimlarning bardoshliligiga to'la ishonch bildirmay ishonchsizlik va ikkilanish bilan qaraydigan ba'zi kriptolog mutaxassislar, foydalanuvchilarga muhofazalangan uslubda ochiq kalitlarni taqsimlash va maxfiy kalitlarni uzatish masalalarini, ya'ni kalitlar bilan bog'liq jarayonlarni maqsadli boshqarishni kriptografiyaning bosh amaliy masalasi, deb biladilar. Misol uchun, agarda kriptotizim foydalanuvchilarining soni S ta bo'lsa va har bir mumkin bo'lgan aloqa juftlari uchun alohida maxfiy kalit talab etilsa, ularning soni (1)/ 2 2 cs = s s – bo'lib, foydalanuvchilar soni ko'p bo'lgan tizimlar uchun bunday holat ba'zida maqsadga muvofiq bo'lmasligi mumkin. Biror foydalanuvchining boshqa barcha foydalanuvchilarga maxfiy bo'lgan ma'lumotni yuborishi maxfiy aloqa mohiyatiga zid jarayon. Bundan tashqari maxfiy (muhofazalangan) aloqa tizimida qaysi foydalanuvchining boshqa qaysi bir foydalanuvchi bilan maxfiy aloqa qilishni xohlashi oldindan ma'lum emas. Mana shunday holatlar foydalanuvchilarga kalitlarni taqsimlash tartibi va qoidalari masalalarini keltirib chiqaradi. Bunday masalalarning yechilishi esa, axborot-kommunikasiya tizimida ma'lumotlarning maxfiyligi muhofazasini ta'minlovchi

kriptotizimda kalitlarni ro‘yxatga olish markazi (KROM) tashkil etishni taqozo etadi. Kalitlarni taqsimlash protokoli quyidagicha:

1. KROM muhofazalangan aloqa tarmog‘i orqali barcha i=1,2,...,S foydalanuvchilarga maxfiy Z_i kalitlarni taqdim etadi.

2. Foydalanuvchi i foydalanuvchi j bilan maxfiy aloqa o‘rnatmoqchi bo‘lsa, u umumiy aloqa tarmog‘i orqali (ochiq matn bilan bo‘lishi mumkin) KROMga murojaat qilib, foydalanuvchi j bilan maxfiy aloqa qilish kalitini so‘raydi.

3. KROM maxfiy aloqa uchun ochiq matnning biror qismini tashkil etuvchi Zij maxfiy kalitni tanlab oladi. Qolgan qismini i va j foydalanuvchilar ko‘rsatilgan “bosh qism” (“zagolovok”) yoki “nomlanish qismi” deb ataluvchi bo‘lak tashkil etadi. KROM bu ochiq matnni kriptotizimda qabul qilingan shifrlash algoritmiga ko‘ra Z_i va Z_j kalitlar bilan shifrlab, umumiy aloqa tarmog‘i orkali Z_i kalit bilan shifrlangan kriptogrammani i foydalanuvchiga va Z_j kalit bilan shifrlangan kriptogrammani j foydalanuvchiga jo‘natadi.

4. Olingan kriptogrammalarni i va j foydalanuvchilar deshifrlab, keyingi olingan ma’lumotlarni deshifrlashning maxfiy kalitiga ega bo‘ladilar. Kalitlarni taqsimlashning bunday protokoli oddiy bo‘lib, uning bardoshliligi shifrlash algoritmining bardoshliligi bilan belgilanadi. Haqiqatdan ham 3-bandda (qadamda) keltirilganidek, kriptotahlilchiga har xil kalitlar bilan shifrlangan bir xil ochiq matnning kriptogrammasi ma’lum bo‘lib, bunday holat unga kriptotahlil qilishda qo‘l keladi.

Shunday qilib, ochiq matnni shifrlash algoritmi kriptotahlilga bardoshli bo‘lsa, kalitlarni taqsimlash protokoli ham bardoshli bo‘ladi. Bu yerda shuni ham unutmaslik kerakki, kalitlarni taqsimlashda shifrlash algoritmidan foydalanish shu taqsimlash protokolining buzilishiga, kriptobardoshsizlikka va shu kabi nomutanosibliklarga olib kelmasligi kerak.

Endi Kompyuter tizimlarida kriptografik shifrlari uchun ba’zi bir generatorlar haqida ma’lumot bersak:

1) **ANSI X9.17 generatori**. Bu algoritm AQShda psevdotasodifiy ketmaketlik ishlab chiquvchi Milliy standart hisoblanib, FIPS (USA Federal Information Processing Standart) tarkibiga kiradi. Algoritmda bir tomonlama funksiya sifatida 3DES ikkita K1, K2∈V64 kalit ishlatiladi: DESK1DESK2 DESK1(64 bit) .

2) **FIPS-186 generatori**. Bu algoritm ham AQSh Milliy standarti sifatida qabul qilingan bo‘lib, DSA elektron raqamli imzo algoritmining maxfiy parametrlarini va kalitlarini generasiya qilish uchun mo‘jallangan. Algoritm bir tomonlama funksiya sifatida DES shifrlash algoritmi va SHA-1 xeshlash algoritmini ishlatadi.

3) **Yarrow-160 generatori**. Yarrow-160 psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatori Kelsi, Shnayer va Fergyuson tomonidan taklif qilingan. Bu yerda uchlik DES va SHA-1 xeshlash algoritmi ishlatilgan. Sonlar nazariyasi muammolariga asoslangan generatorlar sifatida: 1) RSA algoritmi asosidagi; 2) Mikali-Shnorr RSA algoritmi asosidagi; 3) BBS (Blum-Blum-Shub) - algoritmi asosidagi generatorlarni keltirish mumkin. Agar chiziqli va multiplikativ kongruent generatorlar bilan aniqlangan sonlar ketma-ketligi uchun n + z– bitlari ma’lum bo‘lsa, u holda hosil qilingan ketma-ketlikning qolgan hadlarini topish imkoniyati mavjud Sonlar nazariyasining muammolariga (tub ko‘paytuvchilarga ajratish va diskret logarifmlash) asoslangan generatorlardan simmetrik shifrlash algoritmlari bardoshli kalitlarining generasiya qilinishida foydalanish maqsadga muvofiq, chunki bu generatorlardan foydalanib, hosil qilingan ketma-ketlik hadlarining biror qismini bilgan holda undan oldingi yoki keyingi qismlarini aniqlash imkoniyati murakkab masala hisoblanadi.

FOYDALANILGAN ADABIYOTLAR RO’YXATI:

1. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: Учебное пособие. – Брянск, 2007.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С, Черемушкин А.В. Основы криптографии: Учебное пособие. – М., 2002.
3. Арипов М. , Пудовченко Ю. Е., Арипов М. Основы Интернет. – Т., 2003.
4. Безбогов А.А. Методы и средства защиты компьютерной информации. Учебное пособие. – Тамбов, 2006.
5. Давыдов А.С., Маслова Т.В. Информационные технологии в деятельности органов внутренних дел: Учебное пособие. – Челябинск, 2007.
6. Зайцев А.П., Голубятников И.В., Мещеряков Р.В. Программноаппаратные средства обеспечения информационной безопасности: Учебное пособие. – М., 2006.
7. Информационные технологии управления в органах внутренних дел: Учебник / Под ред. доцента Ю.А. Кравченко. – М., 1998.

8. Мельников В.П. и др. Информационная безопасность и защита информации: Учебое пособие. – М., 2008.
9. Казиев В.М. Введение в правовую информатику.
10. – http://www.intuit.ru.
11. Karimov I.M. va boshqalar. Axborot texnologiyalari: Darslik. – T., 2011.
12. Karimov I.M. va boshqalar. Informatika: Darslik. – T., 2012.
13. Левин М. Безопасность в сетях Internet и Intranet. – М., 2001.
14. Мельников В.П. Информационная безопасность. Учебое пособие. – М., 2005.
15. Миродова Ш. Проблемы обеспечения информационной безопасности Республике Узбекистан в условиях глоболизации. – Т., 2008.
16. Муҳаммадиев Ж.Ў. Ахборот хавфсизлиги: муаммо ва ечимлар: Монография. – Т., 2011.
17. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. – М., 2005.