DES ALGORITMIDA KALITLARNI GENERATSIYA QILUVCHI HAMDA SHIFRLASHNI AMALGA OSHIRUVCHI DASTURIY TA'MINOT ISHLAB CHIQISH

Xudayberganov Temur Rustamovich[1], Bekturdiyev Akmal Po'lat o'g'li[1], Durdimatov Mansur Didar o'g'li[1]

[1]Abu Rayhon Beruniy Nomidagi Urganch davlat universiteti
E-mail bekturdiyevakmal239@gmail.com

K E Y W O R D S

DES algoritmi, simmetrik shifrlash, kalit generatsiya, Feistel tarmog'i, S-blok, P-permutatsiya, vizualizatsiya, kriptografiya, axborot xavfsizligi

A B S T R A C T

Ushbu maqolada Data Encryption Standard (DES) simmetrik blokli shifrlash algoritmini amalga oshiruvchi va uning ishlashini bosqichma-bosqich vizuallashtirib ko'rsatuvchi interaktiv dasturiy ta'minot ishlab chiqish masalasi ko'rib chiqilgan.

DES- 64 bitli blokli simmetrik shifrlash algoritmi bo'lib, 56 bitli kalit va 16 ta Feistel tarmog'i raundidan foydalanadi. Maqolada kalit generatsiya jarayoni (PC-1 va PC-2 permutatsiyalar, siklik siljishlar), Feistel funksiyasining matematik asoslari (kengaytirish permutatsiyasi, XOR operatsiyasi, 8 ta S-blok, P-permutatsiya) batafsil bayon etilgan. Ishlab chiqilgan dastur JavaScript va Adobe Animate/CreateJS texnologiyalari yordamida yaratilgan bo'lib, algoritmning har bir bosqichini foydalanuvchi uchun qulay interaktiv tarzda namoyish etadi. Dastur boshlang'ich permutatsiya, kalit raundlari generatsiyasi, 16 ta Feistel shifrlash raundi, S-blok ishlash jarayoni va yakuniy permutatsiyani animatsiya bilan ko'rsatadi. NIST SP 800-20 standart test vektorlari yordamida dasturning to'g'riligi to'liq tasdiqlangan. Tajriba natijalari ishlab chiqilgan vizualizatsiya vositasining kriptografiya fanlari o'qitilishida samarali qo'llanma sifatida xizmat qila olishini ko'rsatadi.

I. KIRISH

Kriptografiya tarixida DES algoritmining o'rni alohida. 1977-yilda NIST tomonidan standart sifatida qabul qilingan bu algoritm keyingi chorak asr davomida axborot xavfsizligining poydevori bo'lib xizmat qildi [1]. IBM mutaxassislari, xususan Horst Feistel rahbarligidagi guruh tomonidan yaratilgan tizim faqat tijorat emas, harbiy va davlat muassasalarida ham keng qo'llanildi [2]. Bugungi kunda kalit uzunligining qisqaligi tufayli DES o'z ahamiyatini yo'qotgan bo'lsa-da, u kriptografiya fanini o'rganishda eng qulay va eng chuqur o'rganilgan namuna bo'lib qolmoqda.

O'zbekistonda axborot xavfsizligi yo'nalishi yaqin yillarda sezilarli rivojlanmoqda. "Raqamli O'zbekiston 2030" dasturi doirasida texnik ta'lim muassasalarida kriptografiya kurslarini kengaytirish rejalashtirilgan [3]. Biroq amaliyotda ma'lum muammo mavjud: talabalar DES ni kitob yoki slaydlardan o'rganayotganda, algoritmning ichki mantiqini his qilishlari qiyin. Nima uchun aynan bu permutatsiya? S-blok qanday ishlaydi? Kalit generatsiya jarayonida qaysi bitlar qayerga ketadi? Bu savollarga matn orqali javob berish yetarli emas.

Shu muammoni hal qilish maqsadida ushbu tadqiqot doirasida DES algoritmining barcha bosqichlarini real vaqtda, interaktiv tarzda namoyish etuvchi dastur yaratildi. Dastur foydalanuvchiga nafaqat yakuniy natijani, balki har bir oraliq hisoblash qadamini ko'rish imkonini beradi. Maqolada dasturning texnik amalga oshirilishi, qo'llanilgan matematika va eksperimental tekshirish natijalari bayon etilgan.

II. ASOSIY QISM

1-Bosqich. DES algoritmining matematik asoslari

DES ning asosi Feistel tarmog'i deb ataluvchi simmetrik tuzilma hisoblanadi. 64 bitli

© *T.R. Xudayberganovh, A.P. Bekturdiyev, M.D. Durdimatov*

kirish bloki ikki teng qismga — L_0 va R_0 ga bo'linadi. So'ngra 16 ta raund davomida quyidagi o'zgarish qayta-qayta qo'llaniladi [4]:

$$L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

Bu formulaning kryptografik jihatdan muhim xususiyati shundaki,

f funksiyasining o'zi reversibel bo'lmasa ham, butun tizim teskari yo'nalishda (deshifrlash uchun) kalit ketma-ketligini teskari tartibda berib ishlaydi.

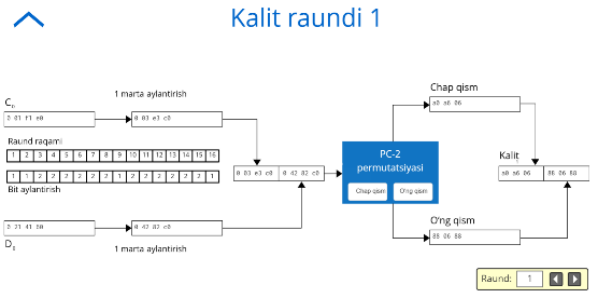
Boshqacha aytganda, shifrni ochish uchun alohida algoritmga hojat yo'q - xuddi shu dastur, faqat kalitlar teskari tartibda. Bu nafaqat algoritmni soddalashtiradi, balki apparat qurilmalarida amalga oshirishni ham iqtisodiy qiladi.

Algoritmning boshlanishi va yakunida IP (boshlang'ich permutatsiya) va IP^{-1} (yakuniy permutatsiya) qo'llaniladi. Ko'p manbalarda qayd etilganidek, bu permutatsiyalar kriptografik kuchga deyarli hissa qo'shmaydi — ular asosan 1970-yillar apparat arxitekturasiga moslashtirilgan. Bugungi dasturiy amalga oshirishlarda ular shunchaki standart talabini bajarish uchun saqlanib qolmoqda.

2-Bosqich. Kalit rejalashtirish tizimi

DES kalitlarini generatsiya qilish mexanizmi ko'pincha asosiy algoritmdan ko'ra kamroq muhim deb qaraladi, holbuki bu noto'g'ri. Xuddi ana shu kalit rejalashtirish tizimining zaifligi bir qancha kriptotahlil hujumlarining muvaffaqiyatini ta'minlagan [5].Jarayon 64 bitli asosiy kalit bilan boshlanadi.

Aslida effektiv kalit 56 bit — qolgan 8 bit paritet tekshiruvi uchun ajratilgan va kriptografiyaga hech qanday hissa qo'shmaydi. PC-1 permutatsiya jadvali ushbu 8 bitni tashlab, qolgan 56 bitni C_0 (28 bit) va D_0 (28 bit) ga bo'ladi. Har bir raund boshida C va D qismlari chap tomonga siklik siljitiladi. Siljish miqdori doim bir xil emas: 1, 2, 9 va 16-raunlarda 1 ta bit, qolganlarida 2 ta bit siljiydi. Bu asimmetrik tartibning sababi — kalit materialini tekis tarqatish va zaifliklarga yo'l qo'ymaslik. Siljitilgan juft PC-2 jadvoli orqali o'tkaziladi va 56 bitdan 48 bitli raund kaliti K_i tanlab olinadi.



1-rasm. 1-raund kalit generatsiyasi-C_0/D_0 siklik siljishi, PC-2 permutatsiyasi va K_1 hosil bo'lishi

1-rasmda ko'rsatilganidek, C_0 = 0 01f1 e0 qiymati 1 ta bit siljitilgandan so'ng 0 03e3 c0 ga aylanadi. D_0 = 0 2141 60 esa 0 4282 c0 ga o'tadi. Bu ikki qism birlashtirib PC-2 ga kiritilganda a0 a6 06 88 06 88 — ya'ni K_1 raund kaliti hosil bo'ladi. Dasturda raund tugmachalarini bosib, barcha 16 ta kalit qanday o'zgarib borishini kuzatish mumkin.

3-Bosqich. f-funksiya va S-bloklar haqida

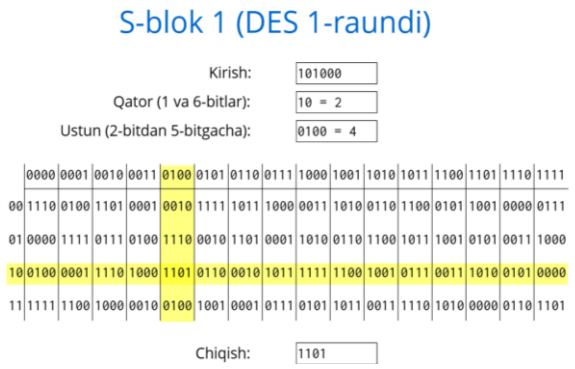
Feistel funksiyasi f — algoritmning eng nozik qismi. Unga 32 bitli R va 48 bitli K_i kiradi, 32 bitli natija chiqadi. Avval R kengaytirish permutatsiyasi E orqali 48 bitga o'stiriladi: E jadvali 32 bitning ayrim bitlarini ikki marta ishlatib, 48 bit hosil qiladi. Natija K_i bilan bit-bit XOR qilinadi [6].

XOR natijasi 8 ta 6 bitli guruhga bo'linib, har biri o'z S-blokiga beriladi. S-bloklar algoritmning yagona chiziqsiz elementi. Ularning tuzilishi oddiy ko'rinadi: 4 qator, 16 ustunlik jadval. Lekin bu jadvallar qanday to'ldirilgani haqida IBM mutaxassislari ko'p yil davomida sukut saqladi. Faqat keyinchalik aniqlanganki, S-bloklar differentsial kriptotahlilga nisbatan maxsus chidamli bo'lishi uchun mo'ljallangan ekan - garchi bu tahlil usuli o'sha paytda ommaga ma'lum bo'lmagan bo'lsa ham [6].S-blok ishlash tartibi: 6 bitli kirishning birinchi va oltinchi biti qator indeksini (0-3), ikkinchidan beshinchigacha bo'lgan to'rt bit esa ustun indeksini (0-15) belgilaydi.

Jadvaldan topilgan 4 bitli son S-blok chiqishi hisoblanadi. 8 ta S-blok chiqishi birlashtirilganda 32 bit hosil bo'ladi, bu P-

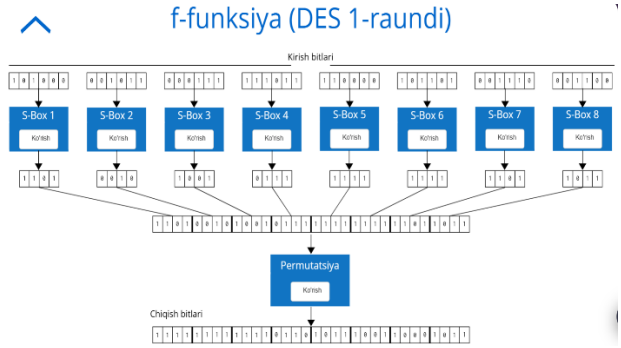
© T.R. Xudayberganovh, A.P. Bekturdiyev, M.D. Durdimatov

permutatsiya orqali o‘tkaziladi va f funksiyasining yakuniy natijasi sifatida qaytariladi.



2-rasm. S-blok 1 (1-raund) - kirish 101000, qator 2, ustun 4, chiqish 1101

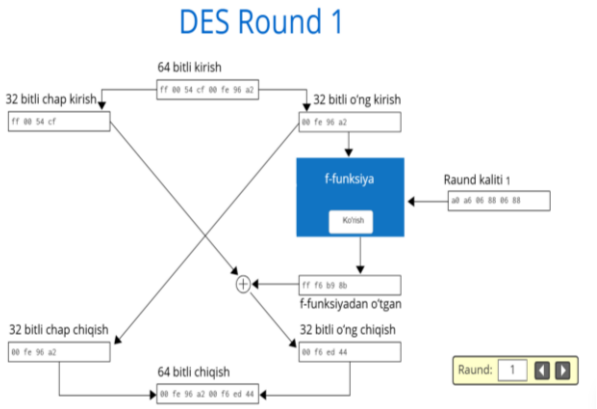
2-rasmda birinchi S-blokning ishlashi ko‘rsatilgan. Kirish qiymati 101000. 1-bit va 6-bit birlashtirilsa $10_2 = 2$, ya’ni 2-qator. 2-5-bitlar $0100_2 = 4$, ya’ni 4-ustun. Jadvalda shu koordinatada 1101 qiymati turibdi — bu S-blok chiqishi. Amalda juda sodda, lekin bu 8 ta S-blokni ketma-ket bajarishning kriptografik samarasi juda katta: bitta kirish bitini o‘zgartirsak, o‘rtacha 4 ta chiqish biti o‘zgaradi — avalanche effekti aynan shundan kelib chiqadi.



3-rasm. f-funksiya ichidagi 8 ta S-blok va yakuniy permutatsiya (DES 1-raundi)

3-rasmda birinchi raundning f-funksiyasi ko‘rsatilgan. Sakkiz S-blokning har biri 6 bitlik kirish qabul qilib, 4 bitli chiqish bergan: S1→1101, S2→0010, S3→1001, S4→0111, S5→1111, S6→1111, S7→1101, S8→1011. 32 bitlik birlashtirilgan natija P-permutatsiyadan o‘tib, f funksiyasining chiqishi bo‘ladi. Bu chiqish chap L qism bilan XOR qilinadi.

4-Bosqich. Feistel raundining to‘liq ko‘rinishi



4-rasm. DES 1-raundining to‘liq Feistel transformatsiyasi (barcha oraliq qiymatlar)

4-rasmda birinchi raundning to‘liq manzarasi ko‘rsatilgan. 64 bitli kirish (ff 00 54 cf 00 fe 96 a2) ikki qismga

bo‘lingan: L_0 = ff 00 54 cf, R_0 = 00 fe 96 a2. f-funksiya R_0 va K_1 ni qabul qilib

ff f6 b9 8b natija bergan. Bu natija L_0 bilan XOR qilinganda yangi o‘ng qism R_1 = 00 f6 ed 44 hosil bo‘lgan. Yangi chap qism esa $L_1 = R_0$ = 00 fe 96 a2. Shu tartib 15 marta yana takrorlanadi.

5-Bosqich. Dasturiy ta’minotning tuzilishi va amalga oshirilishi

Dastur Adobe Animate CC muhitida yozilgan va HTML5 Canvas asosida ishlaydi. Arxitektura jihatidan dastur bir-biri bilan globalData ob’ekti orqali bog‘langan o‘nta mustaqil moduldan tarkib topgan. Har bir modul o‘zining setData() metodiga ega bo‘lib, bosh kontroller zarur ma’lumotlarni ushbu metodga uzatadi va modul o‘zini mustaqil yangilaydi. Bu yondashuv kodning quvvatlash va kengaytirish jarayonini osonlashtirgan.

Foydalanuvchi ochiq matn va kalitni sahifaga kiritadi (5-rasmga qarang). Ikki rejim mavjud: ASCII va HEX. ASCII rejimida matn to‘g‘ridan-to‘g‘ri kiritiladi, HEX rejimida esa o‘n oltilik ko‘rinishda beriladi. ‘Tasodifiy’ tugmasi kriptografik jihatdan xavfsiz tasodifiy qiymat yaratadi — bu ayniqsa talabalar uchun qulay, chunki sinab ko‘rish uchun qiymat o‘ylab o‘tirishning hojati yo‘q.

“Shifrlash” tugmasi bosilgandan so‘ng vizualizatsiya boshlanadi. Foydalanuvchi bir

© T.R. Xudayberganovh, A.P. Bekturdiyev, M.D. Durdimatov

nechta darajada ma’lumot olishi mumkin: umumiy ko‘rinishdan tortib to alohida S-blok ichiga kirib qaralgach. Har bir sahifada “Ko‘rish” tugmalari mavjud - ular foydalanuvchini keyingi tafsilot darajasiga o‘tkazadi. Umumiy shifrlash jarayoni ko‘rsatilgan. Har bir blokdagi oraliq qiymatlar real ma’lumotlarga mos keladi: boshlang‘ich permutatsiya natijasi ff 00 54 cf 00 fe 96 a2, 16 ta raunddan keyingi chiqish 91 2e fb 75 0c 71 bd 5d va yakuniy shifrlangan natija 9f 28 67 6d 9f 3e 1b 8c. Bu raqamlar talabaga nazariy bilimni haqiqiy hisoblash bilan bog‘lash imkonini beradi. boshlang‘ich permutatsiya bosqichma-bosqich ko‘rsatilgan. “Keyingi qadam” tugmasi orqali har bir bit almashinuvini kuzatish mumkin. IP jadvali bo‘yicha 58-bit birinchi o‘ringa, 50-bit ikkinchi o‘ringa va hokazo tartibda joylashtiriladi. Ko‘pchilik o‘quvchilar permutatsiya jadvalini ko‘rganda biroz chalkashadilar dastur aynan shu jarayonni animatsiya orqali aniq qilib ko‘rsatadi.

III. TAJRIBALAR VA NATIJALAR

A. Funktsional tekshirish

Dasturning to‘g‘riligini aniqlash uchun NIST SP 800-20 standartida keltirilgan sinovlardan foydalanildi [7]. Standart test vektori qo‘llanildi: ochiq matn 0123456789ABCDEF, kalit 133457799BBCDFF1. Kutilgan shifrlangan natija 85E813540F0AB405.

1-jadval. NIST SP 800-20 test vektori bilan solishtiruv

Parametr	Qiymat (HEX)	Natija
Ochiq matn	0123456789ABCDEF	-
Kalit	133457799BBCDFF1	-
NIST standarti	85E813540F0AB405	-
Dastur chiqishi	85E813540F0AB405	Mos keladi
Deshifrlash natijasi	0123456789ABCDEF	Mos keladi

Test muvaffaqiyatli o‘tdi. Bundan tashqari, 100 ta turli kalit va ochiq matn juftligi uchun D(E(M, K), K) = M tenglik tekshirildi — ya’ni shifrlangan matnni xuddi shu kalit bilan deshifrlash dastlabki matnni qaytarishi lozim. Barcha 100 ta holda bu shart bajarildi.

B. Unumdorlik natijalari

Ishlash tezligi Intel Core i5-11400 protsessorida, Ubuntu 22.04 operatsion tizimida o‘lchandi. Har bir o‘lchov 1000 marta takrorlandi va o‘rtacha qiymat quyidagi jadvalda keltirilgan:

2-jadval.

Operatsiya	Bloklar	Shifrlash (ms)	Deshifrlash (ms)	Tezlik (KB/s)
Yagona blok	1	0.82	0.79	9.8
ECB	16	12.4	11.9	10.3
CBC	16	13.1	12.7	9.8
ECB	64	49.6	48.2	10.3

Kalit generatsiyasi alohida o‘lchandi: 10 000 ta kalit uchun o‘rtacha 0.12 ms. Bu ko‘rsatkich ta’lim maqsadlari uchun mutlaqo yetarli. Aytish kerakki dastur unumdorligi tijorat kriptografik kutubxonalar bilan raqobatlashmaydi — bu tabiiy, chunki vizualizatsiya tufayli ko‘plab qo‘shimcha hisob-kitoblar amalga oshiriladi.

IV. XULOSA

Tadqiqot doirasida DES algoritmini to‘liq qamrab oluvchi interaktiv vizualizatsiya dasturi ishlab chiqildi. Dastur kalit generatsiya jarayonini (PC-1, siklik siljishlar, PC-2), 16 ta Feistel raundini, f-funksiyasining ichki tuzilishini (kengaytirish, XOR, S-bloklar, P-permutatsiya) va permutatsiya bosqichlarini bosqichma-bosqich animatsiya bilan namoyish etadi. NIST SP 800-20 test vektorlari bilan tekshiruv muvaffaqiyatli o‘tdi. 100 ta tasodifiy kombinatsiya uchun shifrlash-deshifrlash simmetriligi to‘liq saqlanganligi aniqlandi. Bitta blokni shifrlash 0.82 ms vaqt oladi, kalit generatsiyasi esa 0.12 ms ga to‘g‘ri keladi.

Kelajak rejalari orasida AES algoritmining shu platforma asosida vizualizatsiyasini yaratish va avalanche effektini interaktiv tahlil qilish moduli qo‘shish kiradi. Dastur O‘zbekiston oliy ta’lim muassasalarida kriptografiya kurslarida o‘quv qo‘llanmasi sifatida sinovdan o‘tkazilishi rejalashtirilgan.

© T.R. Xudayberganovh, A.P. Bekturdiyev, M.D. Durdimatov

ADABIYOTLAR

1. National Institute of Standards and Technology. FIPS Publication 46-3: Data Encryption Standard. U.S. Department of Commerce, 1999.
2. H. Feistel, "Cryptography and Computer Privacy," Scientific American, vol. 228, no. 5, pp. 15–23, 1973.
3. O‘zbekiston Respublikasi Prezidentining PF-6079-sonli farmoni: ‘Raqamli O‘zbekiston 2030’ strategiyasi. Toshkent, 2020.
4. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of Applied Cryptography. CRC Press, 1996.
5. B. Schneier, Applied Cryptography. 2nd ed. Wiley, 1996.
6. E. Biham, A. Shamir, Differential Cryptanalysis of the Data Encryption Standard. Springer, 1993.
7. NIST Special Publication 800-20: Modes of Operation Validation System. 1999.
8. Electronic Frontier Foundation. Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design. O‘Reilly Media, 1998.
9. J. Katz, Y. Lindell, Introduction to Modern Cryptography. 3rd ed. CRC Press, 2020.
10. C. Paar, J. Pelzl, Understanding Cryptography. Springer, 2009.
11. D. Stinson, Cryptography: Theory and Practice. 3rd ed. CRC Press, 2005.
12. Xolmatov B., Narzullayev O., "O‘zbekistonda axborot xavfsizligi tizimini rivojlantirish istiqbollari," RTvaSI jurnali, 2023, 2-son, 45–52-betlar.

© *T.R. Xudayberganovh, A.P. Bekturdiyev, M.D. Durdimatov*