Проблемы, решаемые криптографией

- конфиденциальность
- целостность
- аутентификация
- невозможность отказа от авторства

Виды шифрования

Симметричное

- Общие или легко связываемые ключи шифрования
- Типичные длины ключей 128-256 бит

Ассимметричное

- Различные, неочевидно связанные ключи для шифрования
- Типичные длины ключей: 1024-4096 для операций в конечном поле, 256 бит для операций на эллиптической кривой

Принцип Керкхоффса

Надежность системы шифрования не должна основываться на ее секретности. Система должна оставаться надежной даже если все ее компоненты, кроме ключа стали известны атакующему.

Симметричные шифры

Типы симметричных шифров

Блочные

- Шифруется блок данных
- Типичный размер блока - 64 или 128 бит

Потоковые

- Генерируется поток псевдослучайных данных, зависящих от ключа
- Выход - поток бит (или байт), называемый *гаммой* - складывается по модулю с потоком данных

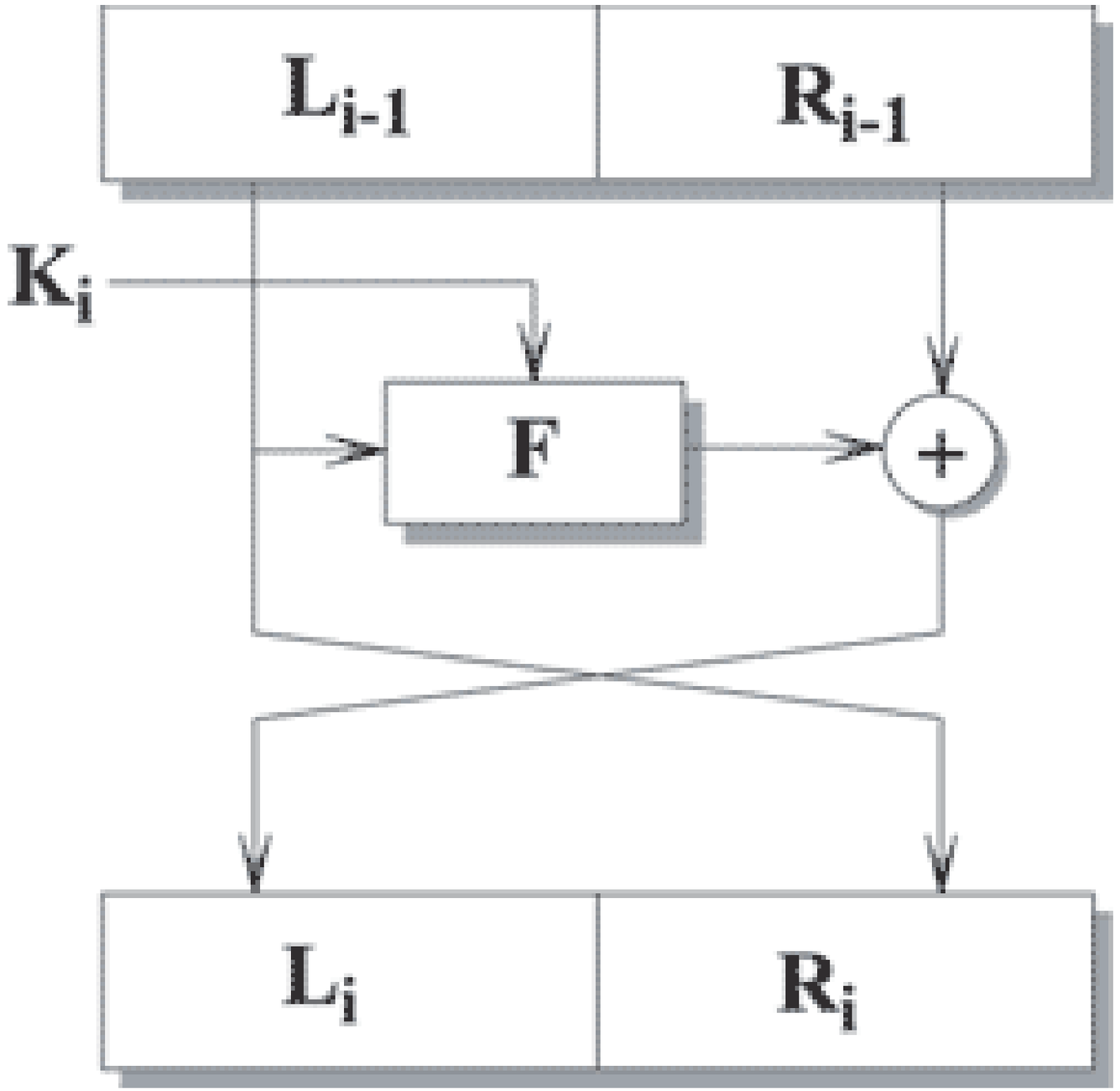
Шифры подстановки

- Табличная подстановка
- Шифр Цезаря
  - Методика взлома
- Полиалфавитные шифры подстановки
- Шифр Виженера

Шифры перестановки

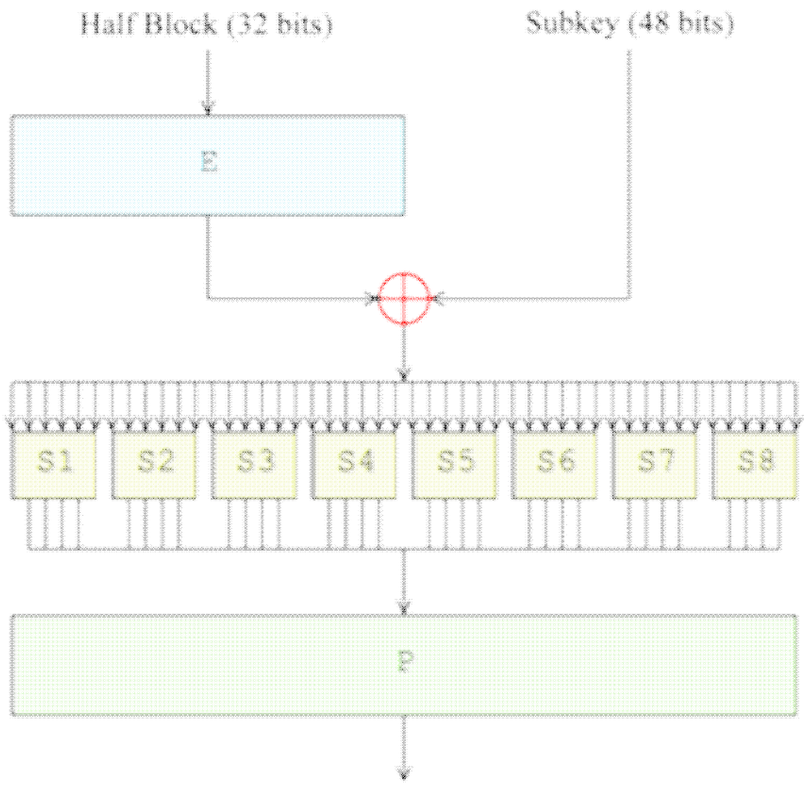
- Простая перестановка
- Перестановка по ключу

Сеть Фейстеля



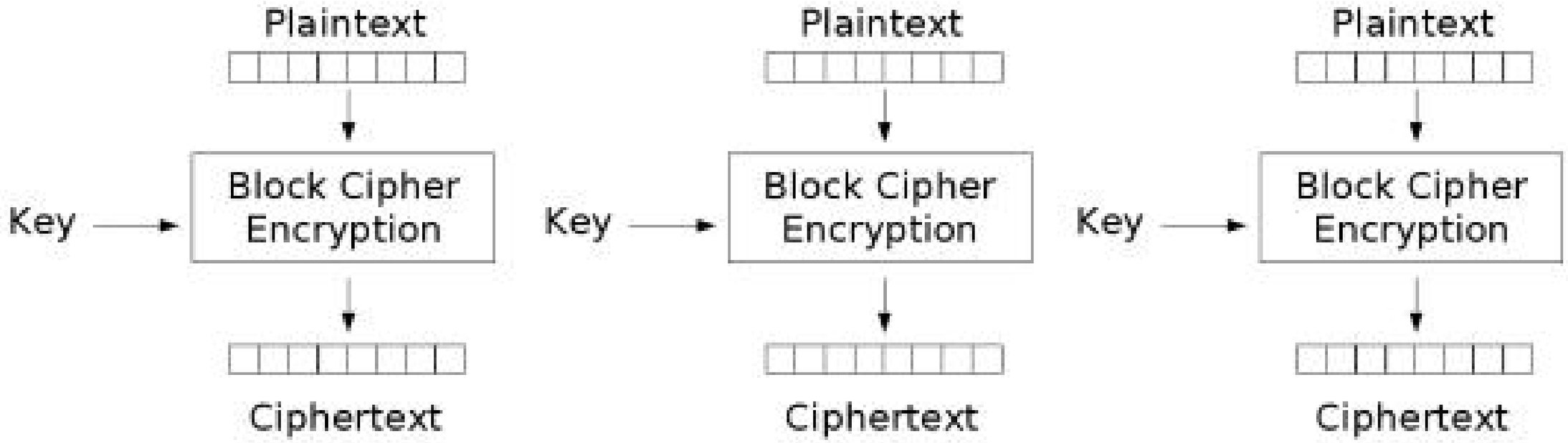
DES

- Сеть Фейстеля
- Размер блока - 64 бита
- Размер ключа - 56 бит
- 16 раундов



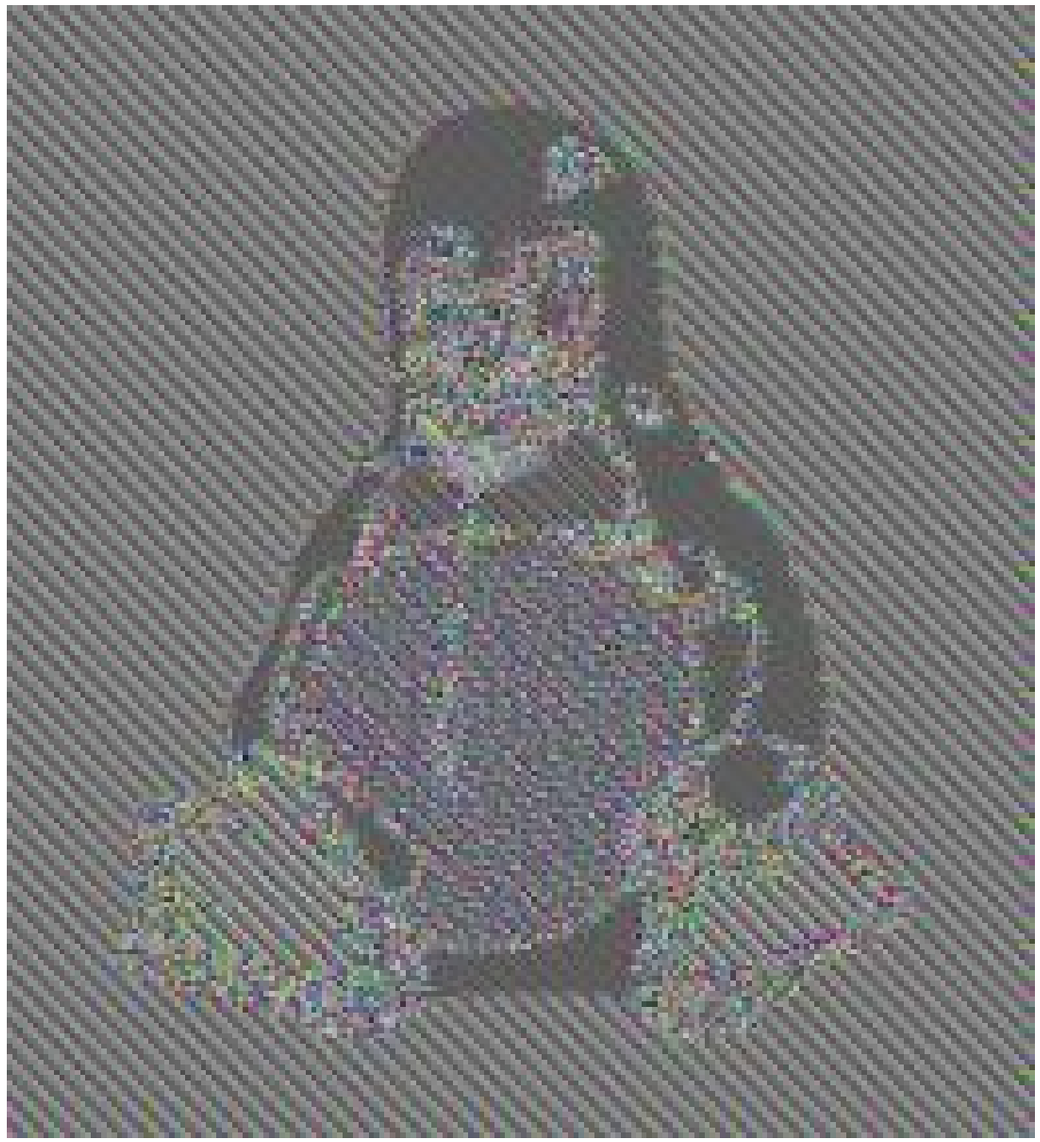
Как зашифровать несколько блоков?

ECB

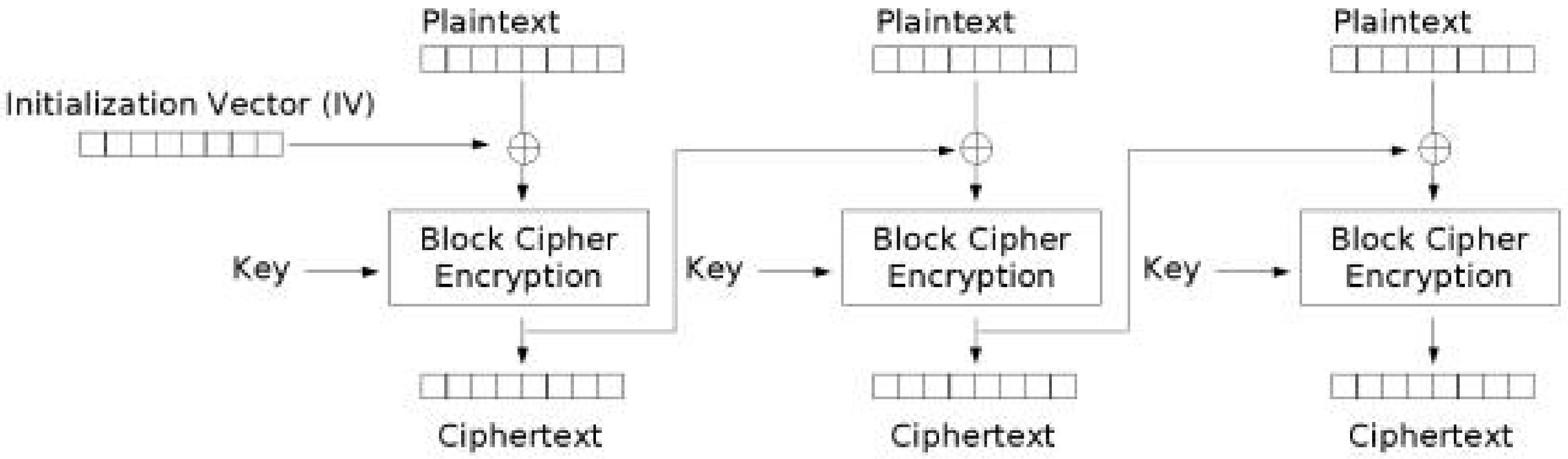


Electronic Codebook (ECB) mode encryption

ECB



CBC

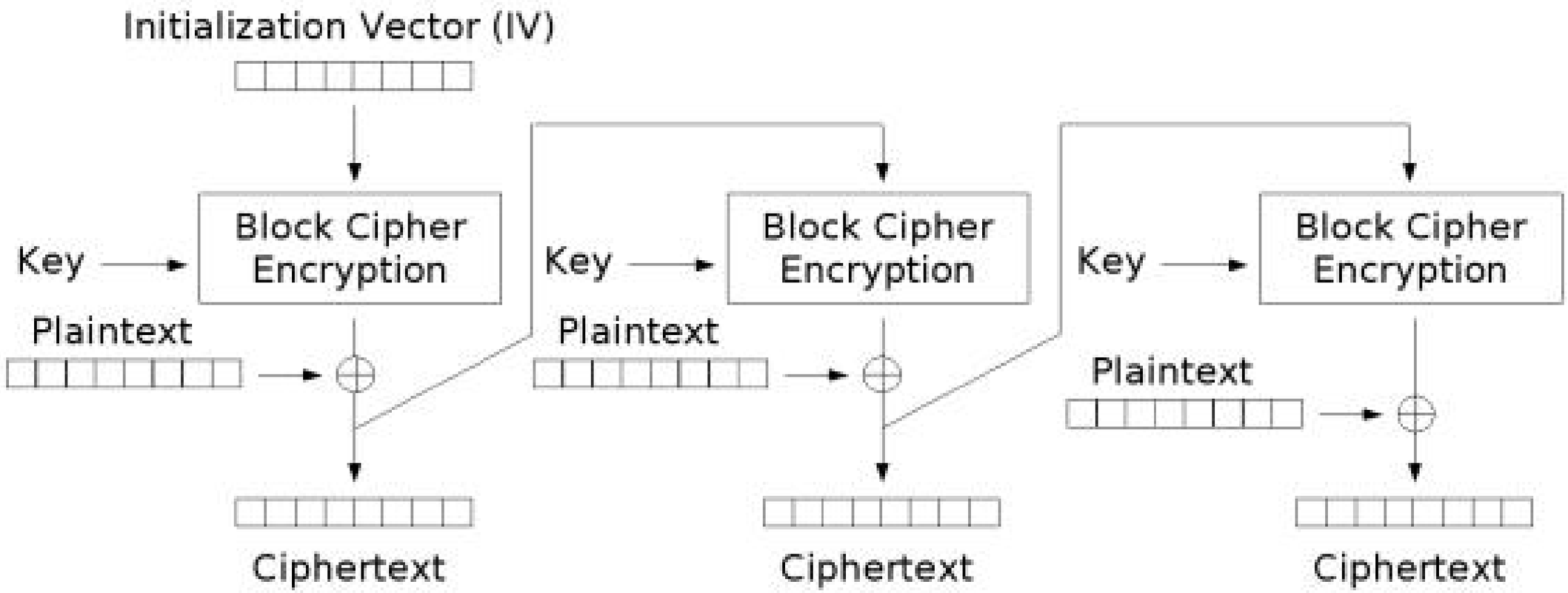


Cipher Block Chaining (CBC) mode encryption

Birthday paradox

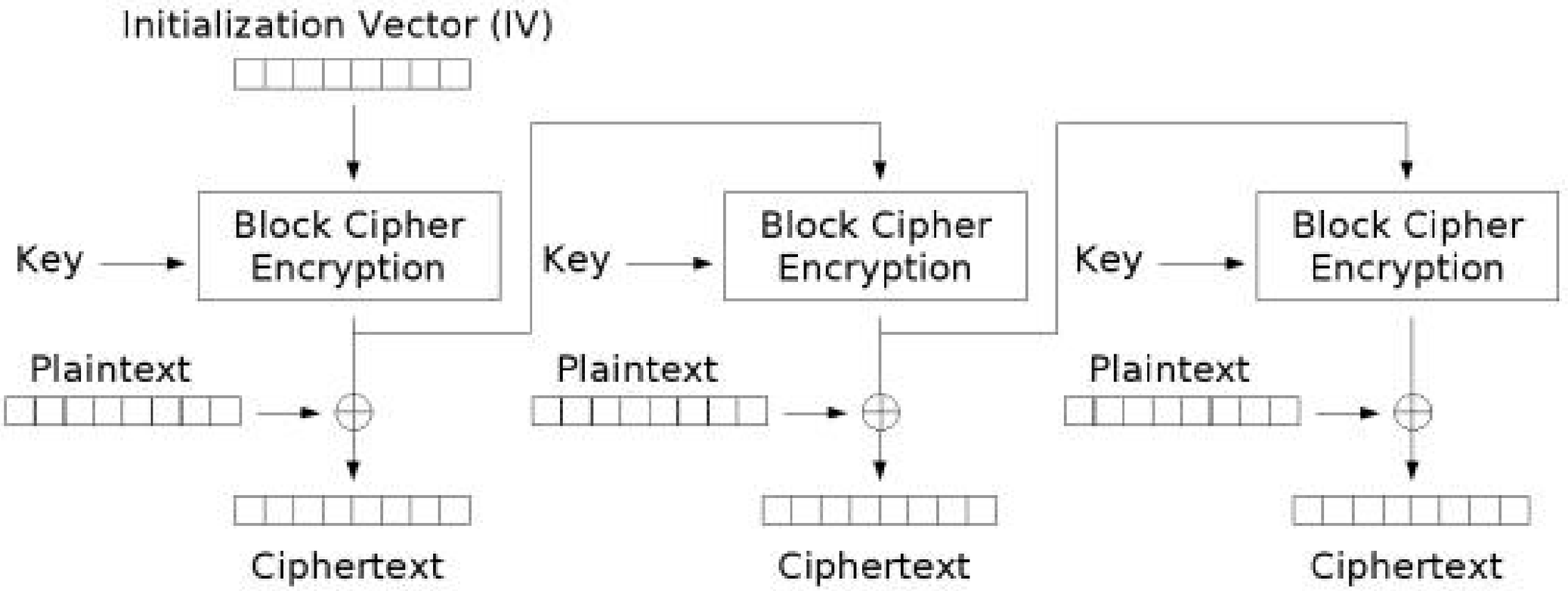
- Какова вероятность совпадения двух блоков выхода шифра?
- Как это влияет на безопасность криптосистемы?
- Сколько времени это займет на реальном трафике?

CFB



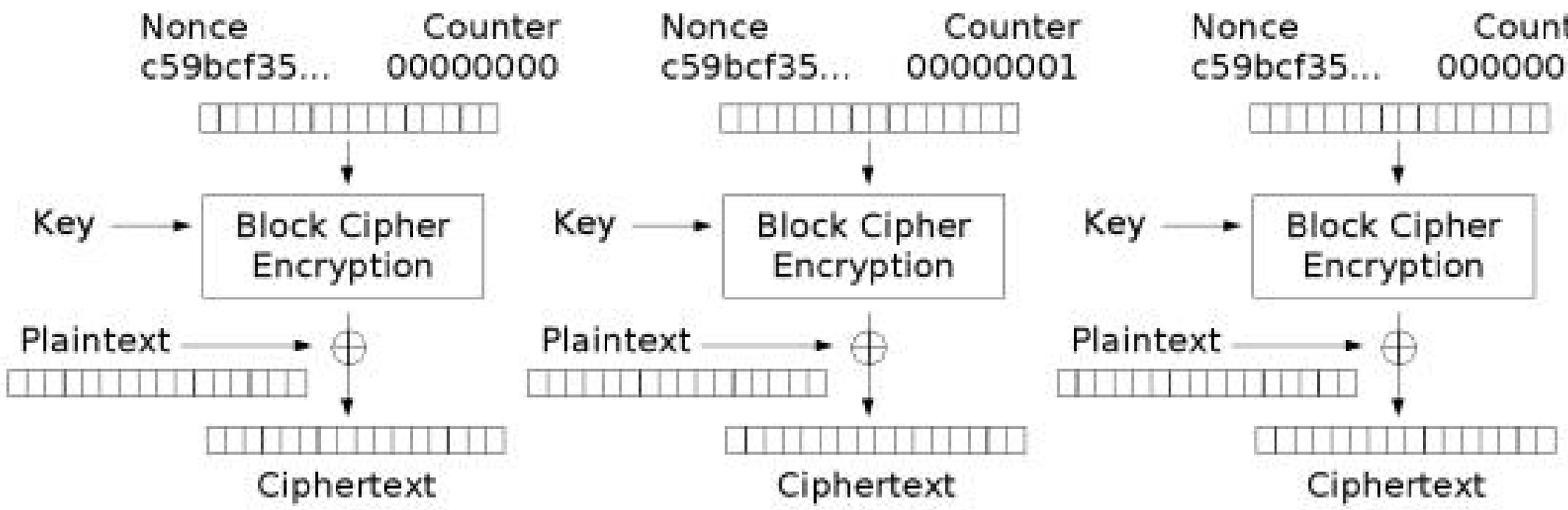
Cipher Feedback (CFB) mode encryption

OFB



Output Feedback (OFB) mode encryption

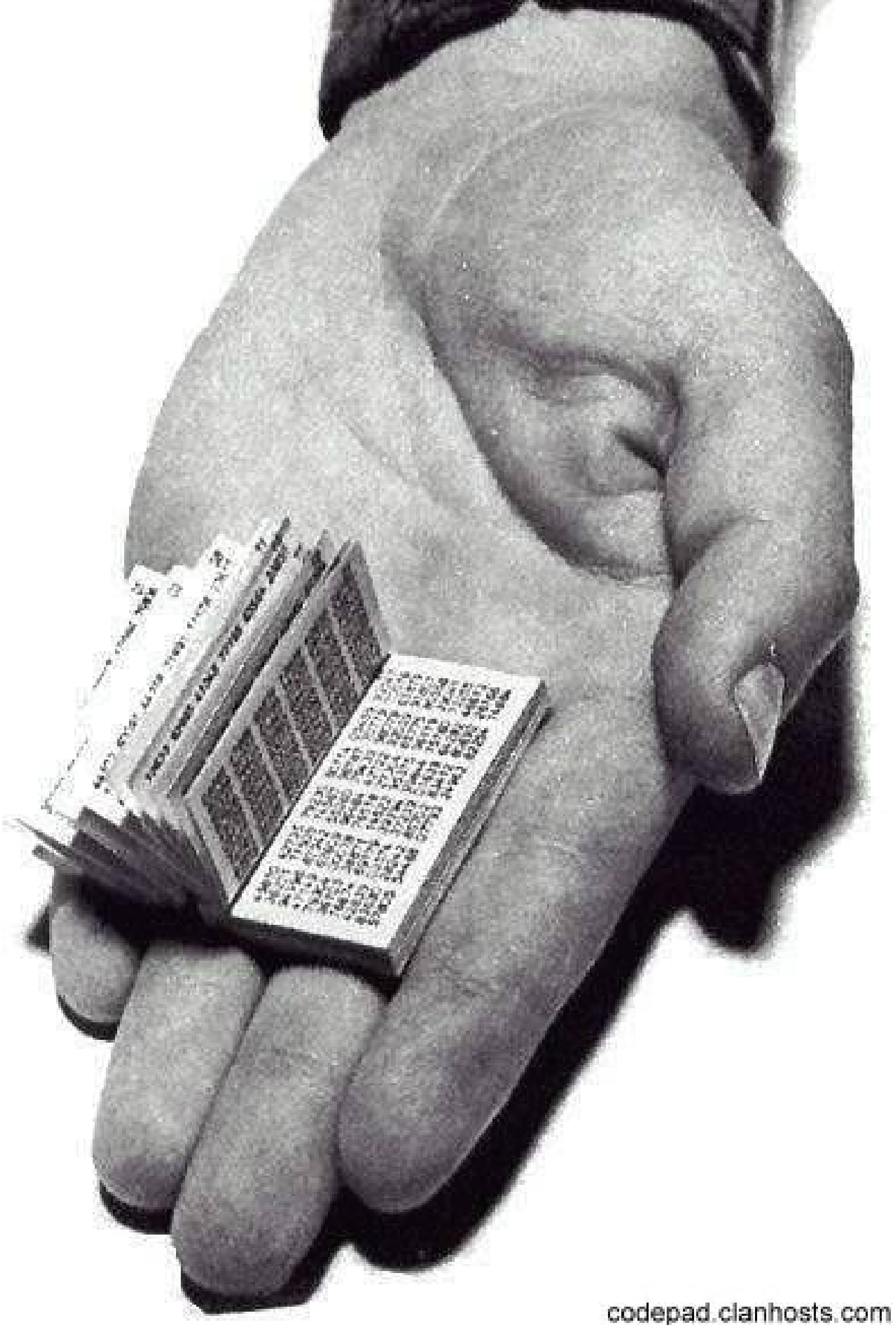
CTR



Counter (CTR) mode encryption

Поточные шифры

- Понятие *гаммы*
- Шифр Вернама



codepad.clanhosts.com