**Лабороторна работа №5**

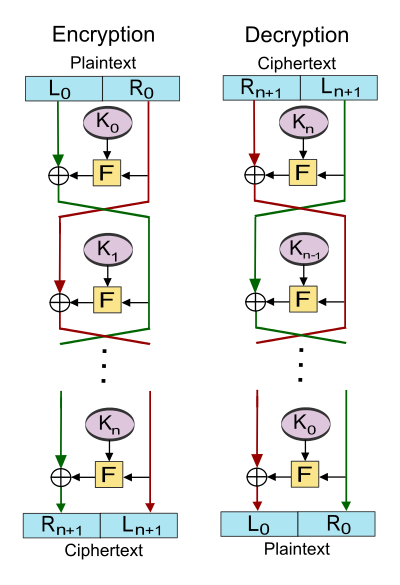
**Тема:** Криптоалгоритм “DES”

**Мета:** Відпрацювання та закріплення теоретичних відомостей криптоалгоритму “DES”

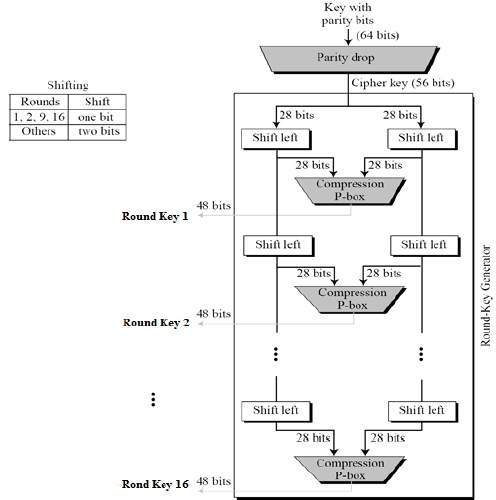
**Короткі відомості:**

DES (Data Encryption Standard) — це симетричний алгоритм шифрування певних даних, стандарт шифрування прийнятий урядом США із 1976 до кінця 1990-х, з часом набув міжнародного застосування. Ще з часу свого розроблення алгоритм мав назву Lucifer і викликав неоднозначні відгуки. Оскільки DES містив засекречені елементи своєї структури, породжувались побоювання щодо можливості контролю з боку Агентства Національного Безпеки США (National Security Agency). Алгоритм піддавався критиці за малу довжину ключа, що, врешті, після бурхливих обговорень та контролю академічної громадськості, не завадило йому стати загальноприйнятим стандартом. DES дав поштовх сучасним уявленням про блочні алгоритми шифрування та криптоаналіз.

Для шифрування в архітектурі DES використовується архітектура Мережи Фейстеля в 16 раундів. Даний алгоритм Мережа Фейстеля розроблявся для апаратної реалізації тому мав високу швидкодію, можливість використання однакові модулі (процедури) при зашифруванні та розшифруванні, не треба обчислювати обернену функцію, отже єдина вимога – раундова функція має бути незворотною, недоліком є те що за раунд шифрується лиш половина блоку дана архітектура також використовувалася в ГОСТ 28147-89. .

DES є блочним шифром - дані шифруються блоками по 64 біти - 64 бітний блок явного тексту подається на вхід алгоритму, а 64-бітний блок шифрограми отримується в результаті роботи алгоритму. Крім того, як під час шифрування, так і під час дешифрування використовується один і той самий алгоритм (за винятком дещо іншого шляху утворення робочих ключів).

Проста схема процесу шифрування симетричного алгоритму DES



Ключ має довжину 56 біт (як правило, в початковому вигляді ключ має довжину 64 біти, де кожний 8-й біт є бітом паритету, крім того, ці контрольні біти можуть бути винесені в останній байт ключа). Ключем може бути довільна 64-бітна комбінація, яка може бути змінена у будь-який момент часу. Частина цих комбінацій вважається слабкими ключами, оскільки може бути легко визначена. Безпечність алгоритму базується на безпечності ключа.

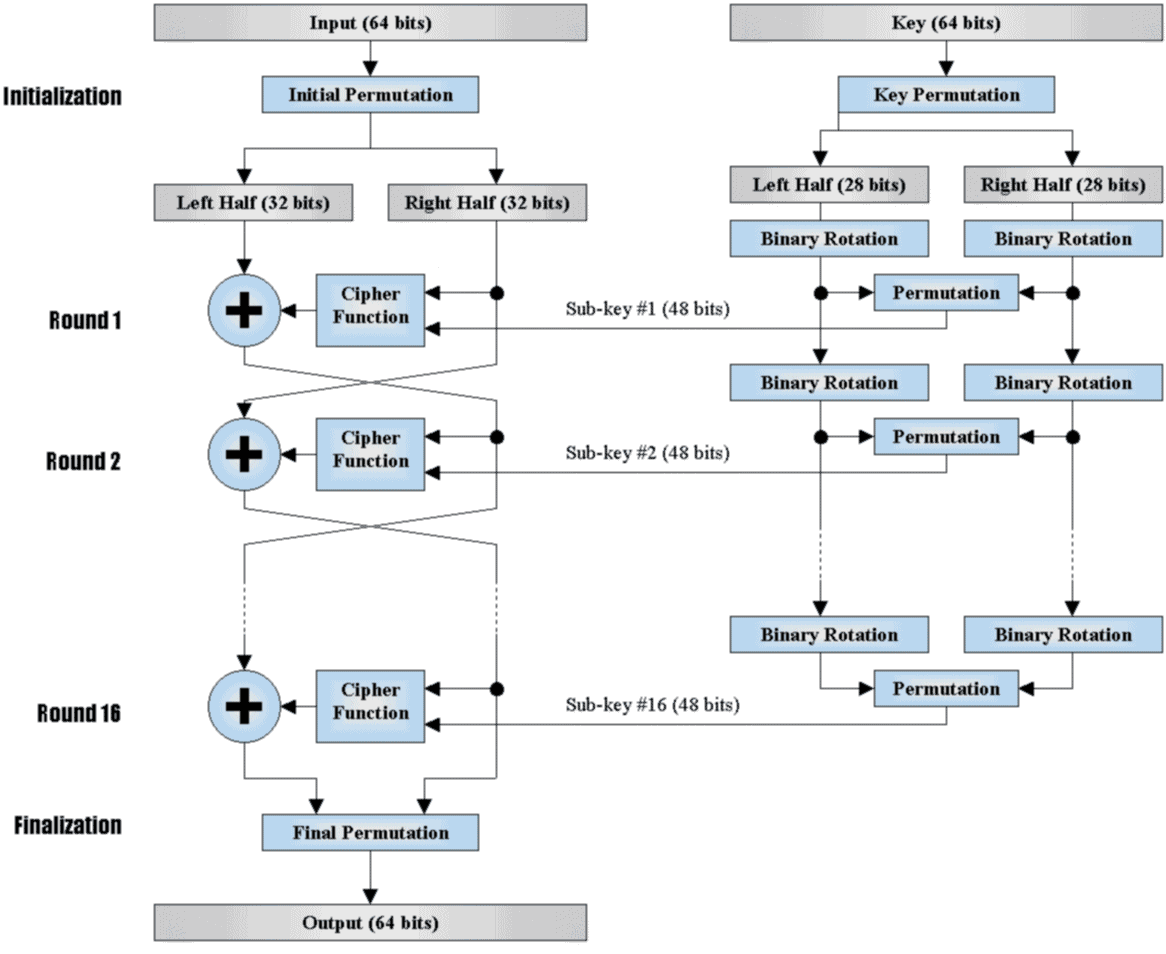
На найнижчому рівні алгоритм є ніщо інше, ніж поєднання двох базових технік шифрування: перемішування і підстановки. Цикл алгоритму, з яких і складається DES є комбінацією цих технік, коли як об'єкти перемішування виступають біти тексту, ключа і блоків підстановок.

Через високу розповсюдженість DES було запропоновано багато ідей щодо підвищення його безпеки, зокрема, замінити S-блоки DES новими, стійкими до лінійної атаки. Однак, широке практичне застосування жодна з видозмінених версій DES не набула. Винятком є потрійний DES (тріпл-DES), однак, це не видозміна алгоритму, а лише особливий режим шифрування звичайним DES.

**Різновиди 3DES:**

* 3DES-EEE3 (використовуються операції шифрування-шифрування-шифрування) з трьома ключами;
* 3DES-EDE3 (використовуються операції шифрування-розшифрування-шифрування) з трьома ключами;
* 3DES-EEE2 – 3DES-EDE2 (різновиди з двома ключами).

Зараз DES вважається ненадійним в основному через малу довжину ключа (56 біт) та розмір блоку (64 біти). У 1999 ключ DES було публічно дешифровано за 22 години 15 хвилин. Вважається, що алгоритм достатньо надійний для застосування у модифікації 3-DES, хоча існують розроблені теоретичні атаки. DES поступово витісняється алгоритмом AES, що з 2002 року є стандартом США.



Початкові та кінцеві перестановки є повністю оберненими

**Висновок:** Оскільки DES - порівняно старий криптоалгоритм, існує багато публікацій щодо його криптоаналізу.

Тепер DES вважається нестійким, оскільки: розмір ключа - 56 бітів - замалий, тому існує реальна загроза пошуку ключа лобовою атакою (послідовним перебором);

DES нестійкий до лінійного криптоаналізу (тобто лінійна атака дозволяє знайти ключ DES швидше, ніж послідовний перебір), в той же час, повний 16-раундовий DES стійкий до диференційного криптоаналізу.

Отже перевагами є: висока швидкодія, можливість використання одних апаратних та програмних продуктів для зашифрування і розшифрування.

Недоліки: мала довжина ключа, за один раунд шифрується лише половина блоку, наявність слабких ключів, застаріла архітектура.