BLOKLI SHIFRLASH ALGORITMLARINING ASOSIY TAMOYILLARI.

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Nurafshon filiali 2-kurs talabasi

Quldoshev Otabek

kuldoshevotabek@gmail.com

Annotatsiya: Blokli shifrlash algoritmlari ma'lumotlarni bloklarga bo'lib shifrlash orqali yuqori darajadagi xavfsizlikni ta'minlaydi. Ushbu algoritmlar ko'pincha bank tizimlari, elektron tijorat, va boshqa xavfsizlik talab qiluvchi sohalarda qo'llaniladi. Ushbu referatda blokli shifrlash algoritmlarining asosiy tamoyillari, ularning dasturiy modulini ishlab chiqish jarayoni va amaliy qo'llanilishi haqida so'z yuritiladi.

Kalit so'zlar: Blokli shifrlash algoritmlari, shifrlash, de-shifrlash, Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), kalit uzunligi, shifrlash rejimlari, ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher Feedback), OFB (Output Feedback), tasodifiylik, Initialization Vector (IV), kalit boshqaruvi, public key infrastructure (PKI), shifr matn, ochiq matn, Rijndael, NIST (National Institute of Standards and Technology), kriptografik mustahkamlik, moliyaviy tranzaksiyalar, VPN (Virtual Private Network), Wi-Fi xavfsizligi, WPA2, WPA3, OpenSSL, C++ dasturlash tili.

Blokli shifrlash algoritmlari ma'lumotlarni ma'lum bir o'lchamdagi bloklarga bo'lib, har bir blokni alohida shifrlaydi. Eng mashhur blokli shifrlash algoritmlariga Advanced Encryption Standard (AES) va Data Encryption Standard (DES) kiradi. AES keng tarqalgan va yuqori xavfsizlikni ta'minlaydigan algoritm hisoblanadi. Blokli shifrlash algoritmlari shifrlash va de-shifrlash kalitlariga asoslangan bo'lib, bu kalitlar ma'lumotlarni shifrlash va qayta tiklashda ishlatiladi. Kalitlar Shifrlash va de-shifrlash jarayonida ishlatiladigan maxfiy kalitlar mavjud. Kalit uzunligi algoritmning xavfsizlik

darajasini belgilaydi. Masalan, AES algoritmida kalit uzunligi 128, 192 yoki 256 bit bo'lishi mumkin. Kalit uzunligi qancha katta bo'lsa, shifrlash algoritmi shunchalik xavfsiz bo'ladi. Shifrlash va De-shifrlash. Blokli shifrlash algoritmlari ikkita asosiy jarayondan iborat: shifrlash va de-shifrlash. Shifrlash: Ochiq matn (plaintext) kalit yordamida shifrlanib, shifr matnga (ciphertext) aylanadi. Har bir blok shifrlanganidan so'ng, shifr matn hosil bo'ladi. De-shifrlash: Shifr matn asl kalit yordamida ochiq matnga qaytariladi. Bu jarayon shifrlash jarayonining teskari yo'nalishidir. Shifrlash Rejimlari Blokli shifrlash algoritmlari turli rejimlarda ishlashi mumkin, bu rejimlar shifrlash jarayonini qanday amalga oshirilishini belgilaydi. Ba'zi mashhur rejimlar: ECB (Electronic Codebook): Har bir blok mustaqil ravishda shifrlanadi. Bu rejim oddiy va tez, ammo xavfsizlik nuqtai nazaridan zaif, chunki bir xil bloklar bir xil shifr matnga aylanadi. CBC (Cipher Block Chaining): Har bir blok avvalgi blokning shifr matniga bog'liq holda shifrlanadi. Birinchi blokni shifrlash uchun tasodifiy boshlang'ich vektor (IV) ishlatiladi. Bu rejim ECB ga nisbatan xavfsizroq, chunki bir xil bloklar turli shifr matnlarga aylanadi. CFB (Cipher Feedback): Shifrlash jarayonida avvalgi blokning shifr matni yangi blok bilan aralashtiriladi. Bu rejim real vaqtda ma'lumotlarni shifrlash uchun qulay. OFB (Output Feedback): Shifrlash jarayonida shifrlash algoritmi chiqishi yangi blok bilan aralashtiriladi. Bu rejim ham real vaqtda ma'lumotlarni shifrlash uchun ishlatiladi. Tasodifiylik va IV (Initialization Vector) Tasodifiylik shifrlash algoritmlarining xavfsizligini oshiradi. CBC, CFB, va OFB kabi rejimlarda boshlang'ich vektor (IV) ishlatiladi. IV tasodifiy ravishda yaratiladi va har bir shifrlash jarayonida yangilanadi, bu esa bir xil ochiq matn bloklarining turli shifr matnlarga aylanishini ta'minlaydi. Kalit Boshqaruvi. Kalit boshqaruvi blokli shifrlash algoritmlarining muhim tamoyillaridan biridir. Kalitlar xavfsiz tarzda yaratilishi, saqlanishi va uzatilishi kerak. Kalitlarni boshqarish uchun quyidagi amallar bajariladi: Kriptografik jihatdan mustahkam random generator yordamida kalit yaratish. Kalit saqlash: Kalitlarni xavfsiz saqlash uchun maxsus apparat yoki dasturiy vositalardan foydalanish. Kalit uzatish: Kalitlarni xavfsiz tarzda uzatish uchun public key infrastrukturalar (PKI) yoki boshqa

xavfsiz protokollardan foydalanish. Shifr Matnning Shifr Matnni Aniq Muvaffaqiyatli Ochilishi. Blokli shifrlash algoritmlarida shifr matnning ochiq matnga qayta tiklanishi aniqligi va to'g'riligi juda muhim. Bu shifrlash va de-shifrlash jarayonlarining o'zaro mos kelishini ta'minlash orqali amalga oshiriladi.

AES va DES blokli shifrlash algoritmlari.

AES (Advanced Encryption Standard) va DES (Data Encryption Standard) Blokli Shifrlash Algoritmlari. Blokli shifrlash algoritmlari ma'lumotlarni xavfsiz saqlash va uzatish uchun ishlatiladi. AES va DES eng mashhur va keng qo'llaniladigan blokli shifrlash algoritmlaridir. Ularning har biri o'ziga xos xususiyatlarga ega va turli maqsadlarda qo'llaniladi.

Data Encryption Standard (DES)

1. Tarixi:

DES 1970-yillarda IBM tomonidan ishlab chiqilgan va 1977-yilda Amerika Milliy Standartlar va Texnologiyalar Instituti (NIST) tomonidan milliy standart sifatida qabul qilingan. U uzoq vaqt davomida keng qo'llanilgan, ammo bugungi kunda eskirgan va xavfsizlik talablariga javob bermaydi.

2. Blok o'lchami va kalit uzunligi:

Blok o'lchami: 64 bit

Kalit uzunligi: 56 bit

3. Shifrlash va de-shifrlash:

DES ma'lumotlarni 64 bitli bloklarga bo'lib shifrlaydi va har bir blokni alohida shifrlaydi. Shifrlash jarayonida ma'lumotlar bir necha marta (odatda 16 marta) transpozitsiya va o'rin almashtirish orqali o'zgartiriladi.

4. Xavfsizlik:

DES ning 56 bitli kaliti bugungi kunda qisqa hisoblanadi, shuning uchun bu algoritmga qarshi hujumlar (masalan, brute-force attack) oson amalga oshirilishi mumkin. Shu sababli, DES bugungi kunda xavfsiz deb hisoblanmaydi va kamdan-kam hollarda qo'llaniladi.

5. Triple DES (3DES):

DES ning xavfsizligini oshirish uchun Triple DES (3DES) algoritmi ishlab chiqilgan. 3DES algoritmi ma'lumotlarni uch marta DES algoritmi yordamida shifrlaydi, bu esa umumiy kalit uzunligini 168 bitga yetkazadi (3 x 56 bit). 3DES DES ga nisbatan xavfsizroq bo'lsa-da, hozirgi kunda AES tomonidan almashtirilmoqda.

Advanced Encryption Standard (AES)

1. Tarixi:

AES 2001-yilda NIST tomonidan DES o'rnini bosuvchi yangi shifrlash standarti sifatida qabul qilingan. AES belgiyalik kriptograflar Joan Daemen va Vincent Rijmen tomonidan ishlab chiqilgan va "Rijndael" algoritmi asosida yaratilgan.

2. Blok o'lchami va kalit uzunligi:

Blok o'lchami: 128 bit

Kalit uzunligi: 128, 192, yoki 256 bit

3. Shifrlash va de-shifrlash:

AES ma'lumotlarni 128 bitli bloklarga bo'lib shifrlaydi. Shifrlash jarayonida ma'lumotlar bir necha marta o'rin almashtirish, aralashtirish va transpozitsiya orqali o'zgartiriladi. AES shifrlash jarayoni kalit uzunligiga qarab 10, 12 yoki 14 marta takrorlanadi.

4. Xavfsizlik:

AES bugungi kunda eng xavfsiz shifrlash algoritmlaridan biri hisoblanadi. 128, 192, va 256 bitli kalit uzunliklari bilan AES yuqori darajada kriptografik mustahkamlikni ta'minlaydi va zamonaviy kompyuterlarning hisoblash quvvatiga qarshi turadi.

5. Amaliy qo'llanilishi:

AES ko'plab xavfsizlik talab qiluvchi sohalarda qo'llaniladi, jumladan:

Bank tizimlari: Moliyaviy tranzaksiyalarni himoya qilish.

VPN (Virtual Private Network): Internet aloqalarini himoya qilish.

Wi-Fi xavfsizligi: WPA2 va WPA3 xavfsizlik protokollarida.

AES va DES ning Solishtirilishi

AES va DES kriptografiyaning muhim tarkibiy qismlari bo'lib, AES bugungi kunda DES ning o'rnini egallab, yuqori xavfsizlik va samaradorlikni ta'minlaydi. DES eskirgan bo'lsa-da, u kriptografiya tarixida muhim o'rin tutadi va Triple DES orqali hali ham ba'zi sohalarda ishlatiladi. AES esa zamonaviy xavfsizlik talablariga to'liq javob beradi va ko'plab amaliy dasturlarda keng qo'llaniladi.

AES blokli shifirlash algoritimini c++ dasturlash tilida ko’rib chiqamiz. Buning uchun dastlab OpenSSL kutubxonasini o’rnatish zarur.

CMD ni administrator sifatida ochamiz va quyidagi komandani kiritamiz: **openssl version.** Agar OpenSSL versiyasi haqida ma'lumot chiqsa, demak, OpenSSL muvaffaqiyatli o'rnatilgan. Keyingi qiladigan ishimiz c++, python yoki birorta dasturlash tilidan foydalanib kodini yozib olamiz.

Xulosa Blokli shifrlash algoritmlari zamonaviy kriptografiyaning ajralmas qismi bo'lib, ma'lumotlarni xavfsiz saqlashda katta rol o'ynaydi. DES, 3DES va AES kabi algoritmlar turli darajadagi xavfsizlikni ta'minlaydi. Blokli shifrlash algoritmlarining dasturiy modulini ishlab chiqish ma'lumotlarning himoyasini ta'minlash uchun zarur bo'lib, bu jarayon aniqlangan talablar asosida amalga oshiriladi va sinovdan o'tkaziladi.

FOYDALANILGAN ADABIYOTLAR:

1.Акбаров Д. Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши – Т 2008

2. Арипов М.М., Пудовченко Ю.Е. Основы криптологии – Т 2004

3. Бабаш А.В., Гольев Ю.И., Ларин Д.А. Шанкин Г.П. Криптографические идеи XIX века. Защита информации. Конфидент. 2004

4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 Жельников В. Криптография от папируса до компьютера. М. ABF, 1997.

5. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие, 2-е изд. –М.: Гелиос АРВ, 2002.-

6. Vernam G.S. Cipher printing telegraph systems for secret wire and radio telegraphic communications, «J. Amer. Inst. Elec. Eng., vol. 55, pp. 109-115, 1926. 4. Шенон К. Э. Теория связи в секретных тизимх. В кн.: Шенон К.Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963, том 1. - С. 333-

7. Шенон К.Э. Теория связи в секретных тизимх. В кн.: Шенон К.Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963, том 2. -С. 243-

8. Diffie W. and HellmanM.E. «New directions in cryptography» IEEE Trans. Informat. Theory, vol. IT-22, pp. 644-654, Nov. 1976. 7. R. C. Merkle «Secure communication over insecure channels», Comm. ACM, pp. 294-299, Apr. 1978.