Жаңа дәуірдегі симметриялық криптожүйелер: DES және ГОСТ 28147-89

Пән атауы: Ақпараттық қауіпсіздік негіздері

Лекция №3

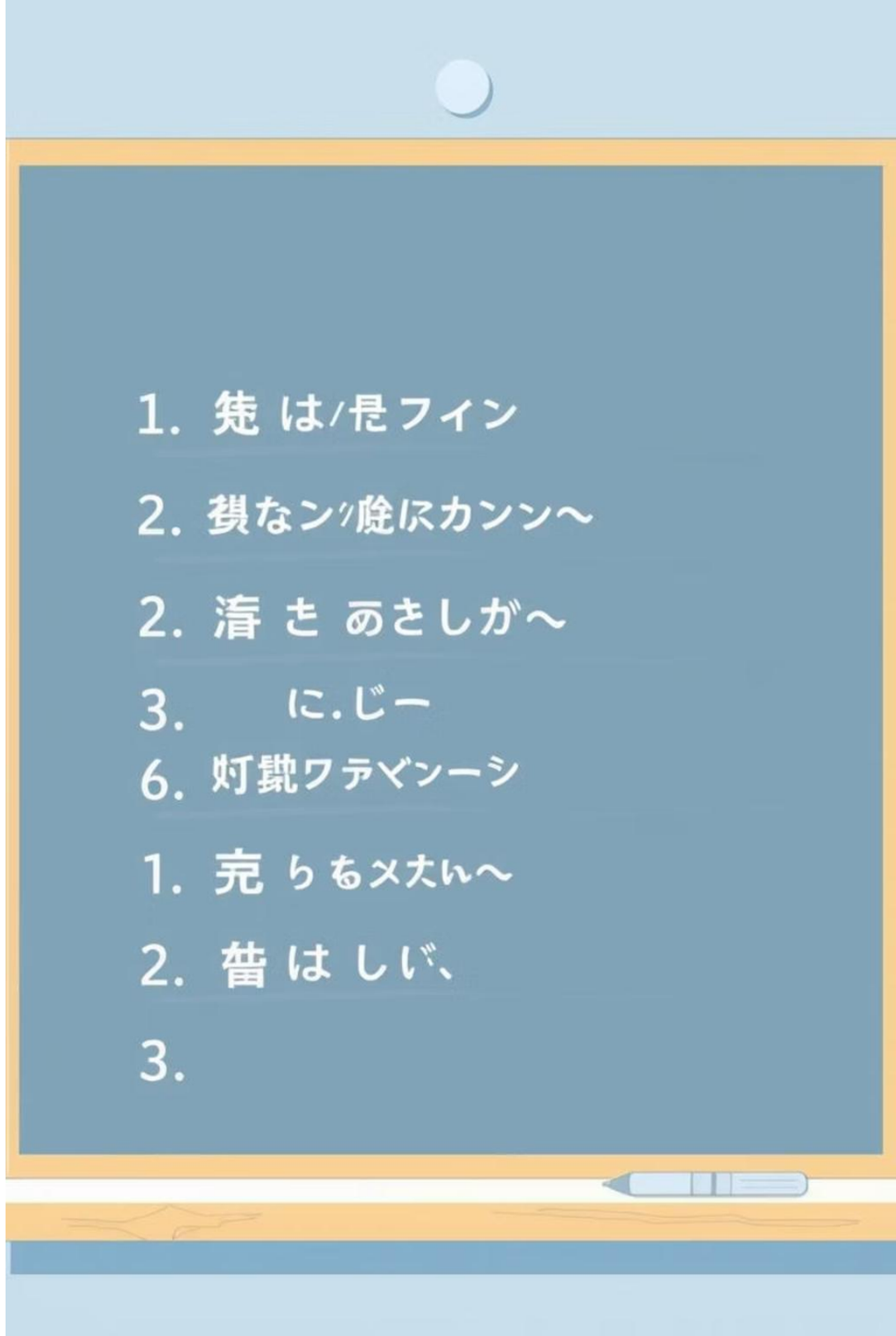
Лекцияның мақсаты мен негізгі сұрақтар

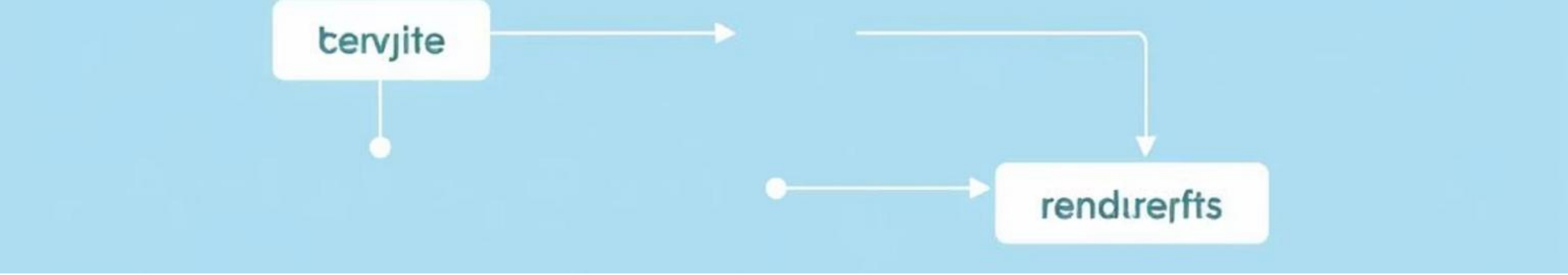
Лекцияның мақсаты:

- Симметриялық криптожүйелердің негізгі ұғымдарымен таныстыру.
- DES және ГОСТ 28147-89 алгоритмдерінің құрылымын түсіндіру.
- Криптоанализ әдістері туралы қысқаша түсінік беру.

Қарастырылатын сұрақтар:

- Симметриялық криптожүйе деген не?
- DES қалай жұмыс істейді?
- Фейстел желісі деген не?
- ГОСТ 28147-89-дың ерекшеліктері қандай?
- Криптоанализдің рөлі қандай?





Симметриялық криптожүйелер ұғымы

Негізгі идея

Симметриялық криптожүйе – шифрлау мен дешифрлауда бірдей құпия кілт қолданылатын жүйе.

Жұмыс принципі

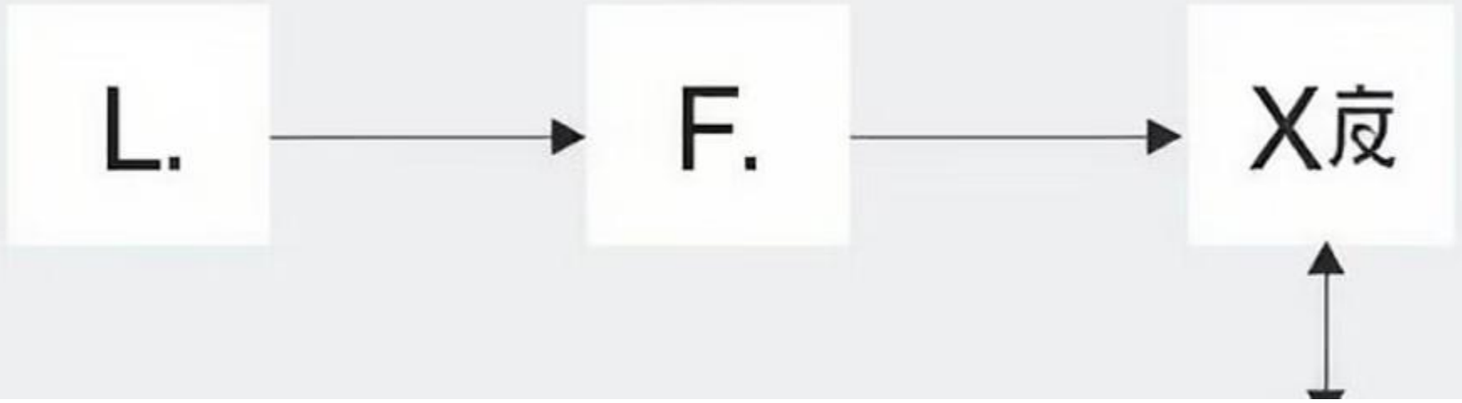
Ашық мәтін → шифрмәтін → қайтадан ашық мәтін (сол кілтпен).

Артықшылығы:

- **Жылдам шифрлау.**
- **Үлкен көлемдегі деректерге ыңғайлы.**

Кемшілігі:

- **Құпия кілтті қауіпсіз тарату қиындығы.**



Фейстел желісінің жалпы құрылымы

Көптеген блоктық шифрларда, соның ішінде DES және ГОСТ 28147-89-да Фейстел желісі қолданылады. Бұл құрылым шифрлау процесіне күрделілік қосады.

1

Блокты бөлу

Бастапқы блок екіге бөлінеді: сол жақ бөлік L және оң жақ бөлік R.

Раундтық операция

Әр раундта жаңа сол бөлік L' = R және жаңа оң бөлік R' = L ⊕ F(R, K) формуласы бойынша есептеледі.

F функциясы

F – кілтке тәуелді түрлендіру жасайтын сызықты емес функция, ол шифрдың қауіпсіздігін арттырады.

Әр раундта бөліктер орын ауыстырып, бір-біріне араласады, осылайша көптеген раундтан кейін шифрмәтін күрделі болып шығады.

DES криптожүйесінің жалпы сипаттамасы

0

0

1 Тарихы

DES (Data Encryption Standard) – IBM компаниясында жасалған, 1977 жылы АҚШ-та стандарт ретінде қабылданған. 20 жылдан аса кең қолданылған симметриялық блоктық шифр.

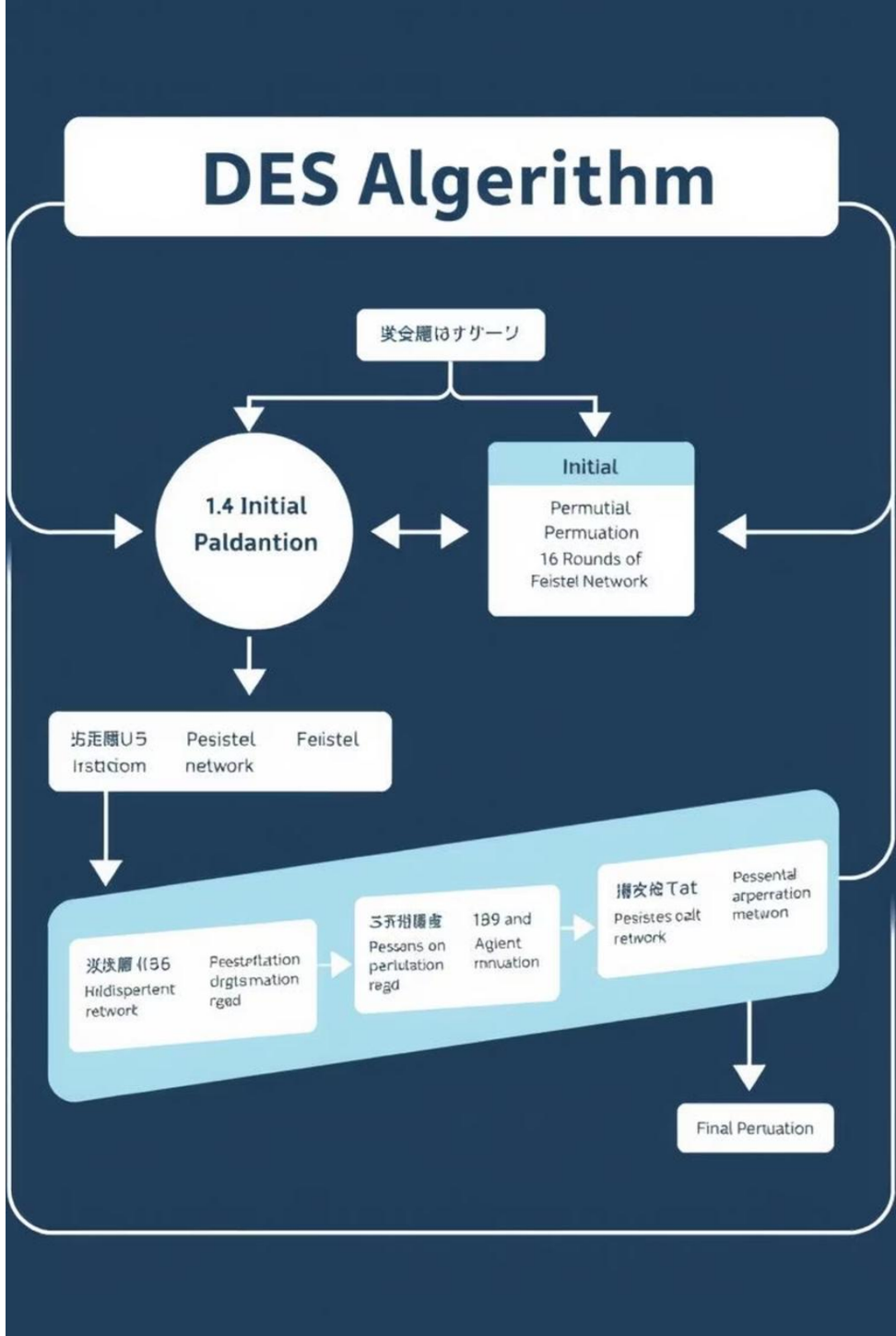
2 Негізгі параметрлері

Блок ұзындығы: 64 бит. Пайдалы кілт ұзындығы: 56 бит. Раунд саны: 16.

0

3 Жалпы жұмыс принципі

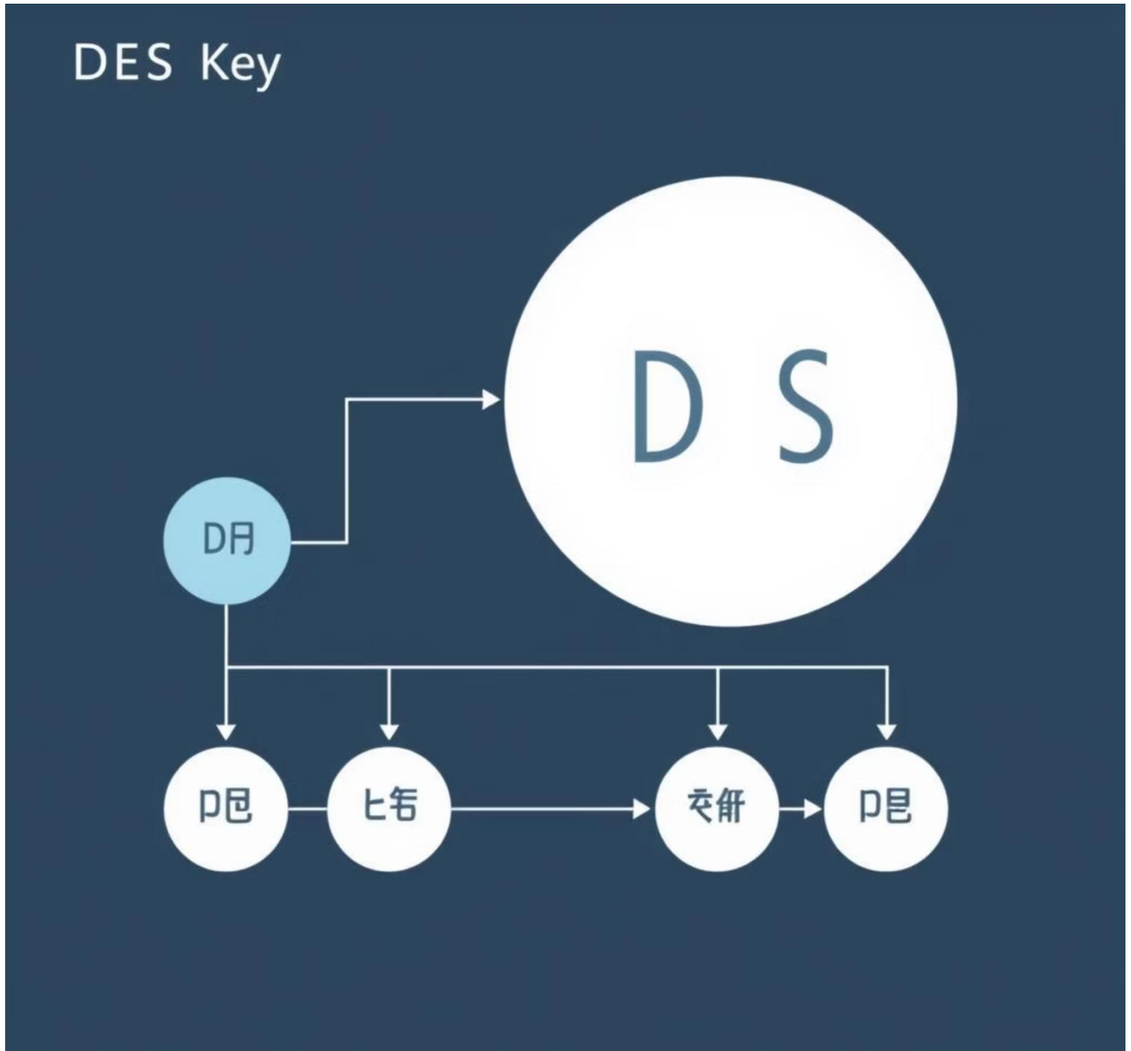
Бастапқы 64 биттік блок алғашқы алмастыруға түседі, содан кейін 16 Фейстел раунды орындалады. Соңында ақырғы алмастыру орындалып, шифрмәтін алынады.



DES кілтін қалыптастыру және раунд функциясы

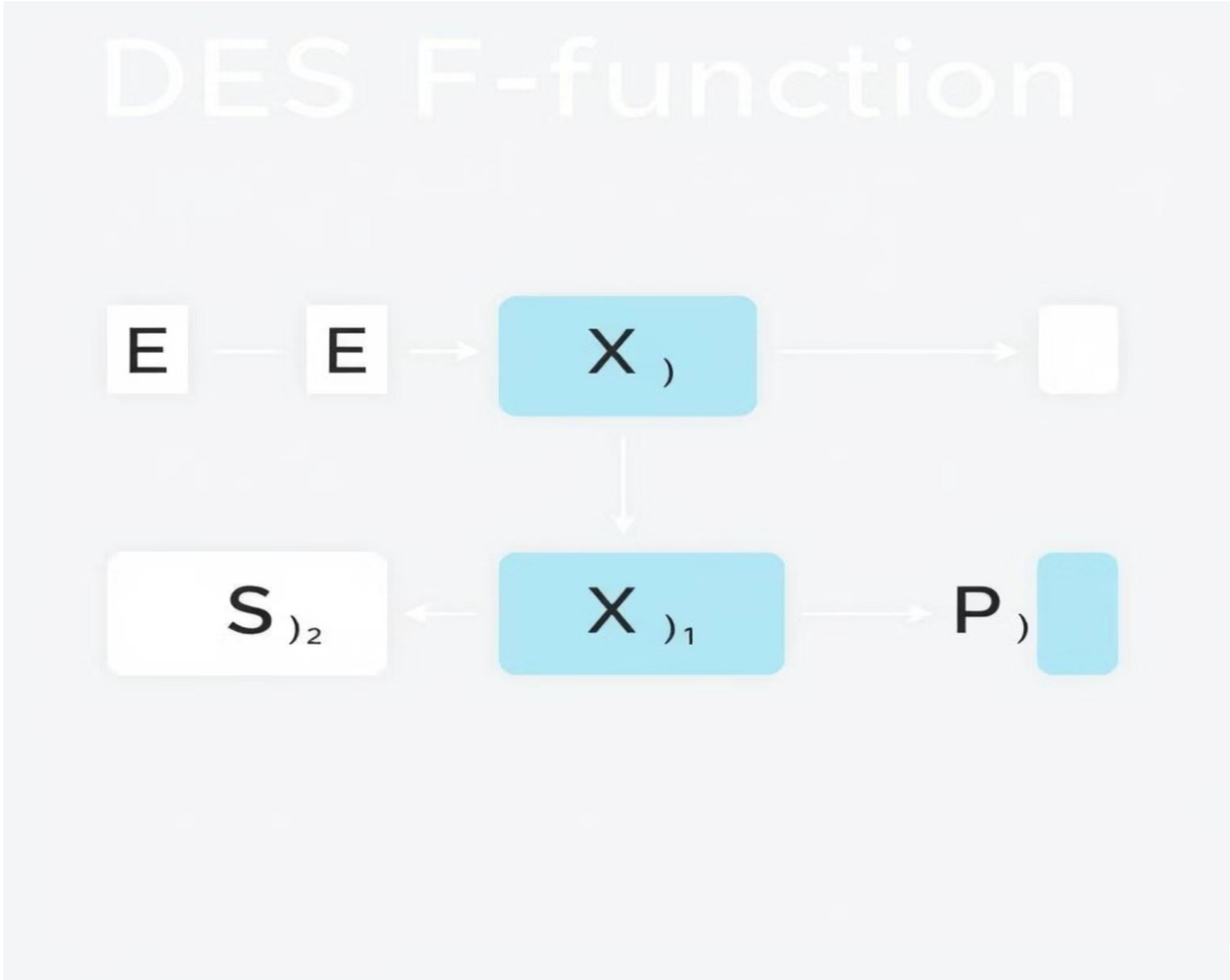
Кілтті таңдау (Key Schedule)

- 64 биттік бастапқы кілттен 56 биттік C_0 және D_0 екі блок алынады.
- Олар кесте бойынша 1 немесе 2 битке циклдік жылжытылады.
- Әр раунд үшін 48 биттік кіші кілт K_i (i = 1...16) түзіледі.



Раундтық F функциясы

- Оң жақ бөлік 32 биттен 48 битке кеңейтіледі (E-кеңейту).
- 48 биттік бөлік кіші кілтпен XOR жасайды.
- Нәтиже 8 S-блок арқылы өтеді (әр 6 бит → 4 бит).
- Соңында P-алмастыру орындалады.



DES-тің артықшылықтары мен әлсіз тұстары

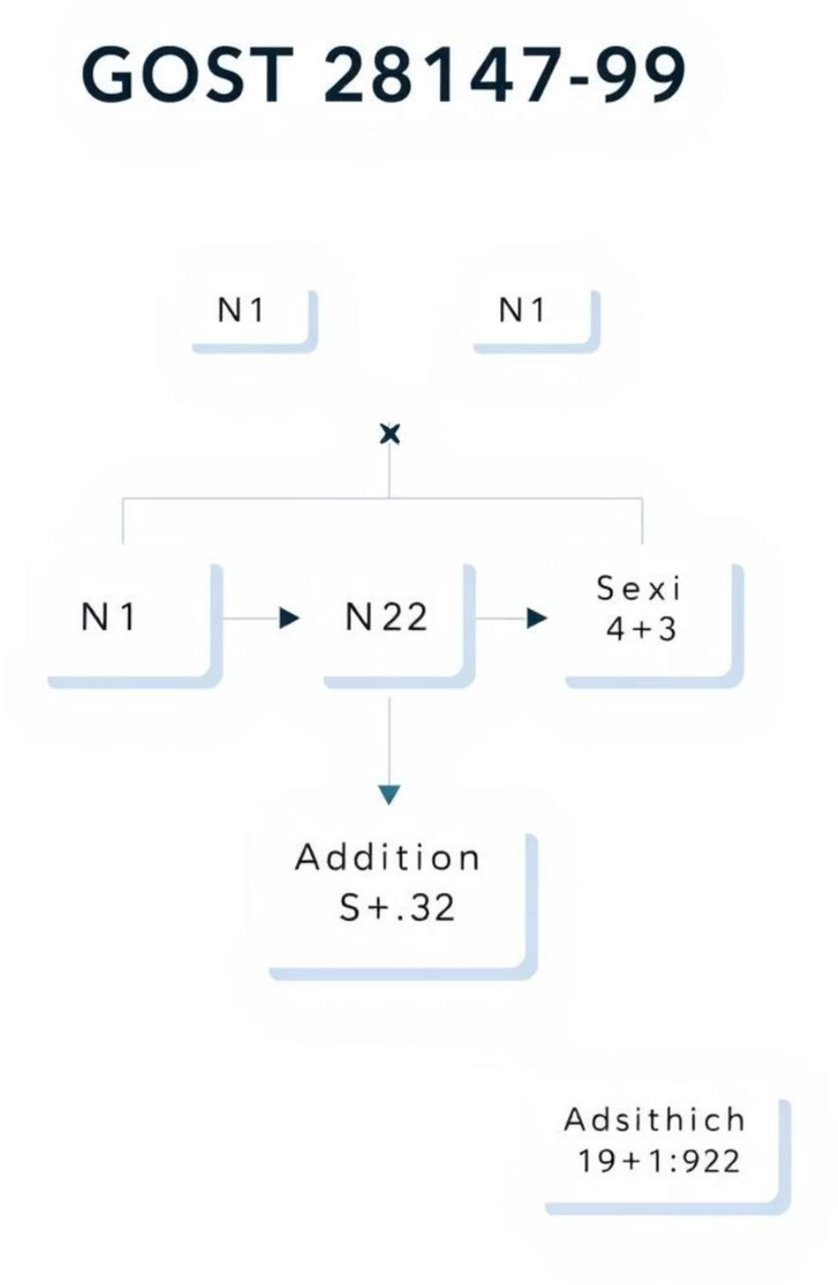
Артықшылықтары

- Шифрлау/дешифрлау жылдамдығы жоғары.
- Алгоритм ашық, қауіпсіздік кілт құпиялылығына негізделген.
- Әр блок бір-біріне тәуелсіз шифрлана алады.

Әлсіз жақтары

- Кілт ұзындығы 56 бит – қазіргі заманда қысқа.
- Толық іздеу (brute force) әдістерімен сындыруға болады.
- Практикада үлкен компьютер кластерлері DES кілтін таба алатыны дәлелденген.

Қорытындылай келе, DES толық қауіпсіз деп саналмаса да, қазіргі көптеген алгоритмдерге негіз болған маңызды шифр болып қала береді.



ГОСТ 28147-89 алгоритмі

Жалпы сипаттамасы

ГОСТ 28147-89 – ТМД елдерінде қолданылатын ұлттық блоктық шифр. Блок ұзындығы 64 бит, раунд саны 32, бұл DES-тен екі есе көп.

Кілт және режимдер

Кілт ұзындығы 256 бит (8 × 32 биттік вектор). Негізгі қолдану режимдері: жай алмастыру, гаммалау, кері байланысты гаммалау, шифрмәтін блоктарын тізбектеу.

Негізгі операциялар

32 биттік сөздермен жұмыс істейді. 2^{32} модулі бойынша қосу, 11 битке циклдік жылжыту және 4×4 өлшемді S-блоктарды қолданады.

DES пен ГОСТ-тың салыстырмасы және криптоанализ

Блок ұзындығы	64 бит	64 бит
Раунд саны	16	32
Кілт ұзындығы	56 бит	256 бит
Негізгі операциялар	XOR, S-блоктар, алмастырулар	2^{32} модулі бойынша қосу, циклдік жылжыту, S-блоктар

Криптоанализ

Криптоанализ – шифрды кілтті білмей ашу тәсілдерін зерттейтін ғылым бөлігі. Негізгі әдістері: дифференциалдық криптоанализ және сызықтық криптоанализ.

Алгоритмнің қауіпсіздігі көбіне S-блоктардың қасиетіне және раунд санына байланысты.

Бақылау сұрақтары және пайдаланылған әдебиеттер

Бақылау сұрақтары:

- Симметриялық криптожүйелердің жұмыс принципі қандай?
- DES алгоритмі қалай жұмыс істейді, Фейстел желісі қандай рөл атқарады?
- ГОСТ 28147-89 DES-тен қандай негізгі айырмашылықтарға ие?
- Криптоанализ дегеніміз не және ол симметриялық шифрлардың қауіпсіздігін қалай бағалайды?
- DES жүйесін жетілдіру үшін криптография тұрғысынан қандай ұсыныстар айтуға болады?

Пайдаланылған әдебиеттер:

- Cortez R. M., Okoshi M. P., Okoshi K. (2022). Cryptographic Algorithms and their Applications. Journal of Cryptographic Research.
- Monte I. P., Faro D. C., Trimarchi G., et al. (2023). A New Approach to Symmetric Cryptosystems. Cryptography and Security.
- Martini L., Lisi M., Pastore M. C., et al. (2024). Enhanced Security in Symmetric Cryptosystems. Journal of Computer Security.