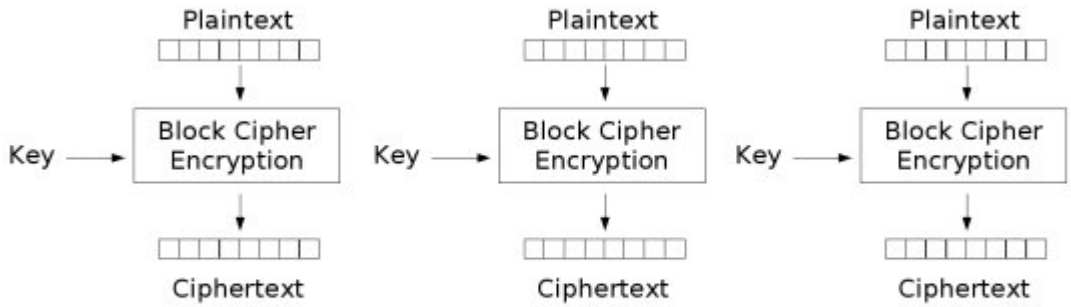
Симетричні криптоалгоритми

Режими роботи симетричних шифрів

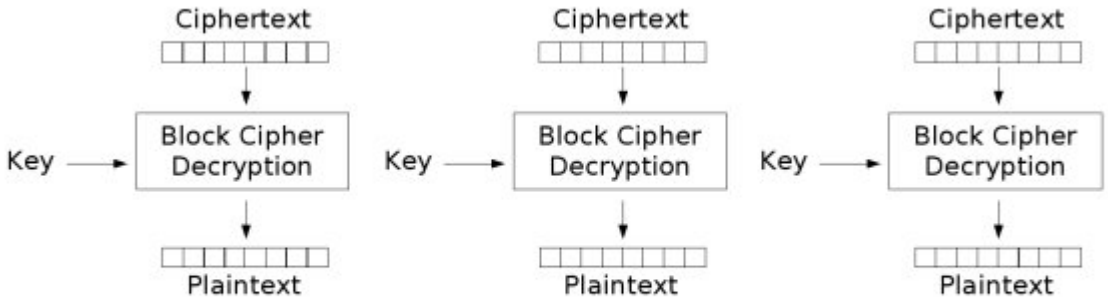
Для чого потрібні різні режими?

- Уявимо ситуацію, коли нам треба зашифрувати документ, довжина якого значно більша за довжину блоку шифру. Як ми будемо це робити?
- Найбільш очевидной варіант такий:
  - Розбиваємо текст на блоки (залежно від довжини вхідного блоку того чи іншого шифру);
  - Генеруємо ключ шифрування;
  - Шифруємо кожен блок на цьому ключі до кінця тексту.

Режим електронної кодової книги (Electronic Code Book - ECB)



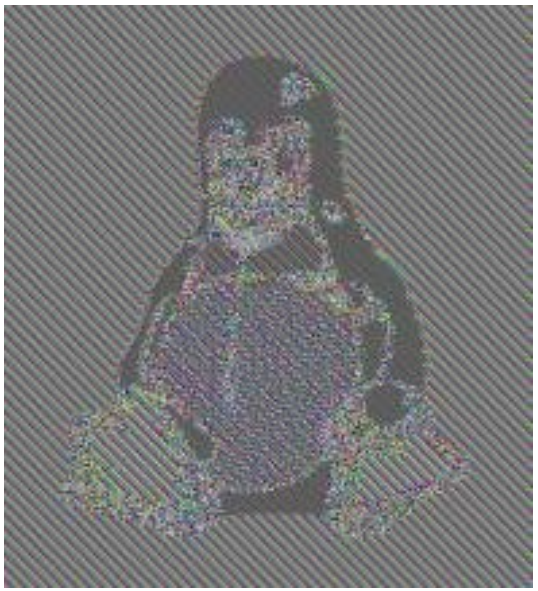
Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

Приклад шифрування ECB

Відкрите повідомлення

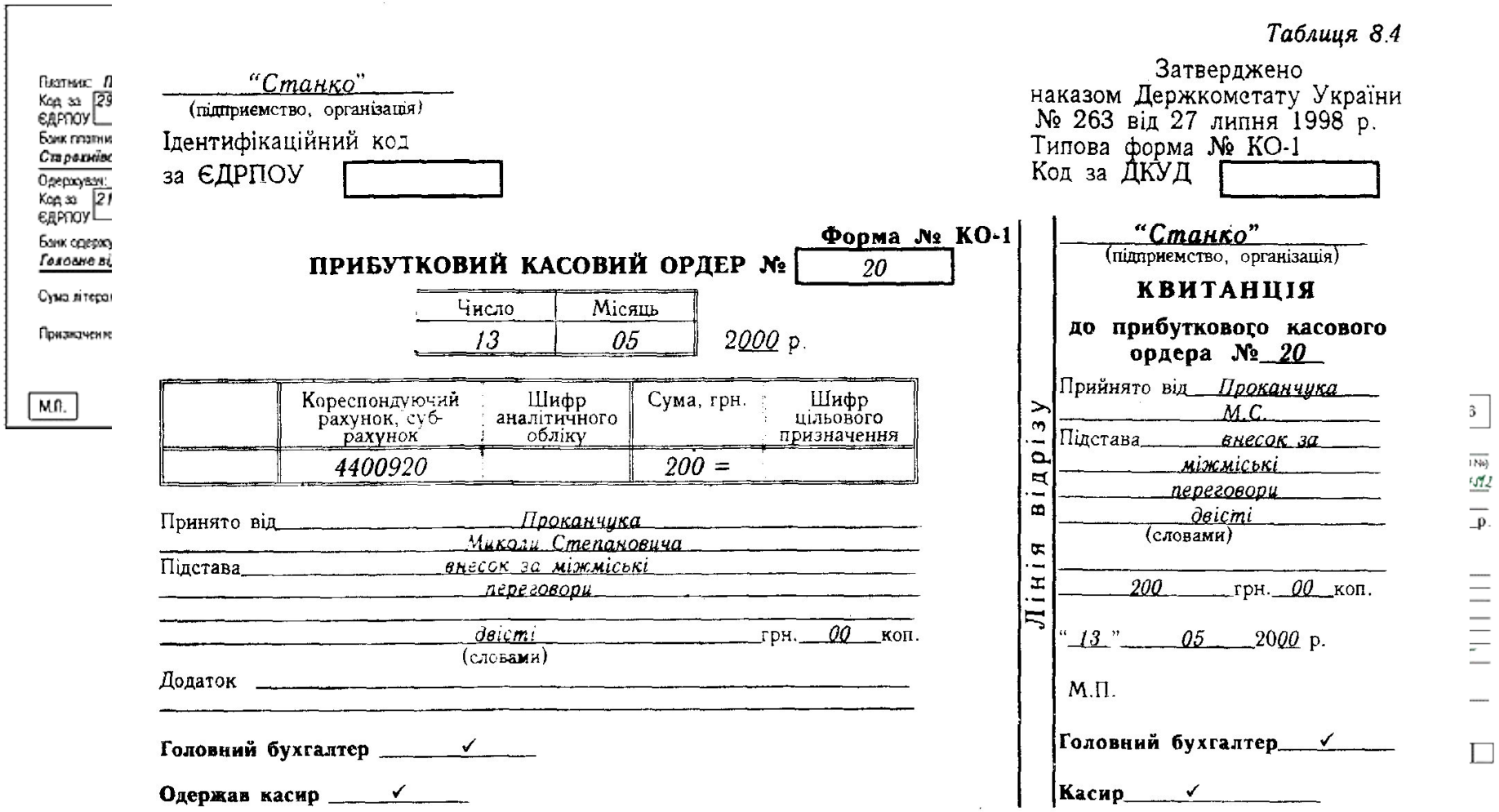


Зашифроване в режимі ECB

Режим електронної кодової книги (Electronic Code Book - ECB)

- Проаналізуємо безпеку цього способу.
  - Все добре, доки у нас не зустрінуться однакові слова;
  - А якщо це фінансовий документ, який має чітку структуру, і ця структура відома зловмиснику?
  - Приклад — платіжне доручення; накладна; будь який платіжний документ.

Режим електронної кодової книги (Electronic Code Book - ECB)



Таблиця 8.4

"Станко"
(підприємство, організація)
Ідентифікаційний код за ЄДРПОУ

Затверджено наказом Держкометату України № 263 від 27 липня 1998 р.
Типова форма № КО-1
Код за ДКУД

Форма № КО-1

ПРИБУТКОВИЙ КАСОВИЙ ОРДЕР № 20

Число	Місяць
13	05

2000 р.

	Кореспондуючий рахунок, суб-рахунок	Шифр аналітичного обліку	Сума, грн.	Шифр цільового призначення
	4400920		200 =	

Принято від Проканчука Миколи Степановича
Підстава внесок за міжміські переговори
двісті грн. 00 коп.
(словами)
Додаток

Головний бухгалтер ✓
Одержав касир ✓

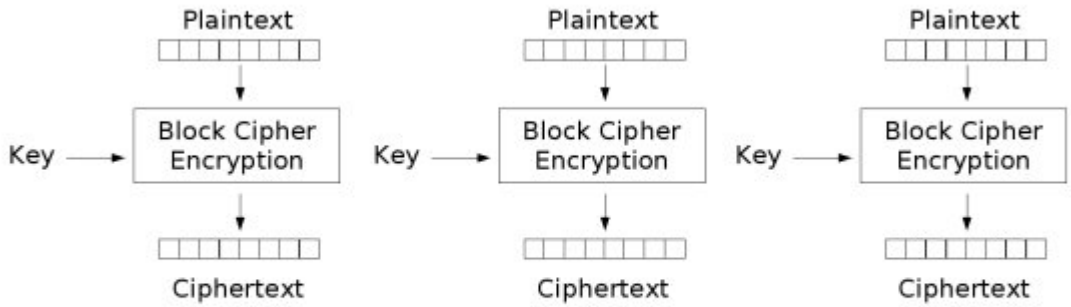
Лінія відрізу

"Станко"
(підприємство, організація)

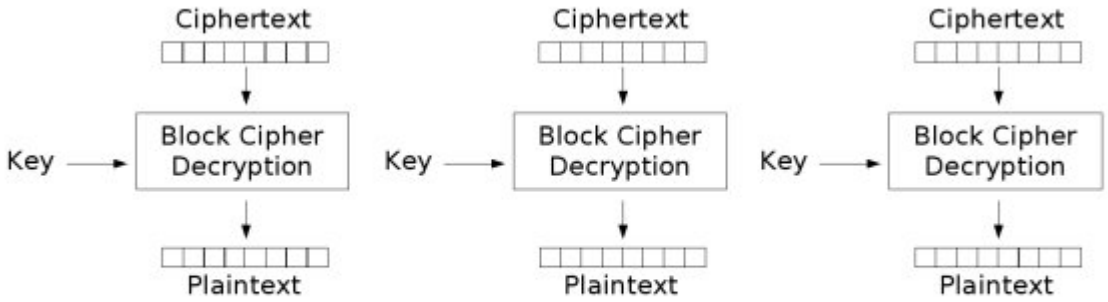
КВИТАНЦІЯ
до прибуткового касового ордера № 20

Прийнято від Проканчука М.С.
Підстава внесок за міжміські переговори
двісті
(словами)
200 грн. 00 коп.
"13" 05 2000 р.
М.П.
Головний бухгалтер ✓
Касир ✓

Режим електронної кодової книги (Electronic Code Book - ECB)



Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

Помилка розповсюджується лише на той блок, де вона сталася.

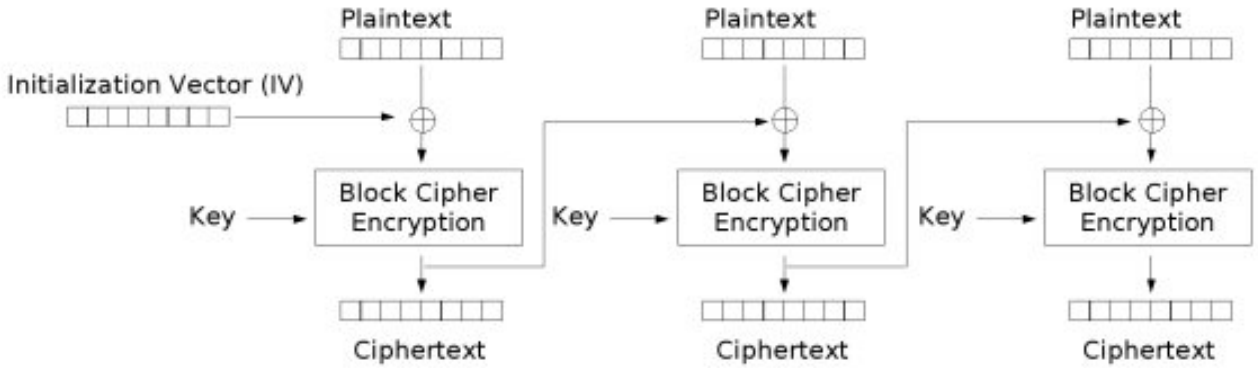
ECB - режим

- Переваги:
  - Простота реалізації;
  - Найвища швидкодія;
  - Малий вплив помилок в каналі зв“язку.
- Неодліки:
  - Однакові блоки шифруються в однаковий шифротекст.
- ==========
- Рекомендовані використання:
  - Шифрування криптографічних ключів, векторів ініціалізації;
  - Шифрування коротких (1 блок) повідомлень.
  - ==========
- **Є основним режимом роботи ГОСТ 28147-89**.

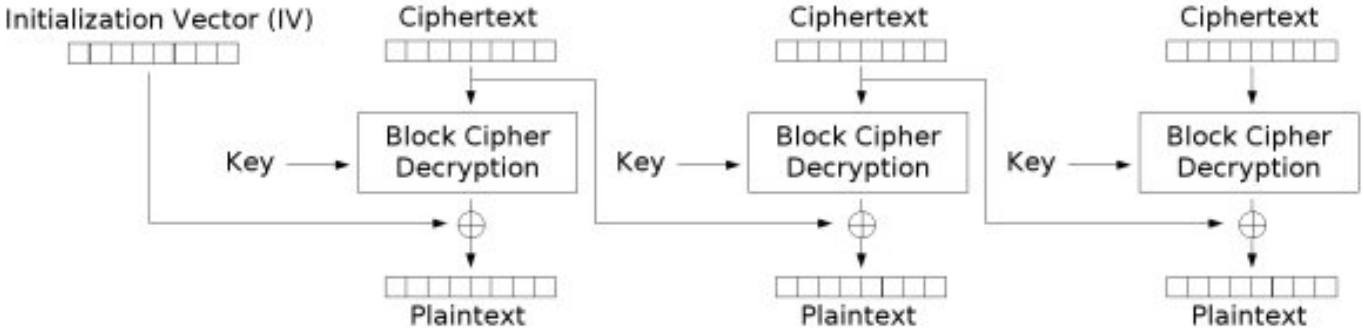
Для чого потрібні різні режими?

- Висновок:
  - Необхідно придумати такі режими роботи, щоби компенсувати вказані недоліки.
- Як це можна зробити?

Режим CBC — Cipher Block Chaining



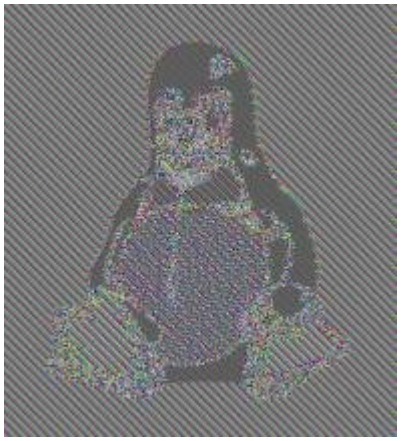
Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

CBC — Cipher Block Chaining

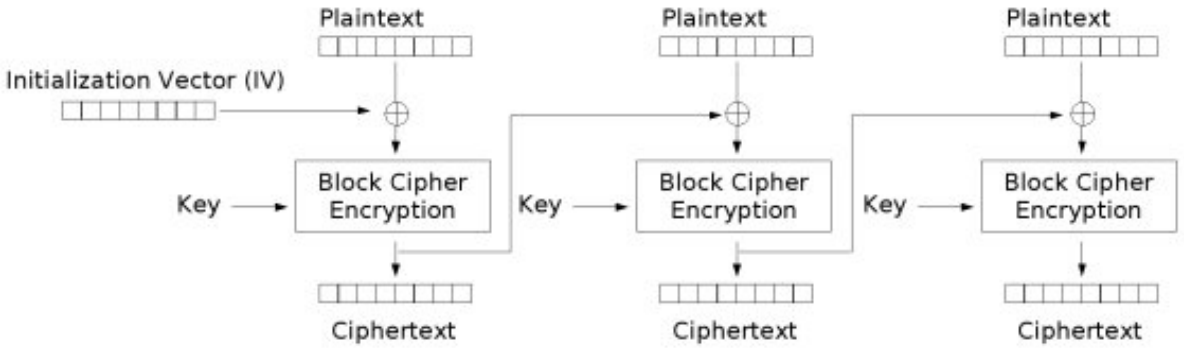
Оригінал



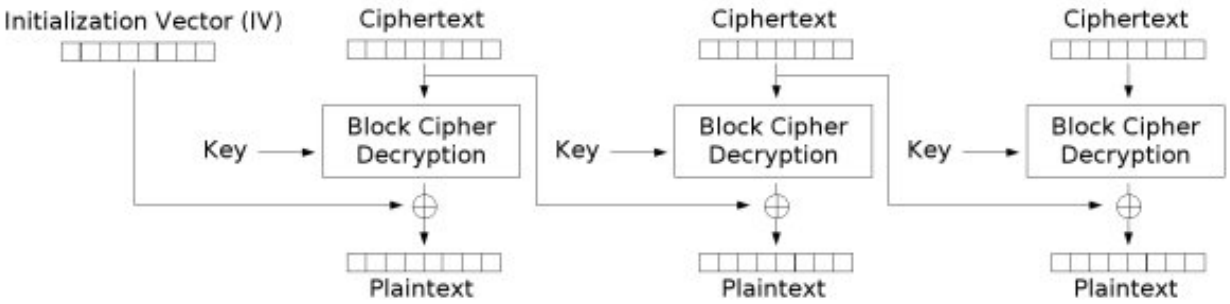
Режим ECB

Режим CBC

Режим CBC — Cipher Blocks Chaining



Cipher Block Chaining (CBC) mode encryption



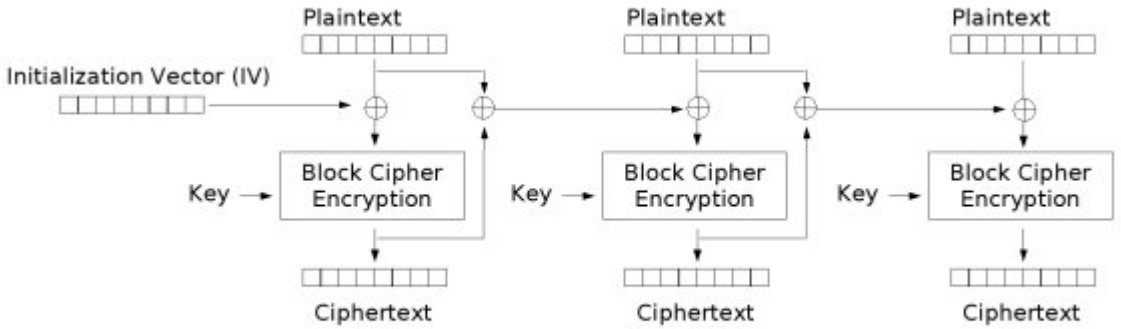
Cipher Block Chaining (CBC) mode decryption

Помилка розповсюджується на поточний та наступний блоки тексту.

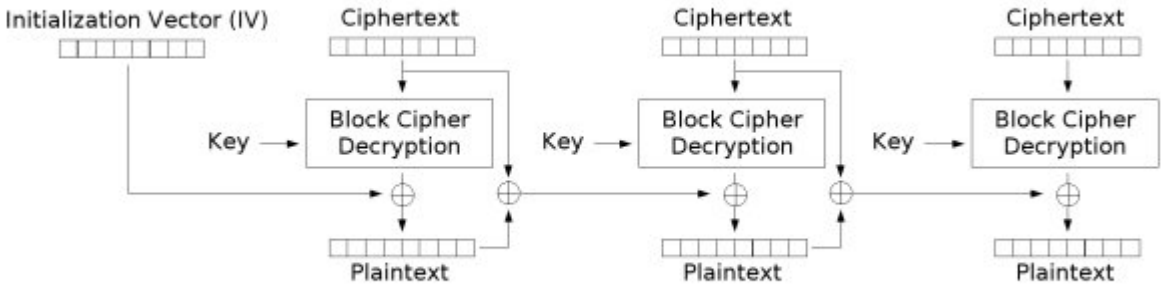
Режим CBC

- Переваги:
  - Значно підвищує криптостійкість симетричного шифру;
  - Висока швидкодія режиму (додатково виконується лише одна операція XOR).
- Недоліки:
  - Вимагає вектора ініціалізації;
  - Помилка розповсюджується на наступні блоки тексту.
  - Проблема з розпаралелюванням.

Модифікації режиму CBC - PCBC



Propagating Cipher Block Chaining (PCBC) mode encryption



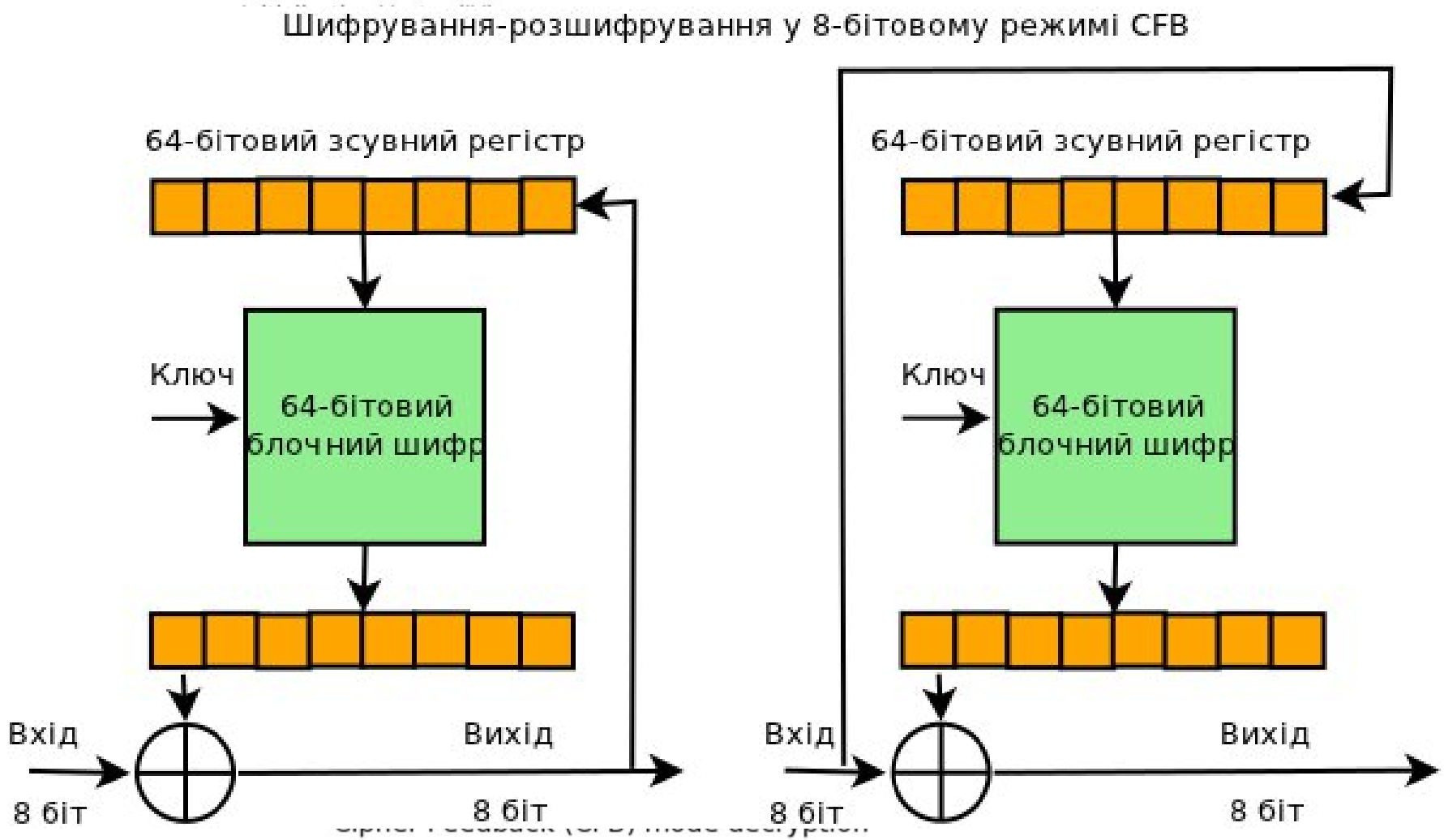
Propagating Cipher Block Chaining (PCBC) mode decryption

Призначення — найменші зміни у відкритому тексті вплинуть на шифротекст.

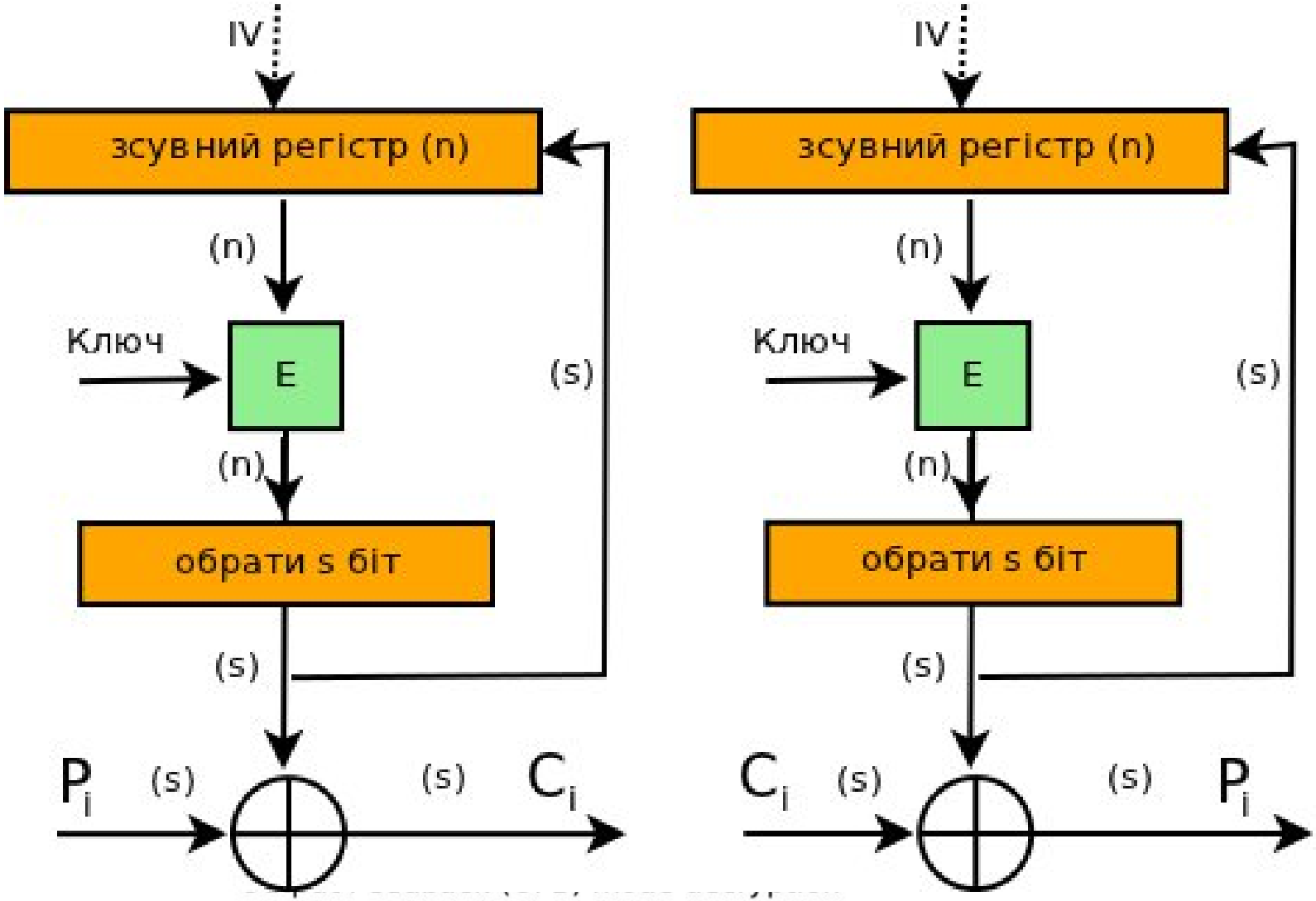
Режим CBCC

- Режим CBCC — CBC with Checksum — відрізняється від CBC тим, що перед шифруванням чергового блоку тексту до нього додається сума за модулем 2 усіх попередніх блоків.
- Таким чином можна організувати захист цілісності повідомлення.

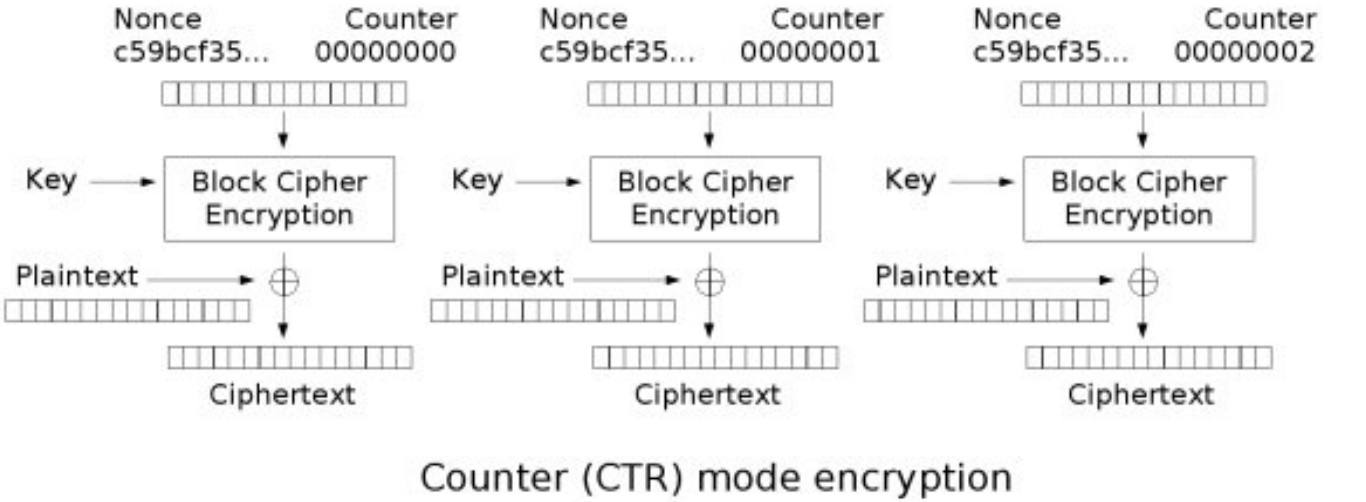
Режим CFB — Cipher FeedBack



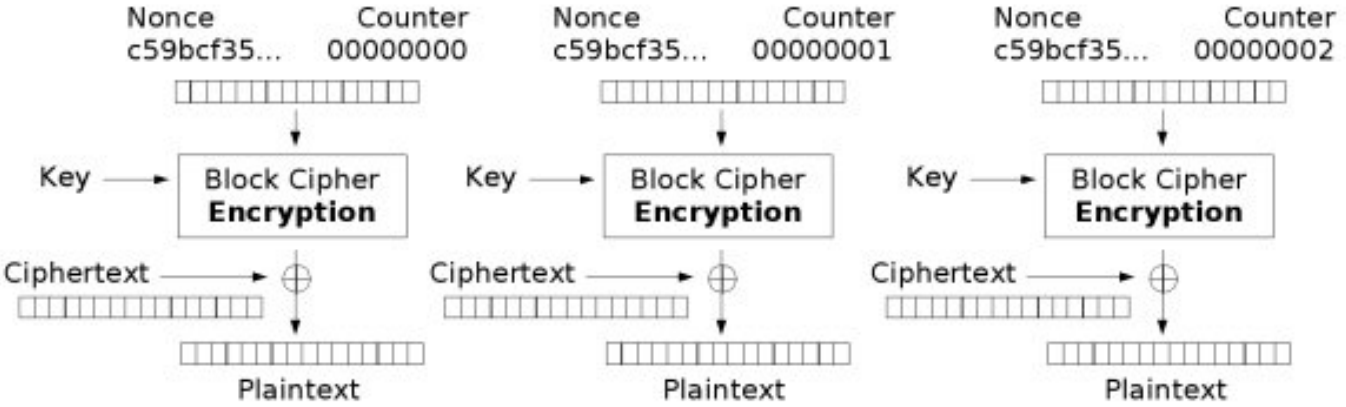
Режим OFB — Output FeedBack



Режим лічильника (CTR - counter)



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Розповсюдження помилок

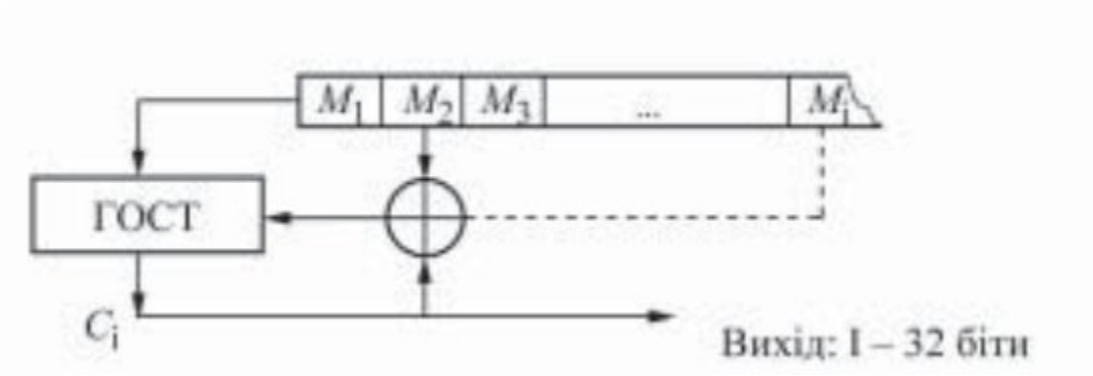
- Режими CFB, OFB та CTR для блоку 8 бітів перетворюють блоковий шифр в потоковий, тобто такий, який шифрує літери окремо.
- Відмінності режиму CFB від інших полягають в тому, що помилка, яка зустрінеться в деякому блоці під час передавання каналом зв“язку, буде розповсюджуватися доти, поки регістр зсуву повністю не очиститься (тобто на 8 наступних символів).
- Режими OFB та CTR не розповсюджують помилки: помилка зустрічається лише в тому блоці, де вона сталася.
- ==========
- Режим ECB також не розповсюджує помилку: вона зустрічається лише в тому блоці, де сталася.
- Режим CBC — розповсюджує помилку на поточний та наступний блоки тексту (64+ 64 біти).

Використання режимів

- Режим ECB використовують для шифрування криптографічних ключів або векторів ініціалізації. В стандарті ГОСТ 28147-89 цей режим роботи — основний.
- Режим CBC — основний режим роботи сучасних симетричних шифрів. Він найбільш придатний для шифрування каналів зв“язку. Крім того, оскільки він залежить від вектора ініціалізації, ключа та усього тексту, то останній блок використовують як MAC (Message Authentication Code — код аутентифікації повідомлень)
- Режими OFB CFB CTR використовують для шифрування каналів зв“язку, особливо OFB, який не розповсюджує помилку. CFB — часто використовують для аутентифікації.

Режим генерування імітовставки

- Ще один режим, який було запропоновано в стандарті ГОСТ 28147-89 — режим генерування імітовставки (імітоприставки).



Імітовставка залежить від усього тексту та ключа шифрування.
Вектор ініціалізації не використовують.
Призначення — аналог хеш-образу тексту, тобто захищає учасників інформаційного обміну від нав“язування хибних повідомлень.

Симетричні криптоалгоритми

- **Симетричними називаються такі криптоалгоритми, коли для зашифрування та розшифрування використовують один і той самий ключ.**
- **Ми розглянули такі симетричні шифри:**
  - DES;
  - 3DES; DESX;
  - AES;
  - Калина.

Симетричні криптоалгоритми

- **Переваги симетричних криптосистем**
  - Висока швидкість;
  - Висока криптостійкість при порівняно невеликому ключі;
  - Дослідженість алгоритмів, а значить мала ймовірність знаходження нових критичних вразливостей;
  - Можливість використання одних модулів для зашифрування та розшифрування.

Симетричні криптоалгоритми

- **Неодліки симетричних криптосистем**
  - Проблема розповсюдження та зберігання ключів;
  - Велика кількість ключів для розгалуженої системи обміну даними;
  - Наявність класів слабких ключів.

Симетричні криптоалгоритми

- Тим не менше, симетричні криптосистеми залишаються найбільш популярним вибором для криптографічного захисту інформації будь-якого ступеня секретності.
- Вони використовуються в усіх сучасних системах захисту інформації та захищених протоколах.