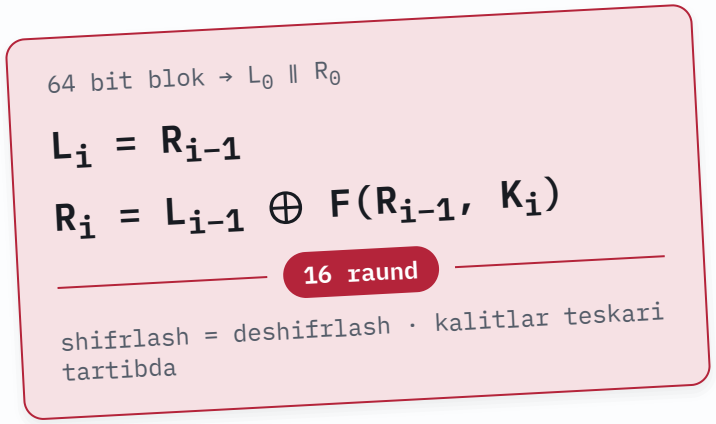
Sharof Rashidov nomidagi Samarqand davlat universiteti

KRIPTOGRAFIYA ASOSLARI · 6-MA'RUZA

Simmetrik blokli shifrlash: Feystel tarmog'i va DES algoritmi

Diffuziya va konfuziyadan raund funksiyasi va S-boxlargacha

Axborot xavfsizligi yo'nalishi talabalari uchun



Muallif: **Esanov Otabek**

2026-yil 25-avgust

REJA · 6-MA'RUZA

Bitta tarixiy shifrni to'liq ochamiz: DES

1. Blokli va oqimli shifrlash — nima farqi bor?
2. Shannon prinsiplari: diffuziya va konfuziya
3. Feystel tarmog'i: raund, teskarilash, F ning erkinligi
4. DES: IBM Lucifer, NSA va parametrlar
5. DES umumiy sxemasi: IP → 16 raund → IP^{-1}
6. Raund funksiyasi F: E, S-boxlar, P
7. Kalit jadvali, zaifliklar va Deep Crack
8. 3DES, Python amaliyoti va xulosa

Diagrammalardagi har bir strelkada bit uzunligi yozilgan — bitlarni kuzatib boring: DESda hech narsa «shunchaki» sodir bo'lmaydi.

Simmetrik shifrlashning ikki yo'li

Oqimli shifr

stream cipher

Ma'lumot **bit yoki bayt oqimi** sifatida ketma-ket shifrlanadi: kalitdan **kalit oqimi** hosil qilinadi va matnga XOR qilinadi.

```
matn          1 0 1 1 0 0 1 0
⊕ kalit
oqimi         0 1 1 0 1 0 1 1
─────────────────────────────
shifrmatn     1 1 0 1 1 0 0 1
```

RC4 · ChaCha20 · A5/1 (GSM)

Blokli shifr

bugungi mavzu

Ma'lumot **qat'iy uzunlikdagi bloklarga** (64 yoki 128 bit) bo'linadi; har blok kalit bilan **yaxlit holda** chuqur aralashtiriladi.

DES · 3DES · AES

Ikkalasi ham **simmetrik**: shifrlash va deshifrlash uchun bitta maxfiy kalit ishlatiladi.

Nima uchun bloklarga bo'lib shifrlaymiz?

1 Klassik shifrlarda birlik — **bitta harf** edi. Har harf alohida almashgani uchun tildagi chastota izi shifrmatnda saqlanib qolardi — 3-ma'ruzada shu iz orqali buzdik.

2 Blok — **64 bitli «super-belgi»**: alifbo 26 ta emas, $2^{64} \approx 1{,}8 \cdot 10^{19}$ ta «belgi»dan iborat bo'ladi. Bunday alifbo uchun chastota jadvalini tuzishning iloji yo'q.

3 Blok ichida **har bir bit boshqa bitlarga ta'sir qiladi** — harfma-harf shifrda mumkin bo'lmagan chuqur aralashtirishga yo'l ochiladi.

Qat'iy blok uzunligi apparatda ham qulay: bitta sxema har qanday uzunlikdagi ma'lumotni blokma-blok qayta ishlayveradi.

"SALOM, DUNYO!" → baytlar → 64 bitli bloklar

1-blok · 8 bayt = 64 bit

53	41	4C	4F	4D	2C	20	44

↓ E_K — blok yaxlit shifrlanadi

9C	7E	02	5B	E1	48	D3	76

2-blok · matn yetmasa — to'ldiriladi (padding)

55	4E	59	4F	21	03	03	03

Kuchli shifrning ikki ustuni

S Konfuziya

Ta'rif: shifrmatn va **kalit** o'rtasidagi statistik bog'lanishni imkon qadar murakkab, chalkash qilish — shifrmatnga qarab kalit haqida hech narsa deb bo'lmasin.

`Ta'minlaydi:` **o'rniga qo'yish** (substitution) — jadval bo'yicha nochiziqli almashtirish, DESda bular **S-boxlar**.

P Diffuziya

Ta'rif: **ochiq matn**ning har bir biti ta'sirini shifrmatnning ko'plab bitlariga yoyish — kirishda 1 bit o'zgarsa, chiqishda o'rtacha yarim bitlar o'zgarsin.

`Ta'minlaydi:` **o'rin almashtirish** (permutation/transposition) — bitlarni tarqatish, DESda **E va P bloklari**.

Klod Shannon · 1949 *«Communication Theory of Secrecy Systems» — har ikkala prinsip ham aynan shu maqolada kiritilgan; zamonaviy har bir blokli shifr shu ikki ustunga quriladi.*

O'rniga qo'yish–o'rin almashtirish tarmog'i (SP-tarmoq)

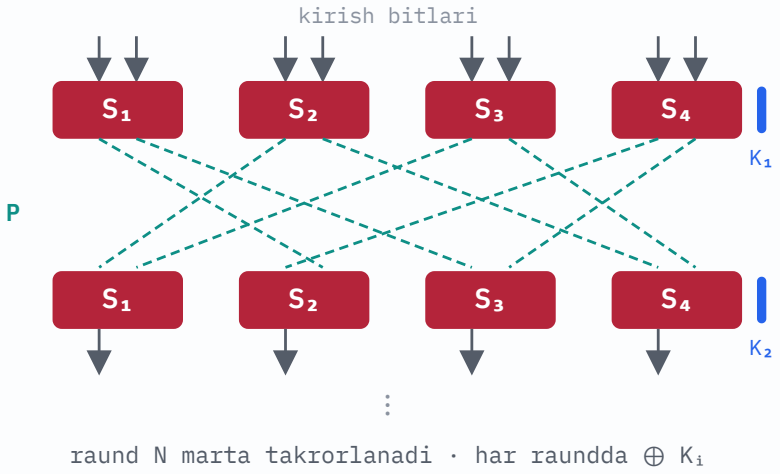
S S-qatlam kichik guruhlarni jadval bo'yicha almashtiradi → **konfuziya**

P P-qatlam bitlarni butun blok bo'ylab tarqatadi → **diffuziya**

⊕K Har raundda kalit materiali aralashtiriladi → sir kiradi

×N Zaif qatlamlar **ko'p raund takrorlanганда** kuchli shifrga aylanadi

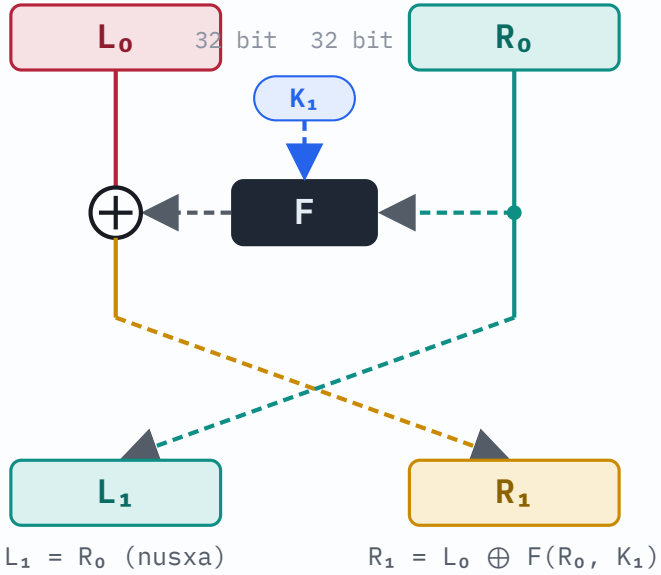
AES — sof SP-tarmoq. DES esa SP g'oyasini **Feystel qobig'iga** o'raydi — keyingi slayd.



Bitta Feystel raundi — to'liq anatomiya

1. 64 bitli blok teng ikkiga bo'linadi: L_0 va R_0 (32 + 32 bit)
2. R_0 raund kaliti K_1 bilan birga **F funksiyasi**ga kiradi
3. F natijasi L_0 ga **XOR** qilinadi: $L_0 \oplus F(R_0, K_1)$
4. Yarimliklar **joy almashadi** — keyingi raund shu ikkisidan boshlanadi

Diqqat: **R_0 hech qanday o'zgarishsiz** chap tomonga ko'chdi. Aynan shu «tegilmagan nusxa» deshifrlashning siri — 9-slaydda ochiladi.



Raundning matematik yozuvi

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

L_i, R_i	i-raunddan keyingi chap va o'ng 32 bitli yarimliklar
K_i	i-raund kaliti — asosiy kalitdan kalit jadvali orqali olinadi
F	raund funksiyasi — shifrning butun «aqli» shu yerda (16-slayd)
$\oplus$	XOR — bitma-bit 2 modul bo'yicha qo'shish

XOR NING SEHRLI XOSSASI

$$X \oplus M \oplus M = X$$

Bir xil niqob (M) ikki marta qo'llansa — o'zini yo'q qiladi. Feystelning teskarilanishi to'liq shu xossaga quriladi.

$0 \oplus 0 = 0$ · $0 \oplus 1 = 1$
$1 \oplus 0 = 1$ · $1 \oplus 1 = 0$

Yana ikki xossa: $X \oplus X = 0$ va $X \oplus 0 = X$ — «niqob yechish»ning asosi.

Asosiy afzallik: shifrlash va deshifrlash — bitta struktura

SHIFRLASH

ochiq matn · $L_0 \parallel R_0$

↓

1-raund K_1

↓

2-raund K_2

⋮

16-raund K_{16}

↓

shifrmatn

=

Sxema aynan bir xil.
Farq faqat kalitlar tartibida.

Bitta apparat sxema / bitta kod ikkala ishga ham yaraydi — 1970-yillar elektronikasi uchun hal qiluvchi tejamkorlik.

DESHIFRLASH

shifrmatn

↓

1-raund K_{16}

↓

2-raund K_{15}

⋮

16-raund K_1

↓

ochiq matn ✓

F haqidagi eng muhim fakt

TA'KID

F funksiyasi teskarilanuvchi bo'lishi shart emas

Feystel tarmog'i F qanday bo'lishidan qat'i nazar teskarilanadi. Deshifrlashda F^{-1} hech qayerda ishlatilmaydi.

1. R_{i-1} raunddan **o'zgarishsiz** o'tadi — F ning kirishi yo'qolmaydi, u L_i sifatida saqlanadi
2. Deshifrlashda F ni «buzish» emas, **qayta hisoblash** kifoya: $F(R_{i-1}, K_i)$ niqobi yana hosil qilinadi va XOR uni yechadi
3. Demak F ni **istalgancha murakkab, nochiziqli** qilib tanlash mumkin — hatto teskarisi umuman mavjud bo'lmasa ham

$$L_{i-1} = R_i \oplus F(R_{i-1}, K_i) \leftarrow F \text{ ning o'zi, } F^{-1} \text{ emas}$$

Lyusiferdan federal standartgacha

1971

IBM «Lucifer» — Xorst Feystel guruhi yaratgan blokli shifr, kalit **128 bit**

1973

NBS (hozirgi NIST) milliy shifrlash standarti uchun **ochiq tanlov** e'lon qildi

1974–76

IBM taklifi **NSA bilan qayta ishlandi**: kalit 56 bitga qisqardi, S-boxlar o'zgartirildi

1977

FIPS 46: DES — AQSh federal standarti; tarixdagi birinchi ochiq standart shifr

NSA aralashuvi yigirma yillik shubha uyg'otdi: **kalit ataylab kuchsizlantirildimi? S-boxlarga «orqa eshik» yashirildimi?** — javobning bir qismi 22-slaydda.

DES ~40 yil davomida bank, hukumat va sanoat aloqalarining asosiy shifri bo'lib xizmat qildi.

DES pasporti: to'rtta raqam

64
bit — blok uzunligi
matn 8 baytlik bloklarga bo'linadi

56
bit — samarali kalit
64 bitning 8 tasi — tenglik bitlari

16
raund — Feystel
har raundga o'z 48 bitli kaliti

Feystel
arxitektura
shifrlash = deshifrlash strukturasi

64 bitli kalit: har baytning oxirgi biti — tenglik (parity) biti, sirga hissa qo'shmaydi

■ 56 bit — maxfiy material

■ 8 bit — tenglik bitlari (8, 16, … 64-pozitsiyalar)

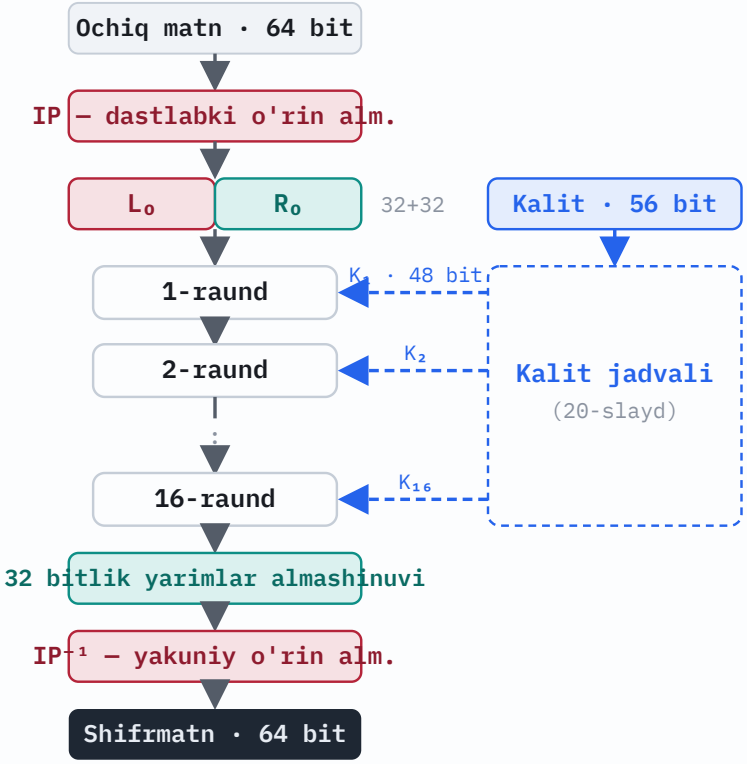
DES ning umumiy sxemasi

IP kirish/chiqishdagi o'rin almashtirishlar — kriptografik kuch qo'shmaydi (14-slayd)

16× yadro — 16 ta Feystel raundi: butun xavfsizlik shu yerda

K_i har raundga kalit jadvalidan alohida 48 bitli kalit keladi (20-slayd)

Oxirgi almashtirish tufayli deshifrlash — xuddi shu sxema, kalitlar $K_{16} \to K_1$ (15-slayd).



IP va IP⁻¹: qat'iy jadval bo'yicha o'rin almashtirish

IP (initial permutation) 64 bitni **qat'iy jadval bo'yicha** qayta joylaydi: chiqishning 1-o'rniga kirishning 58-biti, 2-o'rniga 50-biti keladi va hokazo. IP^{-1} — shuning aynan teskarisi.

`58` → `chiqishning 1-biti = kirishning 58-biti`

Halol gap: IP kriptografik kuch **qo'shmaydi** — jadval ochiq, kalitga bog'liq emas. U 1970-yillar apparatida baytlarni qulay yuklash uchun kiritilgan, xolos.

Shu sabab dasturiy amalga oshirishlarda IP eng «qimmat», lekin eng foydasiz qadam sifatida tez-tez tanqid qilinadi.

IP jadvali — 64 pozitsiya (qatorlab o'qiladi)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

16 raund ichida nima sodir bo'ladi?

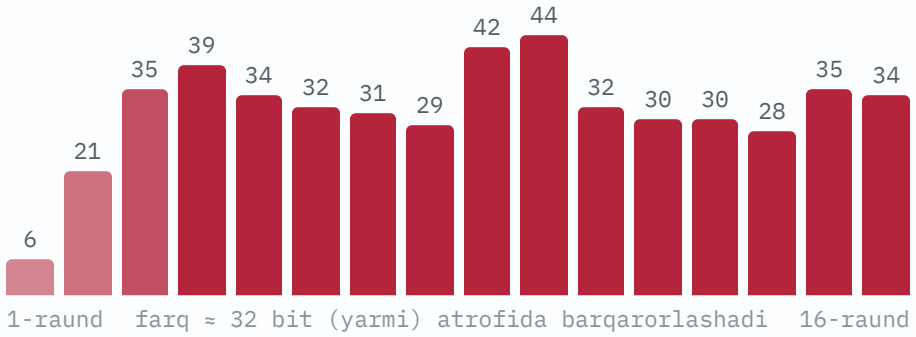
NEGA OXIRIDA YANA ALMASHTIRISH?

16-raunddan keyin yarimliklar **yana bir bor joy almashadi**: natija $R_{16} \| L_{16}$ tartibida IP^{-1} ga uzatiladi. Aynan shu tufayli deshifrlash — **o'sha sxemaning o'zi**, faqat kalitlar teskari tartibda.

Har raund F orqali konfuziya (S-boxlar) va diffuziya (E, P) qo'shadi. Bitta raund kuchsiz — **16 marta takrorlash** ularni to'liq blokga yoyadi.

KO'CHKI (AVALANCHE) EFFEKTI

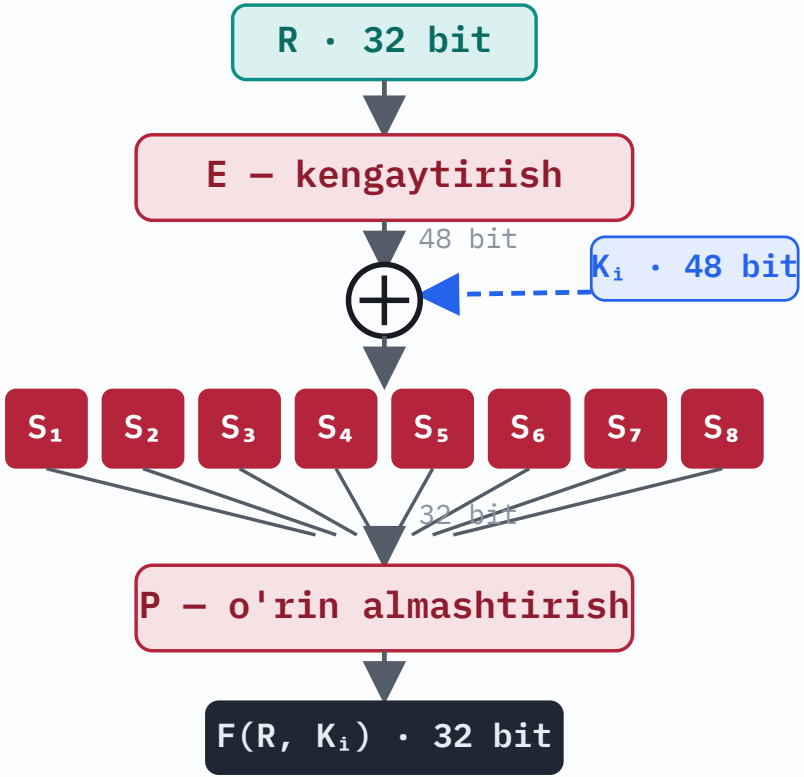
Ikki ochiq matn atigi 1 bitga farq qiladi — raundma-raund shifrmatnlar orasidagi farq (bitlarda), namunaviy o'lchov:



F ichida: E → ⊕K → S-boxlar → P

1. **E**: 32 bit 48 bitgacha kengayadi — chekka bitlar takrorlanadi (17-slayd)
2. ⊕ **K_i**: 48 bitlik raund kaliti aralashadi — sir shu yerda kiradi
3. **S_1…S_8**: har biri 6 bitni 4 bitga jadval bo'yicha almashtiradi — 48 → 32 (18-slayd)
4. **P**: 32 bitni yana bir bor aralashtiradi — S-boxlar chiqishini butun blokka yoyadi (diffuziya)

Bitlar yo'li: **32** → **48** → **48** → **32** → **32**. Shu to'rt qadamdan faqat **bittasi** — S-boxlar — nochiziqli (19-slayd).



E — kengaytirish: 32 bitdan 48 bitga

1. 32 bitlik R sakkiz guruhga bo'linadi — har guruh **4 bit**
2. Har guruh qo'shni guruhlardan bittadan bit **«qarz oladi»** — 4 bit endi 6 bit bo'ladi
3. 8 guruh × 6 bit = **48 bit** — endi 48 bitlik K_i bilan XOR qilish mumkin

Chekka ustunlardagi bitlar (pastda belgilangan) **ikki marta** ishlatiladi — bu takrorlanish qo'shimcha diffuziya beradi.

E ham IP kabi **kalitga bog'liq emas** — qat'iy, ochiq jadval; nochiziqlilik bermaydi.

E jadvali · 8 qator × 6 ustun (qatorlab o'qiladi)

32	1	2	3	4	**5**
4	5	6	7	8	**9**
8	9	10	11	12	**13**
12	13	14	15	16	**17**
16	17	18	19	20	**21**
20	21	22	23	24	**25**
24	25	26	27	28	**29**
28	29	30	31	32	**1**

■ qo'shni guruhdan qarz olingan bit

S-box: 6 bitni 4 bitga qanday aylantiramiz?

chekka 2 bit (1- va 6-bit) → **qator** (0–3)

o'rtadagi 4 bit (2–5-bit) → **ustun** (0–15)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	**9**	1	7	5	11	3	14	10	0	6	13

kirish: **1 0 1 0 1 1** → qator (1,6-bit) = $\mathbf{11}_2$ = 3 · ustun (2–5-bit) = $\mathbf{0101}_2$ = 5 → S1[3][5] = **9** = 1001_2

Nega S-boxlar DESning yuragi?

CHIZIQLI QADAMLAR

$IP \cdot E \cdot P \cdot IP^{-1}$

Faqat **bit pozitsiyasini** o'zgartiradi. Kirish va chiqish orasidagi bog'lanish — oddiy, oldindan aytib bo'ladigan, **matritsa bilan yoziladigan** almashtirish.

Kalitga bog'liq emas — hujumchi bu qadamlarni to'liq biladi.

YAGONA NOCHIZIQLI QADAM

$S_1 \ldots S_8$

Kirish va chiqish orasida **oddiy formula yo'q** — natija faqat jadvaldan qidiriladi. DES xavfsizligining butun yuki shu sakkiz kichik jadvalga tushadi.

S-boxlar chiziqli bo'lsa — butun DES bitta chiziqli tenglamalar tizimiga qisqarib, oson yechilardi.

S-boxlarning tanlov mezonlari 1990-yillargacha to'liq oshkor qilinmagan edi — ularning ataylab qanchalik mustahkam ekani keyinroq isbotlandi (22-slayd).

56 bitdan 16 ta raund kaliti

1. **PC-1**: 64 bitdan tenglik bitlari chiqariladi → 56 bit, ikkiga bo'linadi: C_0 va D_0 (28+28)
2. Har raundda C, D **mustaqil chapga siljitiladi** — 1, 2, 9, 16-raundlarda 1 pozitsiya, qolganlarida 2
3. **PC-2**: siljigan $C_i \| D_i$ (56 bit) dan 48 bit tanlanadi — bu K_i
4. 16 marta takrorlanadi — 16 ta **mustaqil, lekin bog'liq** raund kaliti hosil bo'ladi

PC-1 va PC-2 — E va P kabi ochiq jadvallar; nochiziqlilik faqat S-boxlarda.

56 bit qanchalik kichik ekan?

$$2^{56} \approx 7{,}2 \times 10^{16}$$

mumkin bo'lgan kalitlar — 1977-yilda «astronomik» hisoblangan

Muammo algoritmning o'zida emas — **kalit qisqaligida**

Yechim to'liq qidiruv (brute force) — har bir kalitni sinab ko'rish

1998 | Electronic Frontier Foundation (**EFF**) tomonidan qurilgan maxsus mo'ljallangan qurilma **«Deep Crack»** to'liq qidiruv orqali bitta DES kalitini **56 soatda** topdi.

Bu voqea DESning **amaliy** xavfsizligiga yakun yasadi. Zamonaviy maxsus apparat bilan bu vaqt yanada qisqaradi.

Zaif kalitlar va kutilmagan chidamlilik

Zaif kalitlar Ba'zi maxsus kalitlar (masalan, barcha bitlar 0 yoki barcha bitlar 1) barcha yarim kalitlarni bir xil qiladi. Bunday kalitlar — atigi bir nechtasi, $7{,}2 \cdot 10^{16}$ orasida **amaliy xavf tug'dirmaydi**.

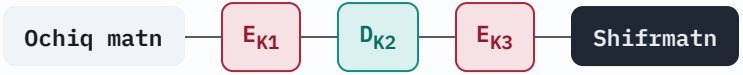
DIFFERENSIAL KRIPTOTAHLIL Biham & Shamir, 1990

Bu kuchli hujum usuli ochiq e'lon qilinganda, DES S-boxlari kutilganidan **ancha chidamli** chiqdi.

Sabab: IBM guruhi bu hujum turini **1970-yillarda allaqachon bilgan** va S-boxlarni ataylab shunga qarshi mustahkamlagan — buni **NSA talabi bilan o'n yillar davomida oshkor qilmagan** (11-slayd).

DES tarixidagi eng ajoyib faktlardan biri: yopiq loyihalashtirilgan tizim o'z davridan 15 yil oldingi hujumga tayyor bo'lib chiqdi.

3DES: nega uch marta, ikki emas?



NEGA EDE (O'RTADA DECRYPT)?

K1=K2=K3 qilib qo'yilsa, $E_K \circ D_K \circ E_K = E_K$ ga teng bo'ladi — natijada 3DES qurilmasi oddiy **DES bilan orqaga mos** ishlaydi.

NEGA IKKI MARTA EMAS?

Meet-in-the-middle hujumi: xotirani vaqtga almashtirib, ikki martalik DES qidiruvini deyarli bitta DES darajasigacha tushiradi — qo'shimcha xavfsizlik deyarli yo'q.

Nominal uzunlik: **3 × 56 = 168 bit**

meet-in-the-middle variantlari tufayli

Samarali xavfsizlik: **≈ 112 bit**

09 · 3DES VA ZAMONAVIY HOLAT

DES: standartdan tarixga

2001

AES qabul qilindi

NIST yangi federal standart sifatida e'lon qildi — bosqichma-bosqich o'tish boshlandi

2005

DES rasman bekor qilindi

NIST FIPS 46-3 standartini 19-may kuni qaytarib oldi

2023

3DES ham taqiqlandi

31-dekabrdan keyin yangi tizimlarda man etildi — faqat eski ma'lumotni deshifrlash uchun qoldi

Xulosa: DES va 3DES **bugun hech qanday yangi tizimda ishlatilmasligi kerak**. Ularning o'rnini **AES** egalladi — Feystel emas, sof SP-tarmoq (6-slayd).

Soddalashtirilgan Feystel — Python

```python
def f(right, key):
return (right * 3 + key) % 256

def round_(l, r, key):
return r, l ^ f(r, key)

def inverse_round(l, r, key):
return r ^ f(l, key), l

def encrypt(l, r, keys):
for k in keys: l, r = round_(l, r, k)
return l, r

def decrypt(l, r, keys):
for k in reversed(keys): l, r = inverse_round(l, r, k)
return l, r

keys = [23, 91, 140, 7]
L, R = 12, 200
CL, CR = encrypt(L, R, keys)
PL, PR = decrypt(CL, CR, keys)
```

```
$ python feistel_demo.py
Ochiq matn:   L=12  R=200
Shifrmatn:    L=19  R=12
Deshifrlangan: L=12  R=200 ✓
```

4 raundli o'yinchoq Feystel — F o'rnida DESdagi E/S-box/P zanjiri emas, bitta oddiy arifmetik funksiya. Struktura bir xil: L/R almashinuvi, XOR, kalitlarni teskari tartibda qo'llab deshifrlash.

`decrypt(encrypt(L,R,keys), keys) == (L,R)` — 9-slaydda ko'rgan simmetriyaning o'zi.

Bitlardan ishonchgacha

1. Blokli shifr butun blokni yaxlit qayta ishlaydi — chastota tahlili ishlamaydi
2. Feystel tarmog'i: L/R bo'linish + XOR — shifrlash va deshifrlash bir xil struktura
3. DES: 16 raund, F = E → ⊕K → S-boxlar → P; S-boxlar yagona nochiziqli qadam
4. 56 bitlik kalit — yagona jiddiy zaiflik; 1998, Deep Crack, 56 soat
5. 3DES vaqtinchalik yechim bo'ldi — 2023-yildan yangi tizimlarda taqiqlangan

KO'PRIK

DES o'rnini kim egalladi?

2001-yilda **AES** qabul qilindi — Feystel emas, sof SP-tarmoq; 128–256 bitli kalitlar. Keyingi mavzu.

Esanov Otabek

SamDU · Sun'iy intellekt va raqamli texnologiyalar fakulteti
Boshqaruv nazariyasi va axborot xavfsizligi kafedrasi

GitHub github.com/EsanovOtabek
Telegram @esanovme
Email esanovotabek688@gmail.com
Tel +998 93 236 04 33