Информациска безбедност

Предавање 2:
Криптографија – прв дел

Проф. д-р Весна Димитрова

Вовед

- Проблем:
  - Како да се спречи некој што неовластено ќе ја преземе пораката да ја открие нејзината содржина?
- Решение:
  - Тоа се прави со “шифрирање” на пораката, така што пристап до оригиналната содржина може да има само оној кому таа му е наменета.

Основни поими од криптологија

Елементи на криптологија

- **Криптологија** - „наука за скриен збор“
- Криптологија е научна област која поврзува два дела:
  - **Криптографија**
  - **Криптоанализа**

Елементи на криптологија

- **Криптографијата** е научна област која се занимава со наоѓање и креирање на методи за шифрирање на податоци со цел да обезбеди нивната тајност и веродостојност.
- **Криптоанализата**, како научна област, се состои од методи за откривање на шифрата, т.е. се занимава со дешифрирање на шифрираните податоци.

Основни поими во криптологија

- Ознаки:
- Со **M** (анг. message) ја означуваме оригиналната порака која сакаме да ја шифрираме и чиј текст е разбирлив за секого.
- Со **C** (анг. cipher) ќе ја означиме шифрираната порака која што претставува неразбирлив текст за оние за кои што не е наменета.

Основни поими во криптологија

- Функцијата која што ја преобразува оригиналната порака **M** во шифрирана порака **C** се нарекува **функција за шифрирање** и се означува со **E** (анг. encryption function).
- Функцијата што ја враќа пораката **C** во нејзината оригинална форма **M** се вика **функција за дешифрирање** и се означува со **D** (анг. decryption function).
  - Оваа функција е инверзна на функцијата за шифрирање.

Основни поими во криптологија

- Постапката со која од некоја почетна состојба се доаѓа до решение на некој проблем се нарекува алгоритам.
  - Алгоритам за шифрирање на оригиналната порака (encryption algorithm).
  - Алгоритам за дешифрирање на шифрираната (decryption algorithm).

Основни поими во криптологија

- Во текот на извршување на функциите за шифрирање и дешифрирање, корисниците мора да имаат:
  - единствен таен клуч **К** (анг. key), доколку се работи за т.н. **симетрично шифрирање**
  - два различни клуча: еден јавен клуч $\mathbf{K_1}$, и друг таен (или приватен) клуч $\mathbf{K_2}$, доколку се работи за т.н **асиметрично шифрирање**.

Основни поими во криптологија

- Успешноста на шифрирањето зависи од јачината на алгоритмот, но често и од должината на клучот.
  - Подолгите клучеви обезбедуваат поголема безбедност, бидејќи на напаѓачот ќе му треба многу повеќе време да ги испита сите можни комбинации на клучеви за да го открие вистинскиот.
  - Од друга страна, за побрза комуникација, се бара клучевите да бидат што е можно покуси.

Историски примери

Пример (Цезарова шифра)

- Шифрирање
- Нека оригиналната порака е

  M = „Prezakazan sostanok na drzaven vrv“.
- Нека за функција **E** го користиме познатато Цезарово шифрирање:
  - секоја буква од оригиналната порака да се замени циклично со третата следна буква од абецедата.

Пример (Цезарова шифра)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Табела 1. Цезарово шифрирање

- Во табелата првиот ред ја претставува оригиналната буква, а вториот ред шифрираната буква.
- Ако се занемарат празните места, шифрираната порака би била

  C = „Suhcdndcdqvrvwdqrnqdgucdyhyuy“.

Пример (Цезарова шифра)

- Дешифрирање
- Да ја искористиме шифрираната порака **C** = „Suhcdndcdqvrvwdqrnqdgucdyhyuy“.
- За функција за дешифрирање треба да го земеме Цезаровото дешифрирање:
  - секоја буква од шифрираната порака да се замени циклично со третата претходна буква од абецедата.

Пример (Цезарова шифра)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Табела 2. Цезарово дешифрирање

- Во табелата првиот ред ја претставува шифрираната буква, а вториот ред дешифрираната буква.
- Тогаш оригиналната порака (повторно со занемарени празни места) би била

  M= „Prezakazansostanoknadrzavenvrv“.

Пример (Цезарова шифра)

- Разбивањето на Цезаровата шифра е многу лесно.
  - Тоа може да се направи со испитување на сите можни поместувања.
- **Пример.** Да се дешифрира пораката TGVGJTKZK, ако се знае дека станува збор за Цезаровата шифра.

Пример (Цезарова шифра)

- Не се знае колку Цезаровата шифра била безбедна во тоа време.
  - Веројатно е дека била многу безбедна, зашто многу од цезаровите непријатели не биле писмени, а оние што биле, не ни помислувале дека станува збор за шифра.
- Цезаровата шифра, како и некои други шифри коишто се појавиле подоцна, биле разбиени дури во 9 век, за време на златното доба на арапската цивилизација.

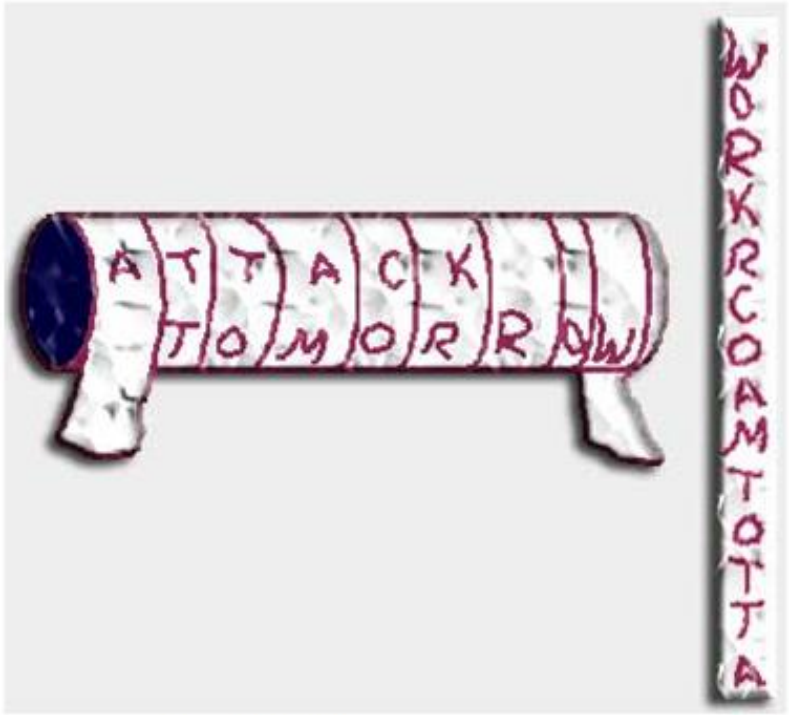
Историја на криптологијата

- Најстариот познат текст кој содржи една од основните елементи на криптографијата - намерна модификација на текст, потекнува од пред 4000 години
  - хиероглифски запис на гробот на благородникот KHNUMHOTEP II.
  - имала цел да го импресионира читателот.
- Кај подоцнежните записи се среќава и вториот елемент на криптографијата – тајноста
  - најчесто со цел да се зголеми мистеријата
  - да се прикаже магичната моќ на некои религиозни текстови.

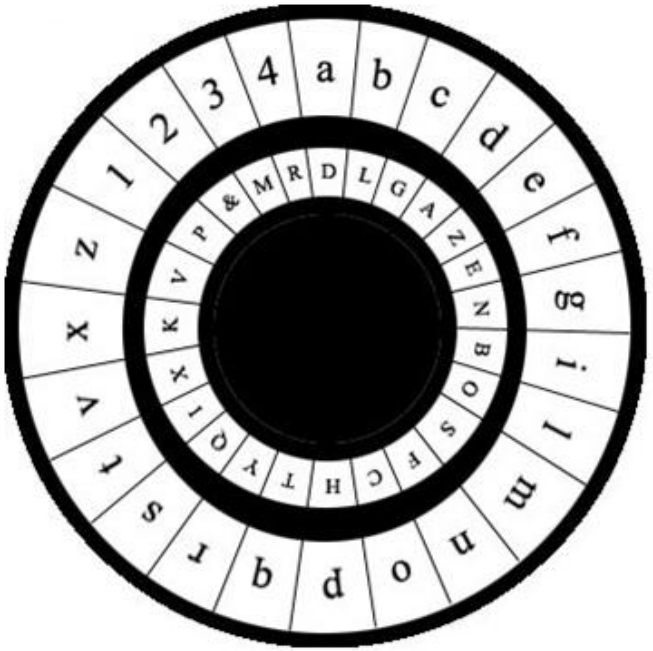
Историја на криптологијата

- Литературата била достапна само на мал број луѓе, па поради ова не постои појава на криптографија.
- Постоеле само некои облици на ***стеганографија***,
  - умешност на криење на пораката, така да никој не знае за нејзиното постоење
- Кај криптографијата тајна е содржината на пораката, а не нејзиното постоење.

Историја на криптологијата



Слика 1. **SCYTALE**



Слика1 Дискот на *Alberti*

Симетрична криптографија

Криптографија со таен клуч

- вклучува користење на таен клуч познат само за учесниците во тајната комуникација
- генерално брзи и погодни за обработка на голем проток на податоци,
- ранливи се.
- вообичаено се мешаат со алгоритми со јавни клучеви за да се добие добра комбинација од сигурност и брзина.

Основни поими

- Се делат на две категории и тоа:
  - проточни шифрувачи (*stream cipher*)
  - блоковски шифрувачи (*block cipher*)

Проточни шифрувачи

- Оригиналниот текст се криптира еднаш и притоа се врши трансформација на секој влезен бит или бајт
- Проточните алгоритми се конструирани врз принципот на единствениот теоретски докажан криптосистем кој не може да се разбие, а тоа е *One-time-pad*.
- Овие алгоритми користат клуч со големина од 128 бита и повеќе

One-time pad

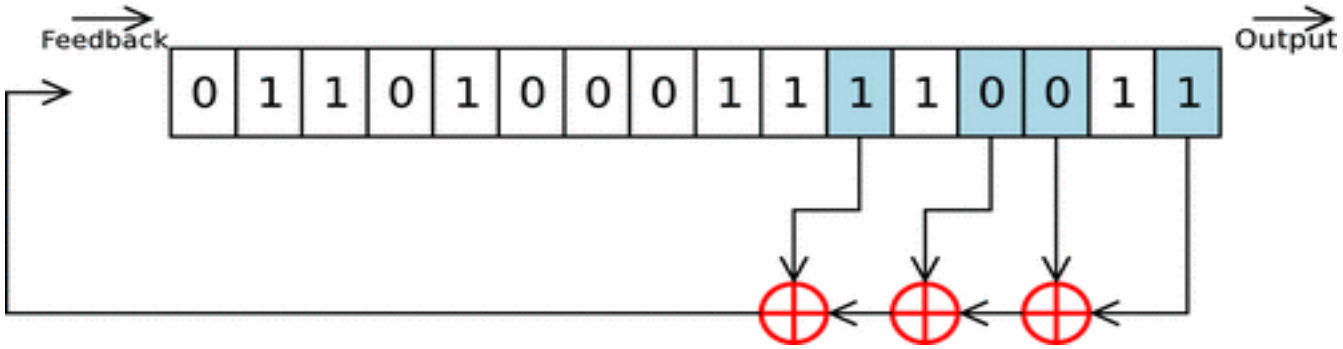
- M-оригиналната порака
  - бинарен стринг
- K-клучот
  - бинарен стринг со должина колку што е оригиналната порака
  - се користи само еднаш
- C=M⊕K - шифрираниот текст
  - шифрирање бит по бит
- M=C⊕K – оригиналната порака
  - добиена со дешифрирање

One-time pad

- Зошто клучот се користи само еднаш?
- Нека имаме две пораки M_1 и M_2
- Шифрираните пораки со ист клуч К се:
- $C_1=M_1 \oplus K$, $C_2=M_2 \oplus K$
- Недостаток:
- $C_1 \oplus C_2=M_1 \oplus K \oplus M_2 \oplus K=M_1 \oplus M_2$

Генератори на клучеви

LFSR *(Linear Feedback Shift Register)*

- Може лесно да се имплементира хардверски и анализира математички.
- 

LFSR

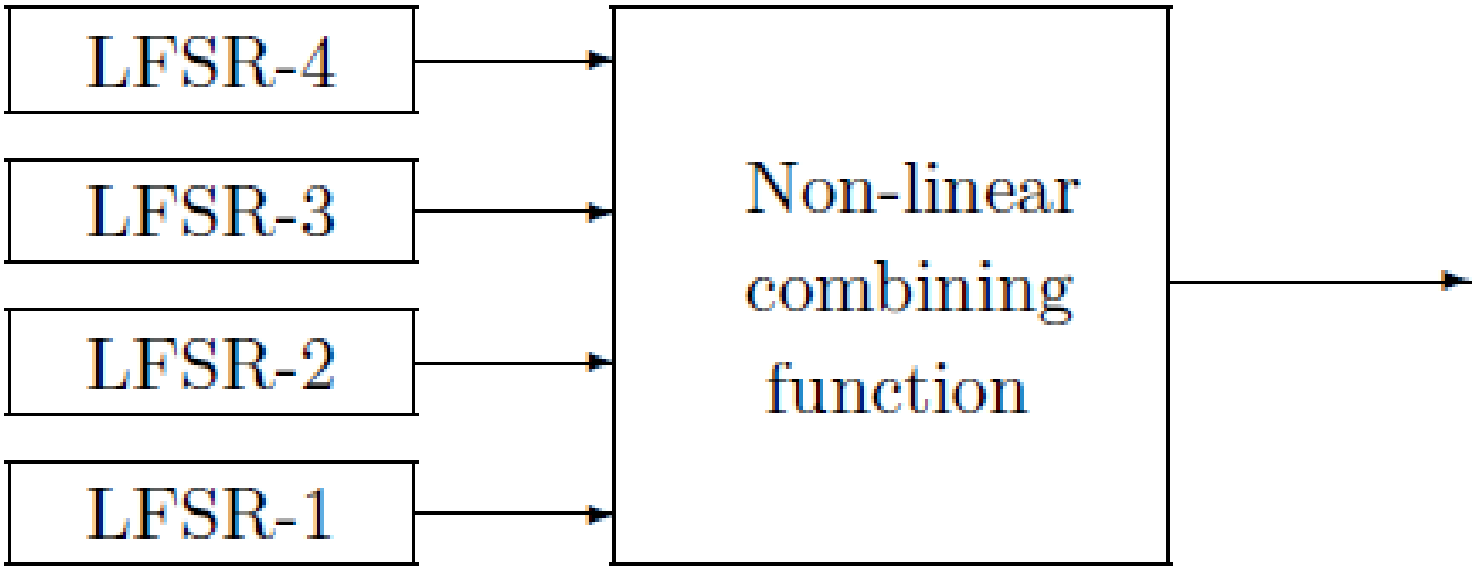
- Означеното предефинирано множество од келии може да се репрезентира како полином по модул 2 кој се нарекува карактеристичен x^{11} полином или *feedback* полином .
- На примерот множеството е {11,13,14,16} па тогаш *LFSR* полиномот е: $x^{11} + x^{13} + x^{14} + x^{16} + 1$.

LFSR

Нелинеарно комбинирање функции

- За да се подобри сигурноста на *LFSR* се оди кон нелинеарно комбинирање на функции.
- Еден начин е да се употребат паралелно *n* *LFSR* генератори и нивните излези да се комбинираат користејќи нелинеарна Булова функција *F* со *n* битни влеза, за да се добие комбинирачки генератор на псевдослучајни низи од битови.

LFSRs



*A*5/1

- *A*5/1
  - е широко употребуваниот симетричен, проточен алгоритам.
  - Се употребува во мобилните уреди за доверливост
  - Користи три LFSR X (19 бита), Y(22 бита), Z(23 бита) и 64 битен клуч К.
  - Лесен за имплементација во хардвер.
  - На почетокот проточните шифрувачи биле лидери во симетричната криптографија.
  - Денес таа улога ја имаат блок шифрувачите.

RC4

- *RC-4* (*ARC4* или *ARCFOUR*)
  - е најшироко употребуваниот симетричен, проточен алгоритам.
  - Се употребува во многу популарни протоколи како што се
    - *SSL* (*Secure Sockets Layer*) за да се заштити мрежниот сообраќај и
    - *WEP* (*Wireless Encoding Protocol*) за да се заштити бежичната мрежа.
  - Генерира псевдослучајни протоци од битови (проточен клуч)
  - Оптимизиран за софтверска имплементација.

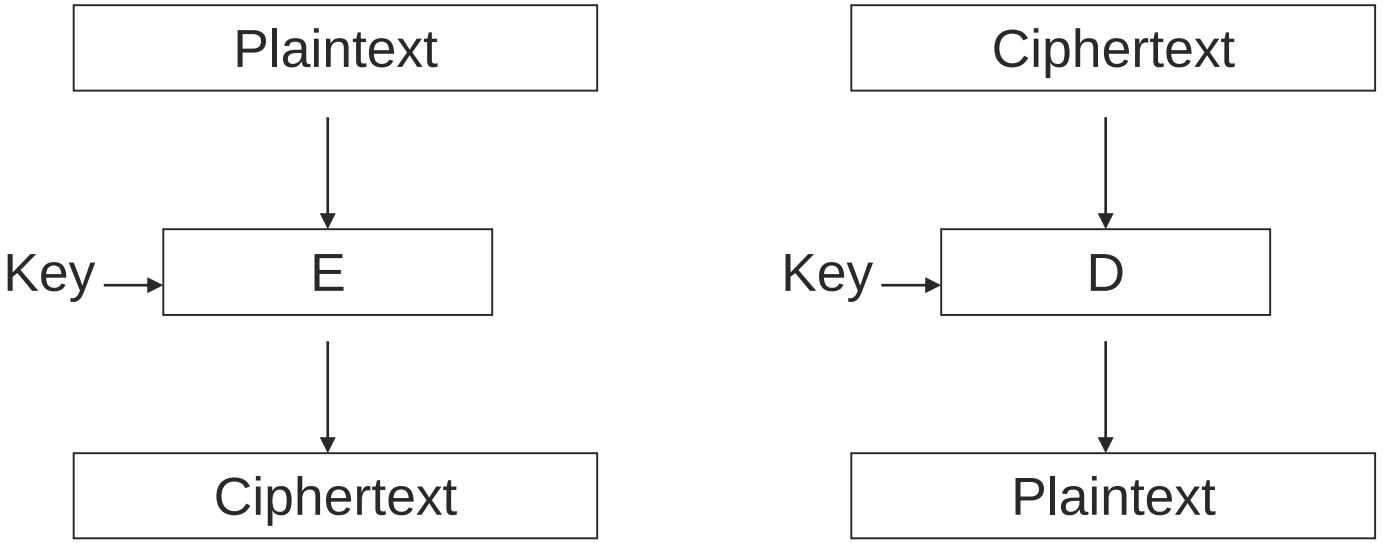
Искористенот на проточните алгоритми

- Безбедна безжична (*wireless*) комуникација.
- Во воената криптографија

Блоковски шифрувачи

- Трансформираат блок со фиксна големина од оригиналната порака во ист таков блок на шифрираната порака.
- Блоковите на кои се дели пораката обично се со големина:
  - 64, 128, 256, ... итн бита.
- Покрај стандардните постојат и итеративни блок шифрувачи (постапката на енкрипција на блок од оригиналната порака трае во повеќе циклуси).

Блоковски шифрувачи



DES

- Кратенка е од *Data Encryption Algorithm*
- Развиен е од страна на фирмата *IBM* со поддршка од *NBS* (*US National Bureau of Standards*)
- Публикуван е во 1977 година како *US FIPS* 46 стандард.
- Во дизајнирањето на овој алгоритам, се содржани два многу важни принципи:
  - конфузија и дифузија.
- Големината на блоковите е 64 бита или 8 бајти колку што е и големината на тајниот клуч за криптирање .

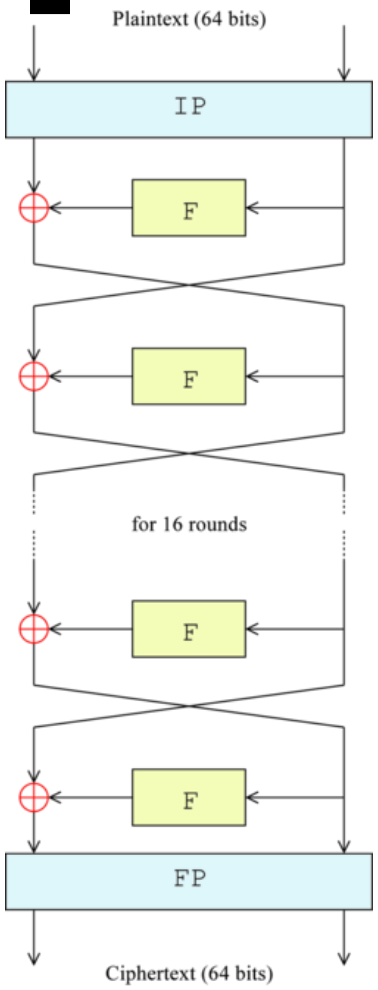
DES

- *DES* алгоритамот се состои од 16 рунди или циклуси, каде секој циклус е блок добиен со супституција и пермутација на текстот од оригиналната порака.
- Влезната порака се дели на блокови од по 64 бита и поминувајќи низ повеќе серии на комплексни операции дава шифриран текст со исто толкава големина.

DES

- *DES* алгоритамот е Феистелов шифрувач со 16 рунди
- Големината на блокот е 64
- Користи 56 битен клуч
- Секоја рунда користи 48 битен подклуч (земени од 56 битниот клуч)

DES

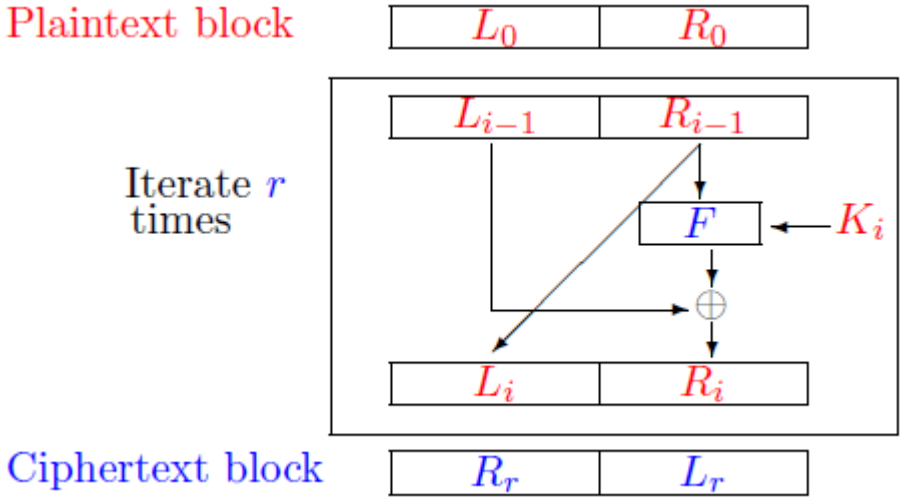


- Чекор 1. блокот од 64-бита се дели на два дела по 32-бита
- Чекор 2. на десниот дел се применува *Feistel* - ова функција
- Чекор 3. на излезот од чекор 2 и левиот дел се применува *XOR*
- Како влезови во наредниот циклус се : излезот од чекор 3 и десниот 32-битен дел само што сега местата им се заменати.

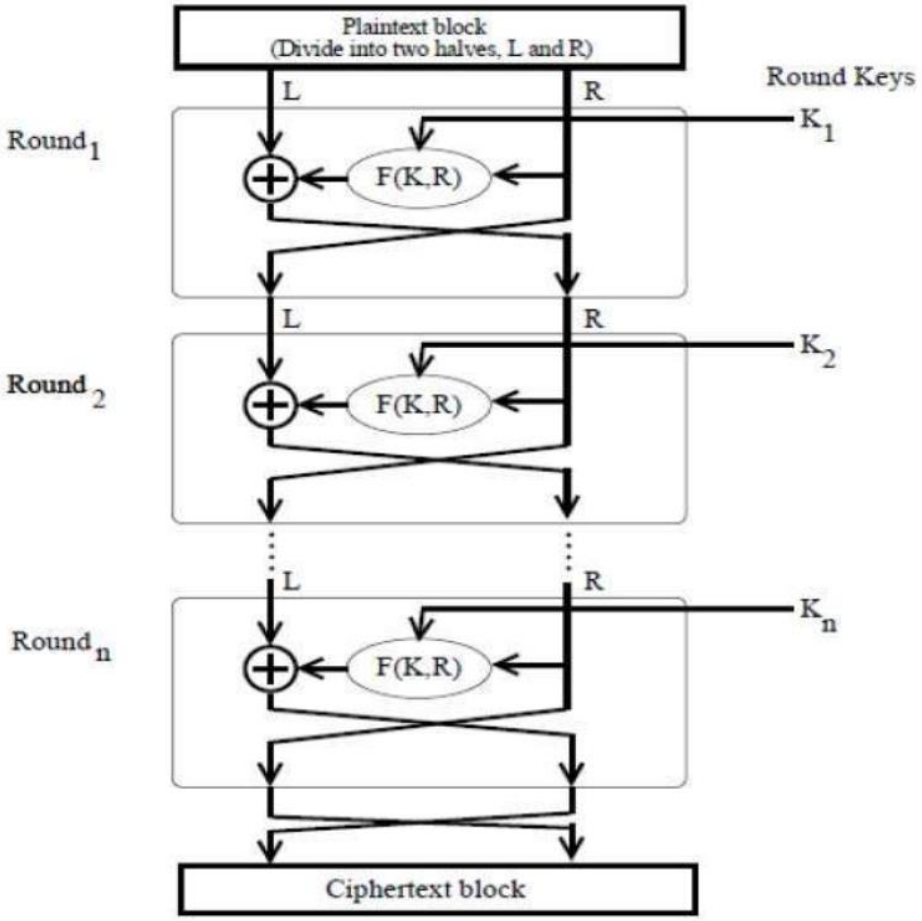
DES

- *Feistel* – оваа функција се состои од четири дела и тоа:
  - проширување,
  - мешање на битови,
  - субституција и
  - пермутација.

Феистелов шифрувач

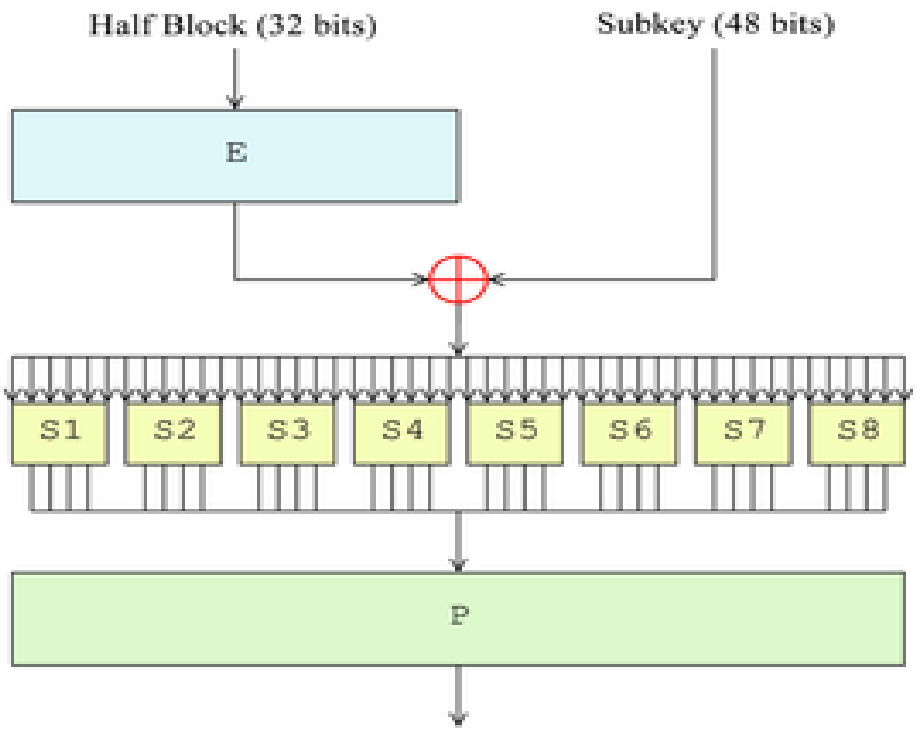


Феистелов шифрувач

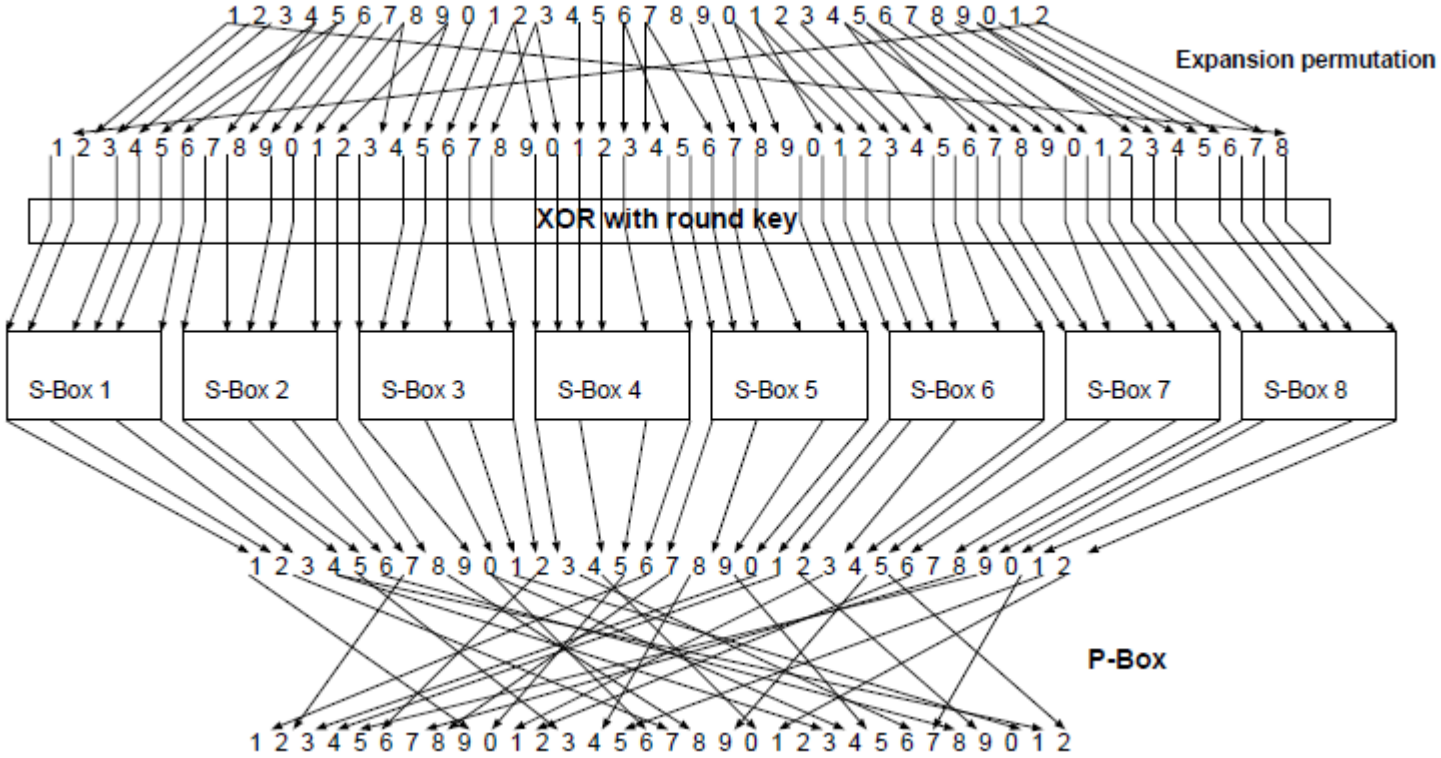


$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus \mathrm{F}(R_i, K_i).$$

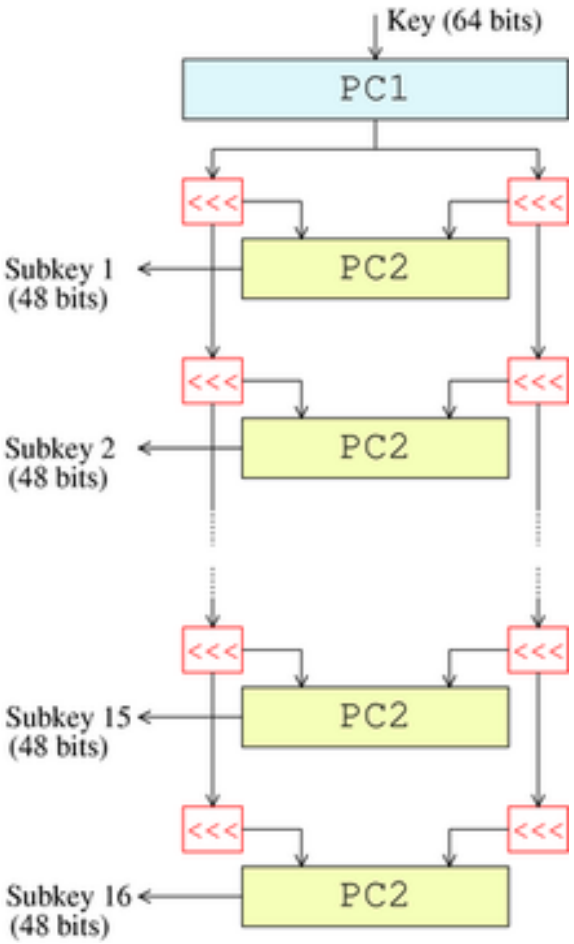
DES



Структура на DES функцијата F



DES



- Подклучевите се добиваат од главниот клуч со користење на алгоритамот за распределба на клучеви (*key schedule*)

AES

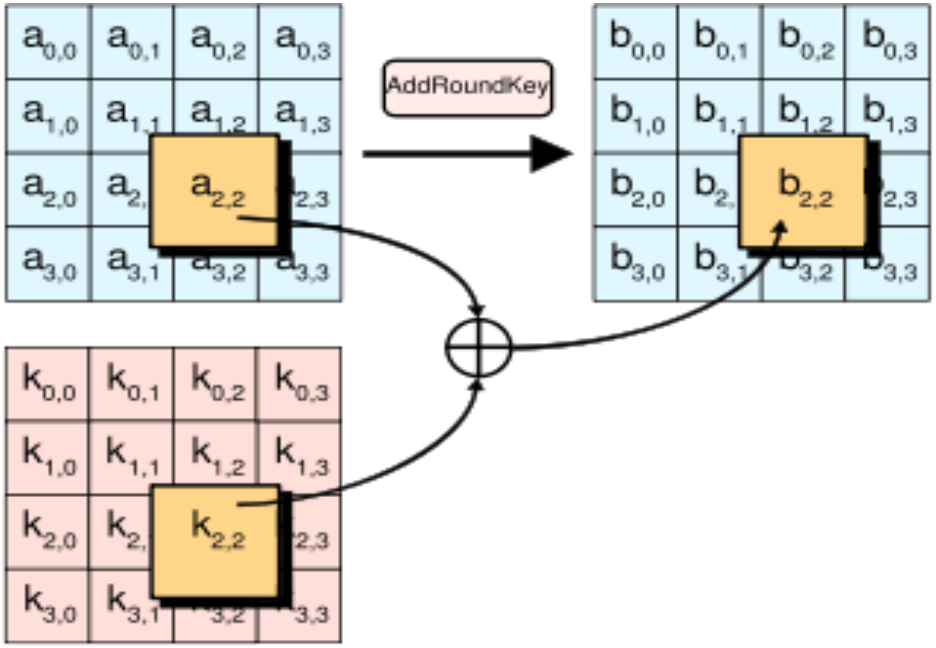
- *Advanced Encryption Standard -RijnDael*
- Се користат 3 големини на блокот: 128, 192 или 256 бита
- Се користат 3 големини за должина на клучот: 128, 192 или 256 бита
- Бројот на рунди е 10 до 14 во зависност од должината на клучот
- Секоја рунда се состои од 4 функции

AES

- *Advanced Encryption Standard -RijnDael*
- *AES* оперира над поле од 4x4 бајти, наречено матрица на состојба.
- За енкрипција секоја рунда на *AES* со исклучок на последната се состои од четири дела и тоа:
  - *AddRoundKey*
  - *SubBytes*
  - *ShiftRows*
  - *MixColumns*

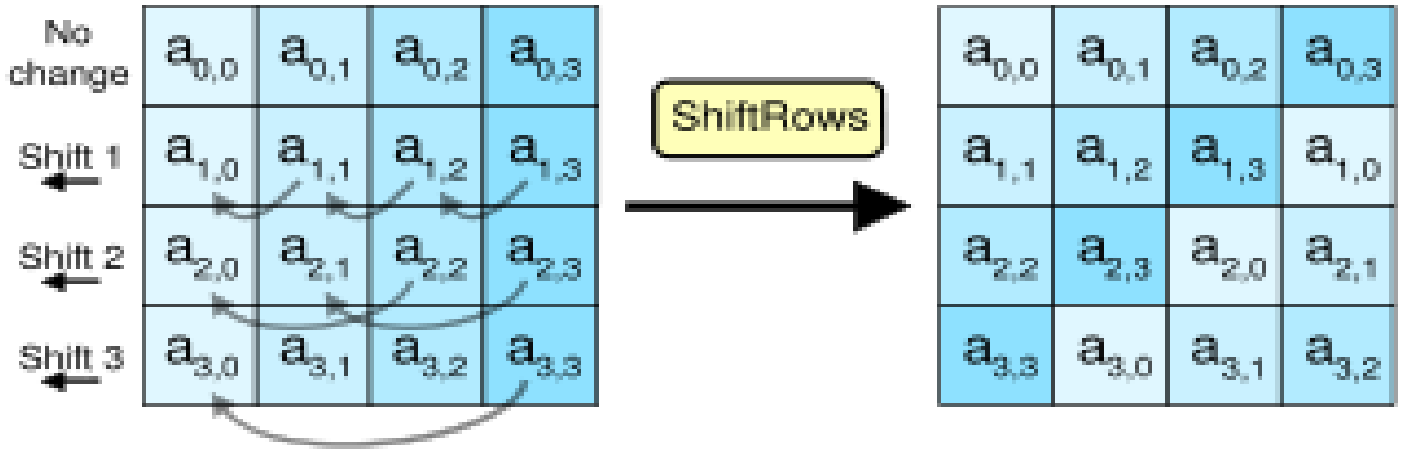
AES

- *AddRoundKey*



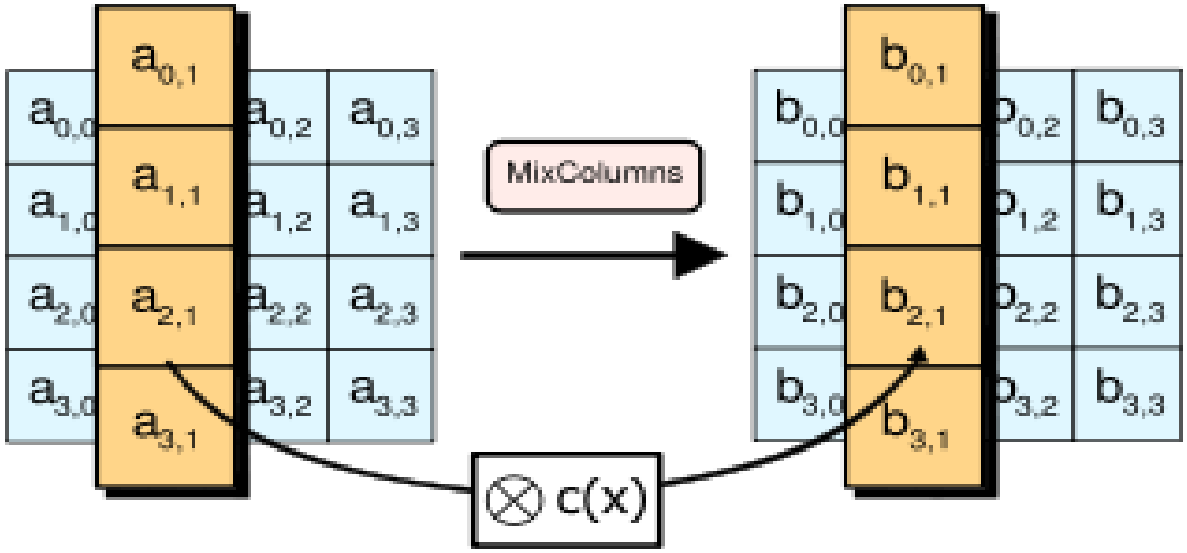
AES

- *SubBytes*
- *ShiftRows*



AES

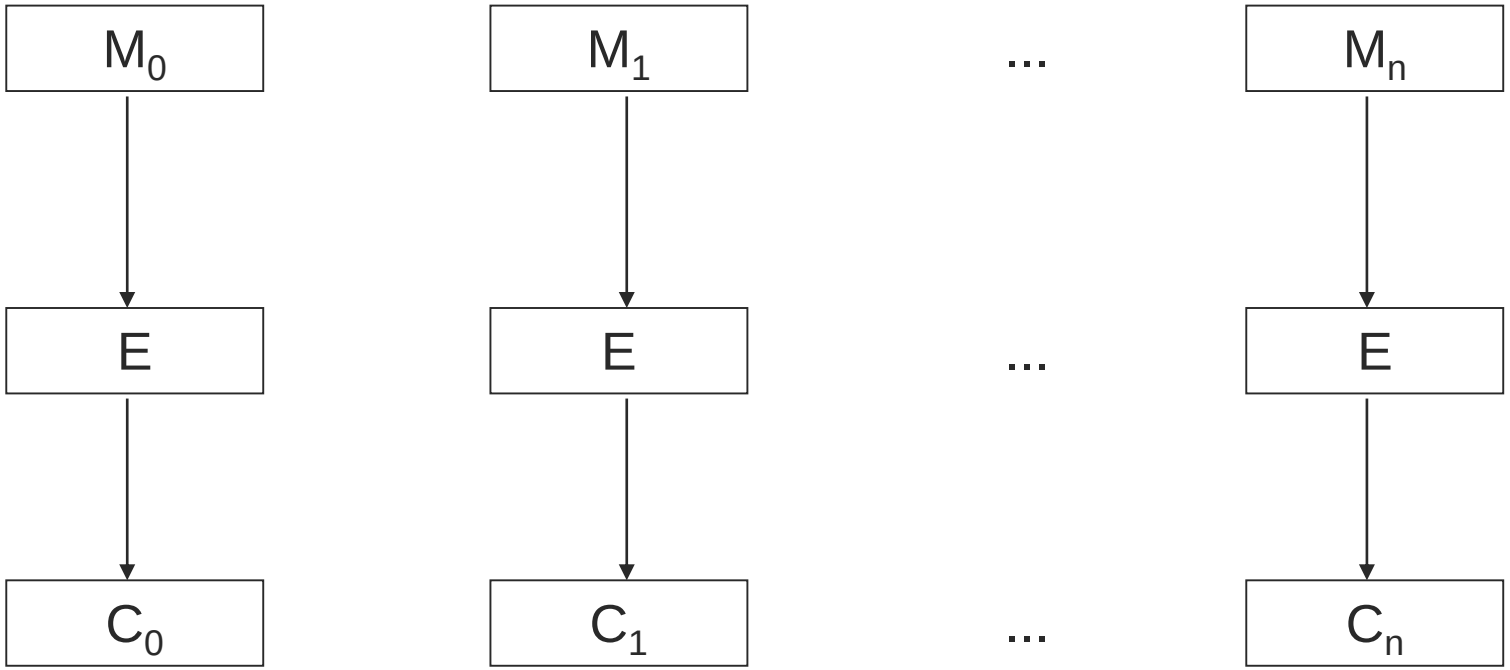
- *MixColumns*



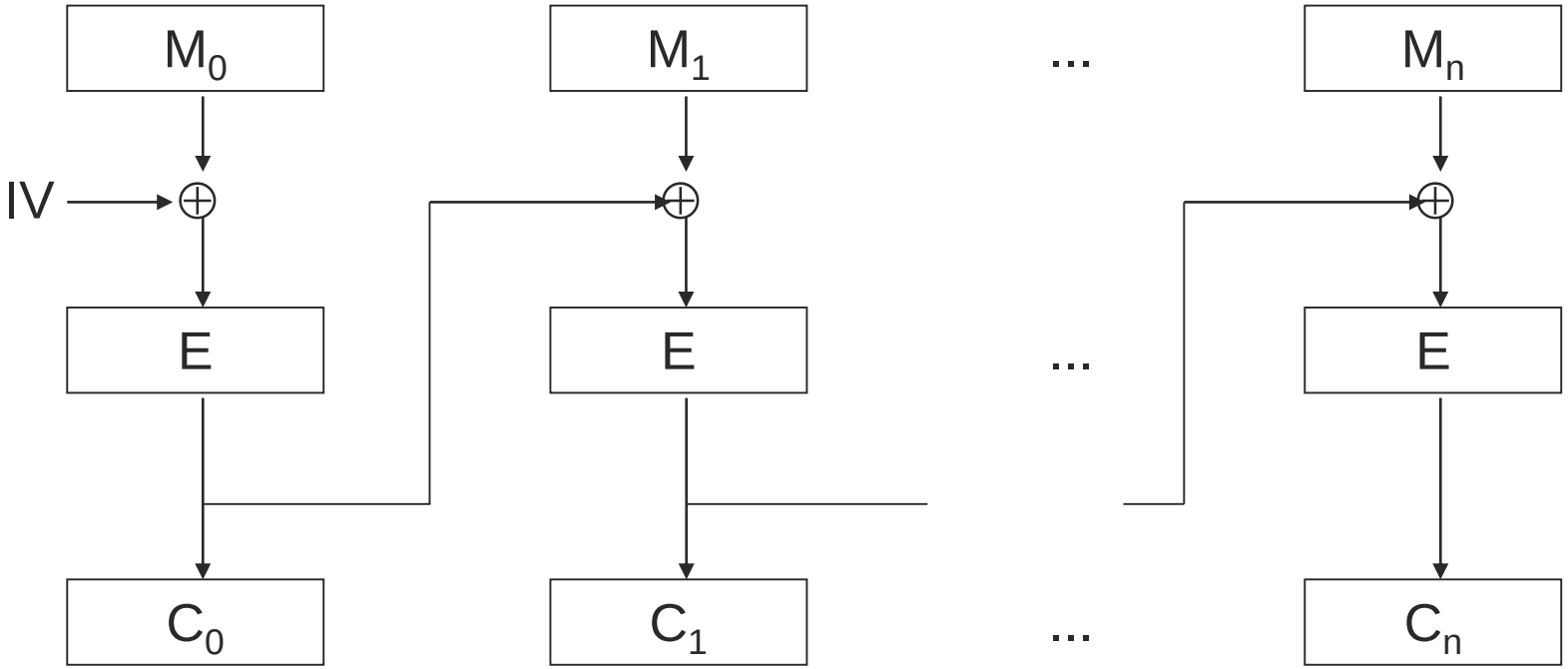
Модови на работа

- Постојат неколку модови на работа:
  - *ECB - Electronic Code Book*
  - *CBC - Cipher Block Chaining*
  - OFB - *Output FeedBack*
  - CFB - *Cipher FeedBack*

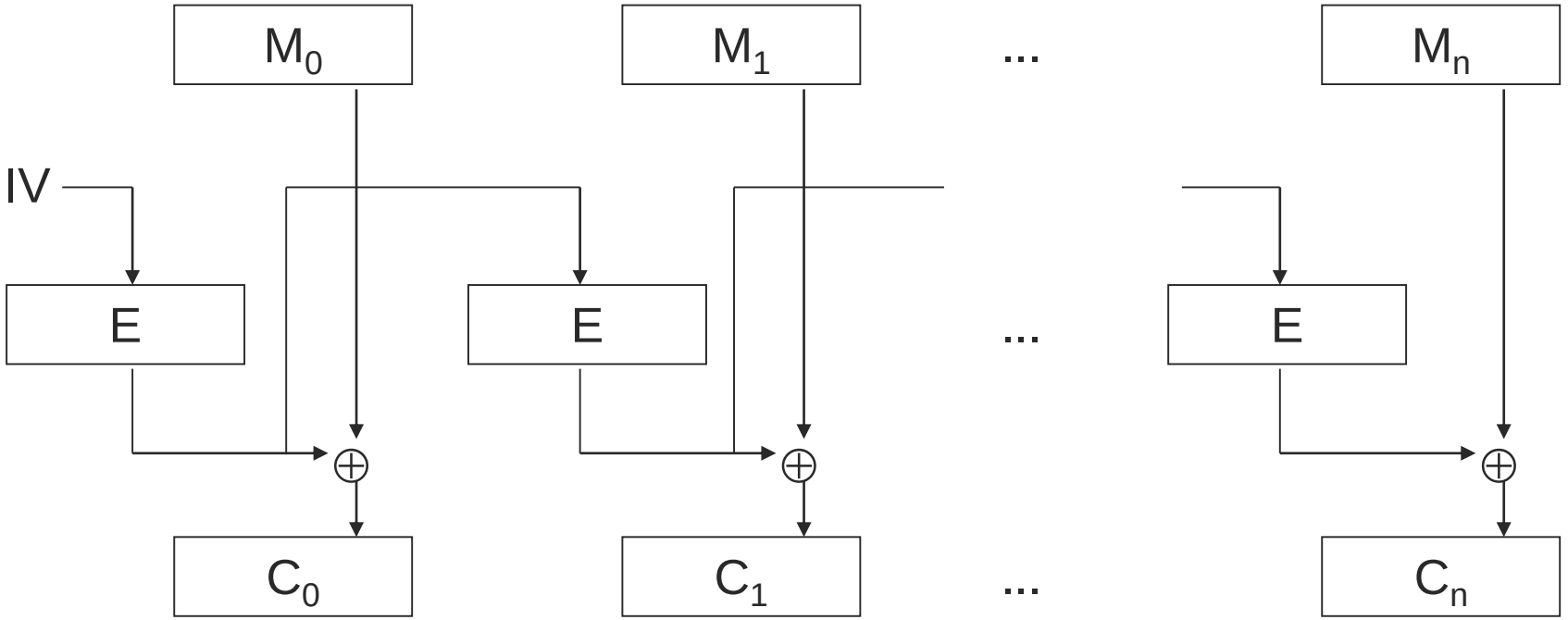
ECB – Electronic Code Book



CBC – Cipher Block Chaining



OFB – Output FeedBack



CFB – Cipher FeedBack