ASIMMETRIK SHIFRLASH TIZIMLAR

Po’latov Doston Normurod o’g’li

Annotatsiya:*Asimmetrik shifrlash tizimlarida ma'lumotlarni shifrlash va de-shifrlash uchun ikki kalitdan foydalaniladi: ochiq kalit (public key) va yopiq kalit (private key). Ochiq kalit ommaviy tarqatiladi, yopiq kalit esa foydalanuvchiga xavfiy tarzda saqlanadi. Bu tizimlarda ochiq kalit ma'lumotlarni shifrlash uchun ishlatiladi, va shifrlangan ma'lumotni de-shifrlash uchun foydalanuvchining yopiq kaliti kerak bo'ladi. Asimmetrik shifrlash tizimlari ma'lumotlarni xavfsiz tarzda almashish imkonini beradi va autentifikatsiya, kalit almashish, va tizimlararo aloqalar jarayonlarini osonlashtirish imkonini beradi. Bu tizimlarning kamchiliklari murakkablik, bajarish tezligi, kalitlar boshqarish, kalitlarning o'tkazilishi, va matn uzunligi bo'lishi mumkin. Standartlarni tanlashda standartning afzalliklarini va kamchiliklarini qarshilashish kerak, va foydalanuvchilar o'zlariga mos standartni tanlashadi.*

Kalit so'zlar:*Kriptoanalize, Kriptografiya, Ochiq kalit, Custom Yopiq kalit, AES, RSA, DES,SSL/TLS*

Abstract:*Designing of microprocessor based controllers requires specific hardware as well as software programming. Programming depends upon type of the software whether operating software or application software. Programming requires knowledge of system configuration and controller specific programming. Programs are always in digital form so microprocessor can control directly at digital level called Direct Digital Control (DDC).*

Keywords:*Controller Software, DDC, Controller Configuration, Controller Programming, Custom Level Programming,Digital Form*

KIRISH

SHIfrlashning asimmetrik tizimlarining kamchiliklari quyidagilar bo'lishi mumkin

1. Murakkablik: Asimmetrik shifrlash algoritmlari murakkabdir va ularning amalga oshirilishi va boshqarilishi uchun katta hissa talab qiladi. Bu murakkablik asosan kriptografiyaga oid matematik amaliyotlardan kelib chiqadi.

2. Bajarish tezligi: Asimmetrik shifrlashning bajarish tezligi simmetrik shifrlashga nisbatan past bo'lishi mumkin. Bu asimmetriklikning natijasi bo'lib, shifrlash va de-shifrlash jarayonlari tezroq bo'lmaydi, chunki ular murakkab matematik amaliyotlarni talab qiladi.

3. Kalitlar boshqarish: Asimmetrik shifrlash tizimlarida kalitlarni boshqarish muammolarini hal qilish kerak. Yopiq kalitlar xavfiy saqlanishi kerakligi sababli ularning himoyalashiga katta e'tibor berilmalidir. Kalitlar to'g'ri saqlanmasa, ma'lumotlar xavfsizlik riskiga duchor bo'lishi mumkin.

4. Kalitlarning o'tkazilishi: Ochiq kalitlar ommaviy tarqatilishi kerakligi uchun ularga xavfsizlik ta'minlash zarurdir. Ochiq kalitlar o'tkazilganida, ulardan foydalanib, shifrlangan ma'lumotlar yana ham xavfsizlikni saqlab turishi kerak.

5. Matn uzunligi: Asimmetrik shifrlash tizimlari uchun matn uzunligi muhimdir. Murakkab matematik amaliyotlar bilan shifrlash uchun matn uzunligi katta bo'lganda, shifrlash jarayonlari tezlasadi va tizim resurslarini ortiqcha ishlatishi mumkin.

Shifrlash standartlarining tanlashida, standartlarning afzalliklarini va kamchiliklarini qarshilashadi va foydalanuvchilar o'zlariga kerakli xavfsizlik darajasiga, imkoniyatlarga va tizimning talablariga mos standartni tanlashadi.

SHIFRLASHNING ASIMMETRIK TIZIMLARINING KAMCHILIKLARI QUYIDAGILAR BO'LISHI MUMKIN

1. Murakkablik: Asimmetrik shifrlash algoritmlari murakkabdir va ularning amalga oshirilishi va boshqarilishi uchun katta hissa talab qiladi. Bu murakkablik asosan kriptografiyaga oid matematik amaliyotlardan kelib chiqadi.

2. Bajarish tezligi: Asimmetrik shifrlashning bajarish tezligi simmetrik shifrlashga nisbatan past bo'lishi mumkin. Bu asimmetriklikning natijasi bo'lib, shifrlash va de-shifrlash jarayonlari tezroq bo'lmaydi, chunki ular murakkab matematik amaliyotlarni talab qiladi.

3. Kalitlar boshqarish: Asimmetrik shifrlash tizimlarida kalitlarni boshqarish muammolarini hal qilish kerak. Yopiq kalitlar xavfiy saqlanishi kerakligi sababli ularning himoyalashiga katta e'tibor berilmalidir. Kalitlar to'g'ri saqlanmasa, ma'lumotlar xavfsizlik riskiga duchor bo'lishi mumkin.

4. Kalitlarning o'tkazilishi: Ochiq kalitlar ommaviy tarqatilishi kerakligi uchun ularga xavfsizlik ta'minlash zarurdir. Ochiq kalitlar o'tkazilganida, ulardan foydalanib, shifrlangan ma'lumotlar yana ham xavfsizlikni saqlab turishi kerak.

5. Matn uzunligi: Asimmetrik shifrlash tizimlari uchun matn uzunligi muhimdir. Murakkab matematik amaliyotlar bilan shifrlash uchun matn uzunligi katta bo'lganda, shifrlash jarayonlari tezlasadi va tizim resurslarini ortiqcha ishlatishi mumkin.

Shifrlash standartlarining tanlashida, standartlarning afzalliklarini va kamchiliklarini qarshilashadi va foydalanuvchilar o'zlariga kerakli xavfsizlik darajasiga, imkoniyatlarga va tizimning talablariga mos standartni tanlashadi.

Asimmetrik shifrlash tizimlari, ma'lumotlarni shifrlash va de-shifrlash uchun ikki kalitdan foydalanuvchi shifrlash usulidir. Bu tizimlarda ochiq kalit (public key) va yopiq kalit (private key) ishlatiladi. Ochiq kalit ommaviy tarqatiladi va foydalanuvchilar tomonidan osonlik bilan olinishi mumkin, yopiq kalit esa foydalanuvchiga xos va xavfiy tarzda saqlanadi.

ASIMMETRIK SHIFRLASH TIZIMLARI: AFZALLIKLAR VA KAMCHILIKLAR

Asimmetrik shifrlash tizimlari, ma'lumotlar almashish va maxfiylikni ta'minlashda yuqori darajada xavfsizlikni ta'minlayan kriptografiya usullaridir. Ularning afzalliklari va kamchiliklari quyidagicha:

Afzalliklar:

1. Xavfsiz kalit almashish: Asimmetrik shifrlash tizimlarida foydalanuvchilar ochiq kalitlar orqali xavfsiz tarzda kalitlarni almashishlari mumkin. Bu, kalit almashishning oson bo'lishini ta'minlayadi va bir-biriga xavfsizlik bilan kalitlarni uzatish imkonini beradi.

2. Maxfiylik: Asimmetrik shifrlashda foydalanuvchilar yopiq kalitni egallashadi, shuning uchun faqat maxfiylikni egasi ma'lumotlarni o'qiyishi mumkin. Bu tizimlar ma'lumotlarni yuqori darajada himoya qilish imkonini beradi va maxfiylik darajasini oshiradi.

3. Autentifikatsiya: Asimmetrik shifrlash tizimlari ochiq kalitlar orqali autentifikatsiyani ta'minlash imkonini beradi. Foydalanuvchilar ochiq kalitlarni ishlatib, ma'lumotlarni tasdiqlash va xavfsiz aloqalar o'rnatishlari mumkin.

4. Ma'lumotlarni himoya: Asimmetrik shifrlash tizimlari ma'lumotlarni yuqori darajada himoya qilish imkonini beradi. Ochiq kalit uzunligi va kalitlarni yaratishdagi matematik usullar tizimga yuqori darajada xavfsizlik ta'minlaydi.

Kamchiliklar:

1. Bajarish tezligi: Asimmetrik shifrlash algoritmlari simmetrik shifrlash algoritmlariga nisbatan tez ishlamaydi. Bu tizimlar katta miqdordagi ma'lumotlar uchun qayta-qayta ishlashni zarur qiladi va hisoblash resurslarini ko'p sarflashga olib kelishi mumkin.

2. Kalitlar boshqarish: Asimmetrik shifrlash tizimlarida kalitlar boshqarish murakkab bo'lishi mumkin. Yopiq kalitlar xavfsiz saqlash, ularga nizolar qo'yish va ularga ruxsat berish,

KAMCHILIKLAR

1. Bajarish tezligi: Asimmetrik shifrlash algoritmlari simmetrik shifrlashga nisbatan tez ishlamaydi. Bu, katta miqdordagi ma'lumotlar uchun qayta-qayta ishlashni zarur qiladi.

2. Kalitlar boshqarish: Asimmetrik shifrlashda kalitlar tizimini boshqarish murakkab bo'lishi mumkin. Kalitlar yopiq tarzda saqlanishi, ruxsat berilmasligi va ularga nizolar qo'yish talablari tizimga qo'shimcha yuk kam qiladi.

3. Energiya sarfi: Asimmetrik shifrlash algoritmlari simmetrik shifrlashga nisbatan yuqori energiya sarflashini talab qiladi. Bu esa batafsil amalga oshirilganida kuchli moliyaviy resurslarni talab qilishi mumkin.

Asimmetrik shifrlash tizimlarining afzalliklarini va kamchiliklarini tahlil qilish kerak, shuningdek, ilgari tizimlar va o'zgaruvchan standartlarning amalga oshirilishi va ushbu standartlarga keng doirada ko'ngil kelganligini hisobga olish kerak. Foydalanuvchilar standartni tanlashda shaxsiy talablari, tizimning iste'mol qilish davomida talab qilingan resurslar va tizimning maxfiylik darajasini qarshilashishlari kerak.

Xulosa:Asimmetrik shifrlash tizimlarining afzalliklari va kamchiliklarini to'liq xulosa qilish mumkin:

Afzalliklar:

- Asimmetrik shifrlash tizimlari maxfiylikni ta'minlashda yuqori darajada xavfsizlik beradi.

- Foydalanuvchilar ochiq kalitlar orqali xavfsiz tarzda kalitlarni almashishlari va uzatishlari mumkin.

- Ochiq kalitlar autentifikatsiya imkonini beradi va ma'lumotlarni tasdiqlash imkonini ta'minlayadi.

- Asimmetrik shifrlash tizimlari ma'lumotlarni yuqori darajada himoya qilishga imkon beradi.

KAMCHILIKLAR

- Asimmetrik shifrlash algoritmlari simmetrik shifrlash algoritmlariga nisbatan tez ishlamaydi va energiya sarflashi talab qiladi.

- Kalitlar boshqarish murakkab bo'lishi mumkin va kalitlar yopiq saqlash, nizolar qo'yish va ruxsat berish bilan bog'liqdir.

Asimmetrik shifrlash tizimlarining afzalliklari, foydalanuvchilar uchun xavfsizlik va maxfiylikni ta'minlash, kalit almashishning osonligi, autentifikatsiya va ma'lumotlarni himoya qilish imkonini beradi. Kamchiliklari esa ish bajarish tezligi, energiya sarfi, kalitlar boshqarishning murakkabligi va bog'liqlikni talab qilishi bilan bog'liq. Asimmetrik shifrlash tizimlarini foydalanishning tartibi ma'lumotlarni xavfsiz almashish, autentifikatsiya, va maxfiylik talablari bo'yicha belgilanadi, ammo ularga oid kamchiliklar va xususiyatlar ham hisobga olingadi.

ASIMMETRIK SHIFRLASH TIZIMLARIGA MISOLLAR QUYIDAGICHA BO'LISHI MUMKIN

1. RSA: RSA (Rivest-Shamir-Adleman) eng mashhur asimmetrik shifrlash algoritmidir. U ochiq kalit va yopiq kalitni ishlatadi. Misol uchun, Alice ochiq kalitni oladi va uni Bobga jo'natadi. Bob shifrlangan xabarni olish uchun yopiq kalitni ishlatadi.

2. Diffie-Hellman: Diffie-Hellman protokoli xavfsiz kalit almashish uchun ishlatiladi. U ochiq kalitlar orqali yopiq kalitni amalga oshiradi. Misol uchun, Alice va Bob ochiq kalitlar orqali bir-biriga xavfsiz kalitlarni almashish uchun Diffie-Hellman protokolidan foydalanishadi.

3. Elliptik asimmetrik shifrlash: Bu tizimda elliptik kurbalarga asoslangan ma'lumotlar shifrlanadi. U ochiq kalit va yopiq kalitlardan foydalanadi. Misol uchun, Alice va Bob elliptik asimmetrik shifrlash tizimini ishlatib, xavfsiz tarzda ma'lumot almashishlari mumkin.

4. ElGamal: ElGamal shifrlash tizimi ochiq kalitni ishlatadi va ommaviy tarqatuvchilarga mo'ljallangan bo'lib, foydalanuvchilarga xavfsizlikni ta'minlaydi. Misol uchun, Alice shifrlangan xabarni Bobga ElGamal shifrlash tizimi orqali jo'natishi mumkin.

5. DSA (Digital Signature Algorithm): DSA elektron imzo qo'yish protokoli bo'lib, ma'lumotni tasdiqlash uchun ishlatiladi. U ochiq kalit va yopiq kalitlarni qo'llab-quvvatlaydi. Misol uchun, Alice imzosini DSA orqali yaratadi va Bob shu imzoni tekshiradi.

Bu misollar asimmetrik shifrlash tizimlarining bir necha namunalari bilan bog'liq. Har bir tizimning o'zining xususiyatlari va qo'llab-quvvatlanishi bor, va foydalanuvchilar maqsadlari va talablari bo'yicha mos tizimni tanlashlari kerak.

FOYDALANILAGAN ADABIYOTLAR:

«Axborot texnologiyasi. Ma’lumotlami kriptografik muho- fazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari» O‘zbekiston Davlat standard. 0‘z DSt 1092:2005.

«Axborot texnologiyasi. Axborotlami kriptografik muhofazasi. Ma’lumotlami shifrlash algoritmi» 0‘zbekiston Davlat standard. 0‘zDSt 1105:2006

«Axborot texnologiyasi. Ochiq tizimlar o‘zaro bogMiqligi. Elek tron raqamli imzo ochiq kaliti sertifikati va atribut sertifikatining tuzil- masi» 0‘zbekiston Davlat standarti. 0‘zDSt 1108:2006.

С.В. Симонов. Анализ рисков в информационнмх систе- мах. Практические советь! // Конфидент. -2001. -№2.

S.S.Qosimov. Axborottexnologiyalari. 0‘quvqoMlanma. - T.: «Aloqachi», 2006.

S.K.G‘aniyev, M.M. Karimov. Hisoblash sistemalari va tar- moqlarida informatsiya himoyasi. Oliy o‘quv yurt.talab. uchun o‘quv qoMlanma. —Toshkent Davlat texnika universiteti, 2003.

Kosimova, A. (2022). MAIN FEATURES OF LANGUAGE LEARNING STRATEGIES. Eurasian Journal of Academic Research, 2(12), 1247-1249.

Kosimova, A. (2022). DRABBLLAR–KICHIK HAJMLI EPIK JANR. In INTERNATIONAL CONFERENCES (Vol. 1, No. 21, pp. 490-493).

Usmonova, D. S., & Muydinova, N. U. Phraseological Units with Proper Nouns in the English and Uzbek Languages. International Journal on Integrated Education, 4(2), 370-374.

Muydinova, N. (2020). DYNAMIC ACTIVITIES FOR SONG IN THE EFL CLASSROOM. In НАУКА И ТЕХНИКА. МИРОВЫЕ ИССЛЕДОВАНИЯ (pp. 11-13).

Муйдинова, Н. (2020). СОСТОЯНИЕ ВДОХНОВЕНИЯ У СПОРТСМЕНОВ. In Психологическое здоровье населения как важный фактор обеспечения процветания общества (pp. 112-113).