

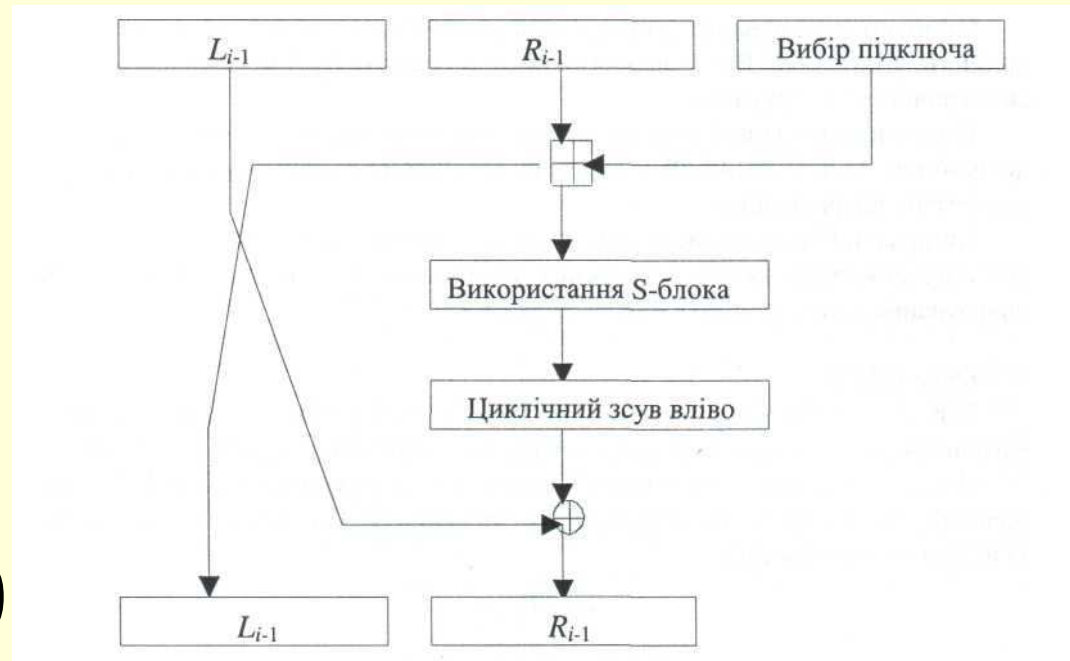
Симетричні криптосистеми.

Блокові шифри:
Стандарт шифрування ГОСТ
28147-89

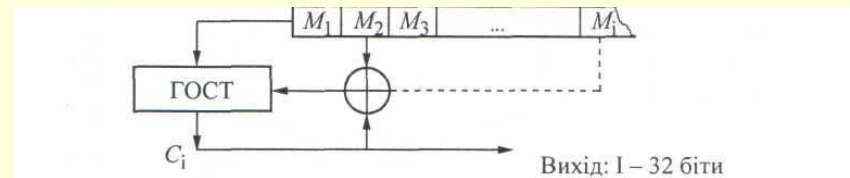
Режими застосування блокових
шифрів

(ілюстративний матеріал до лекції)

Блок-схема одного етапу алгоритму ГОСТ28147-89



Імітовставка стандарту ГОСТ 28147-89



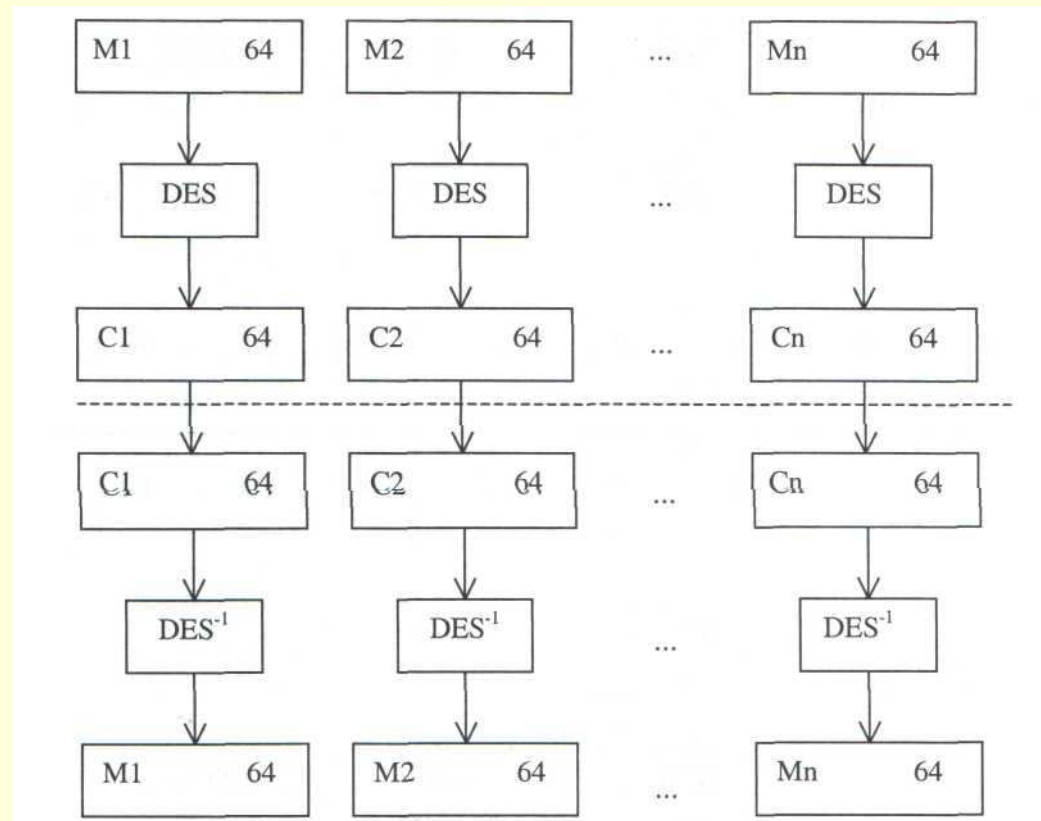
Використання підключів на різних етапах ГОСТу

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

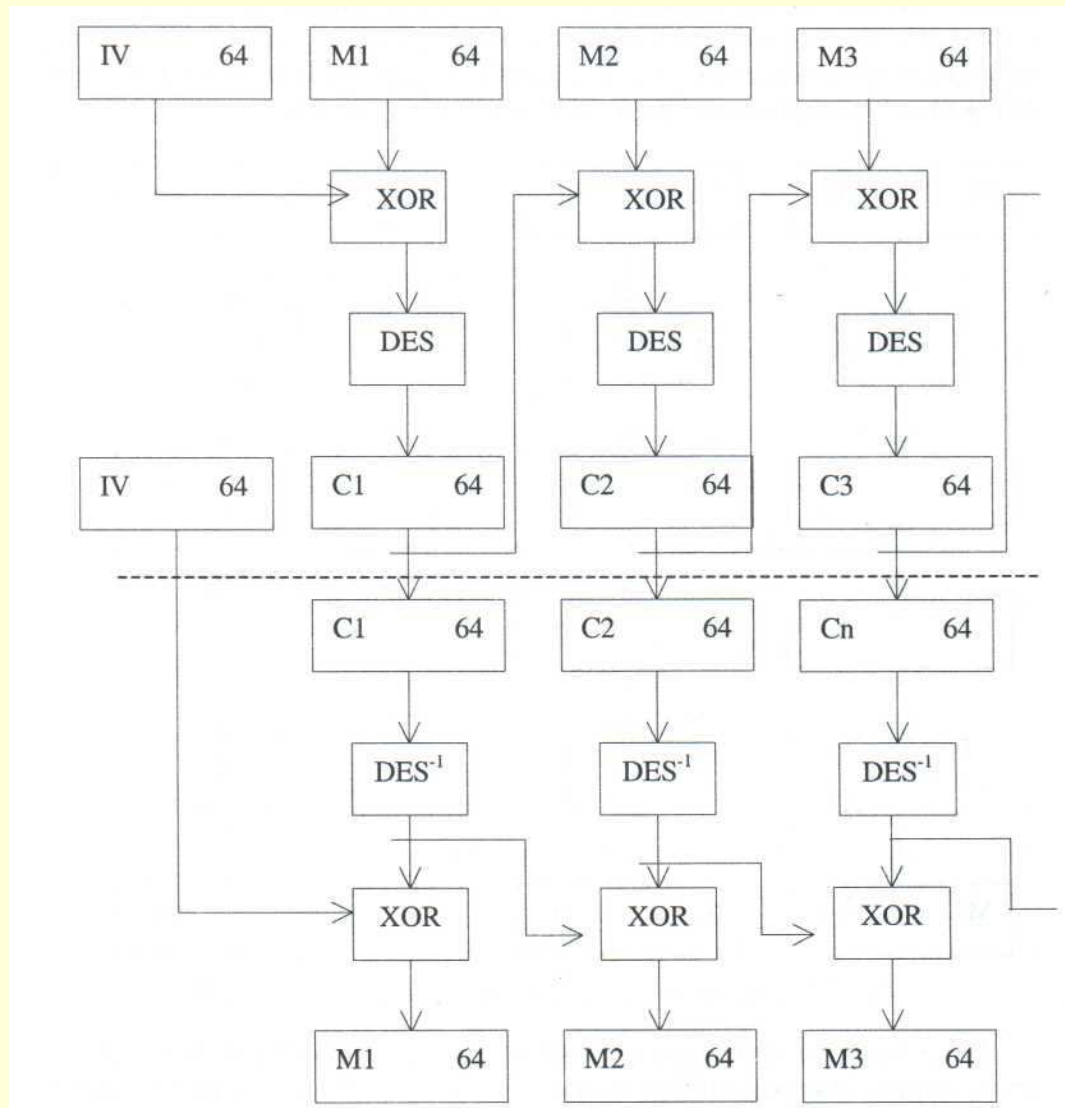
Режими застосування блокових шифрів

Режими застосування блокових шифрів	Модифікації режимів
- електронної кодової книги (ECB – Electronic Code Book)	
- зчеплення блоків шифрованого тексту (CBC – Cipher Block Chaining)	- зчеплення блоків шифрованого тексту з поширенням (PCBC – Propagating; - зчеплення блоків шифрованого тексту з контрольною сумою (CBCC – CBC with Checksum)
- оберненого зв'язку по шифрованому тексту (CFB – Cipher Feedback)	
- оберненого зв'язку по виходу (OFB – Output Feedback)	- оберненого зв'язку по виходу з нелінійною функцією (OFBNLF – OFB with a Nonlinear Function)

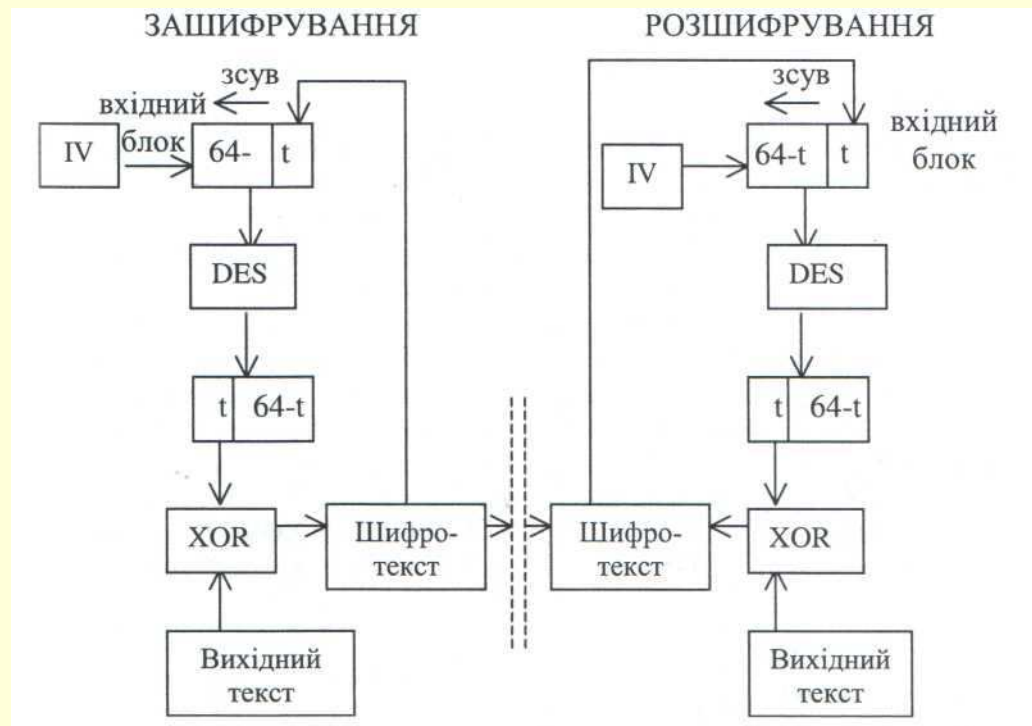
Блок-схема роботи блокового шифру в режимі ЕСВ



Блок- схема роботи блокового шифру в режимі CBC



Блок-схема роботи блокового шифру в режимі CFB



Блок-схема роботи блокового шифру в режимі OFB

