Блок крипто-системи - Фистелова архитектура - ДЕС

Владимир Божовић

Одсјек за математику
Природно-математички факултет

КРИПТОГРАФИЈА

Подсјећање

Као што већ знамо, симетрична криптографија се заснива на сценарију у ком Алиса и Боб имају **заједнички кључ** којим врше енкрипцију и декрипцију порука.

Већ смо се сусрели са једним бројем симетричних крипто-система као:

а. Цезаров крипто-систем.
б. Општи суспституциони крипто-систем.
в. Афини крипто-систем.
г. Виженеров крипто-систем.

Док су прва три **моноалфабетски**, четврти је **полиалфабетски** крипто-систем.

Класификација симетричних крипто-система

Сви практични криптосистеми врше енкрипцију дио по дио. Тај дио може бити један или блок битова. Енкрипција је функција која у општем случају зависи од:

1. Редног броја блока у низу блокова над којим се врши енкрипција.
2. Тајног кључа.
3. Интерног стања уређаја који врши енкрипцију.

Основна подјела симетричних крипто-система је на:

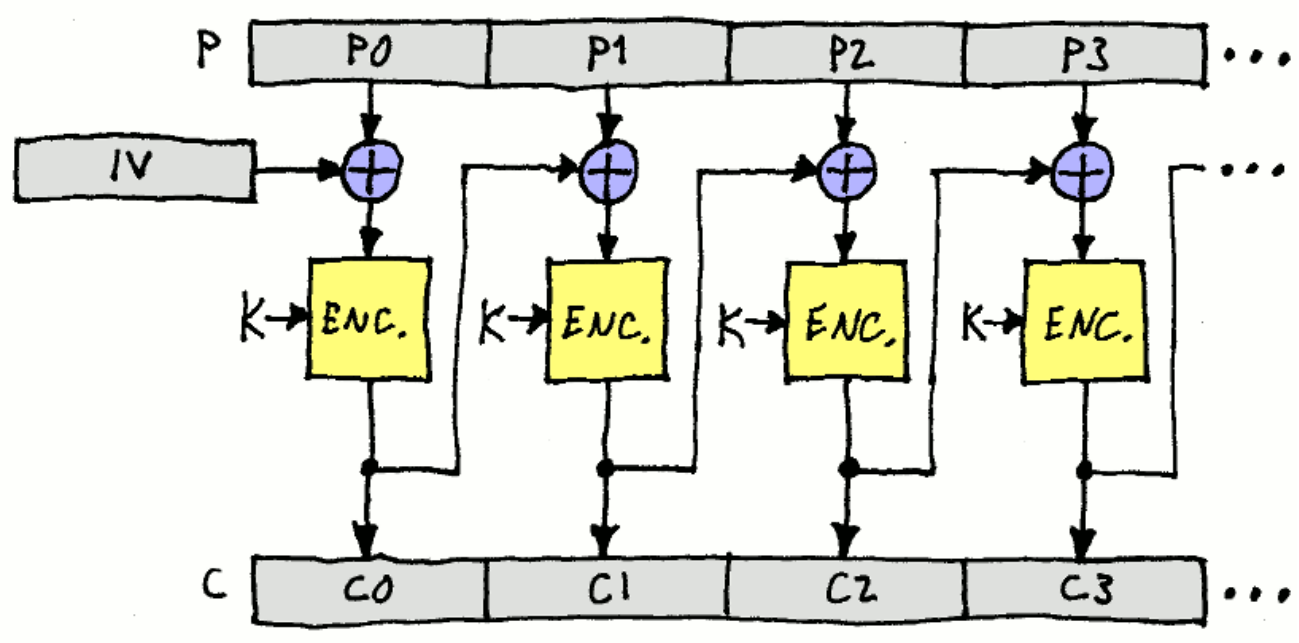
Блок крипто-системе.

Не зависе од интерног стања енкриптора.

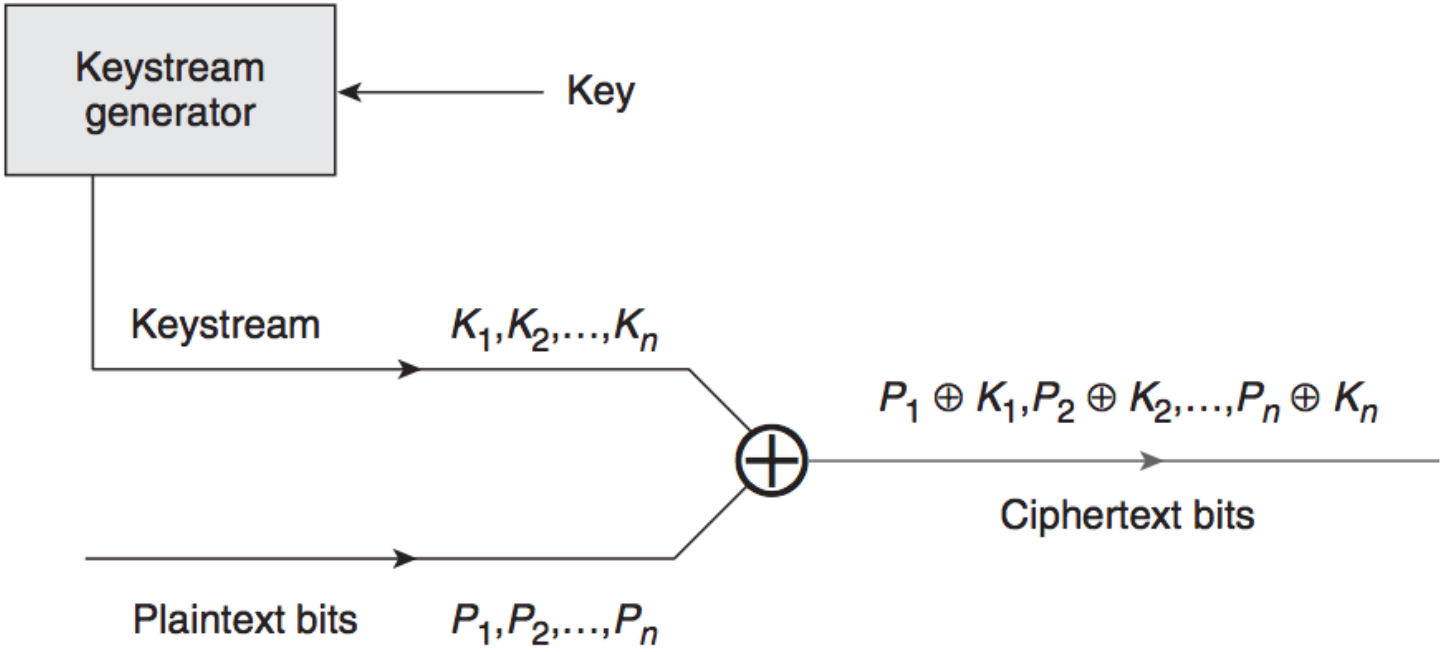
Низ крипто-системе.

Ззависе од интерног стања енкриптора.

Примјер: блок крипто-систем



Примјер: низ крипто-систем



Преглед основних информација

- 1972. године, појавио се револуционаран конкурс од стране NBS-а, садашњег NIST-а за прављење крипто-система који би се користио као стандард у различитим апликацијама.
- NBS је 1974 одабрао крипто-систем направљен од стране тима криптопграфа из IBM-а. Алгоритам који је предложен од стране IBM-а је био заснован на крипто-систему **Луцифер**.
- Луцифер припада типу Фистеловог (Feistel) крипто-система, који врши енкрипцију блокова величине 64 бита помоћу кључа који садржи 128 бита.

Преглед основних информација

- То је почетак јавне употребе криптографског стандарда, **Data Encryption Standard** (DES).
- **DES** је сигурно најпопуларнији блок крипто-систем у последњих 30 година.
- Иако се више не сматра сигурним, још увијек се може наћи у употреби. Принципи и дизајн у DES-у су инспирисали развој многих модерних крипто-система.
- Данас постоје унапријеђене верзије овог система као што су AES, односно 3DES, који су веома заступљени.

Преглед основних информација

- Упркос критици и забринутости, NIST је 1977. објелоданио све спецификације модификованог IBM крипто-система.
- Иако је комплетан систем објашњен до последњег детаља, дизајнерски критеријуми, односно мотивација није никад дата у званичној форми.
- Због раширености употребе и добрих перформанси, NIST је модификовану верзију користио све до 1999. године, када је успостављен Advanced Encryption Standard (AES).

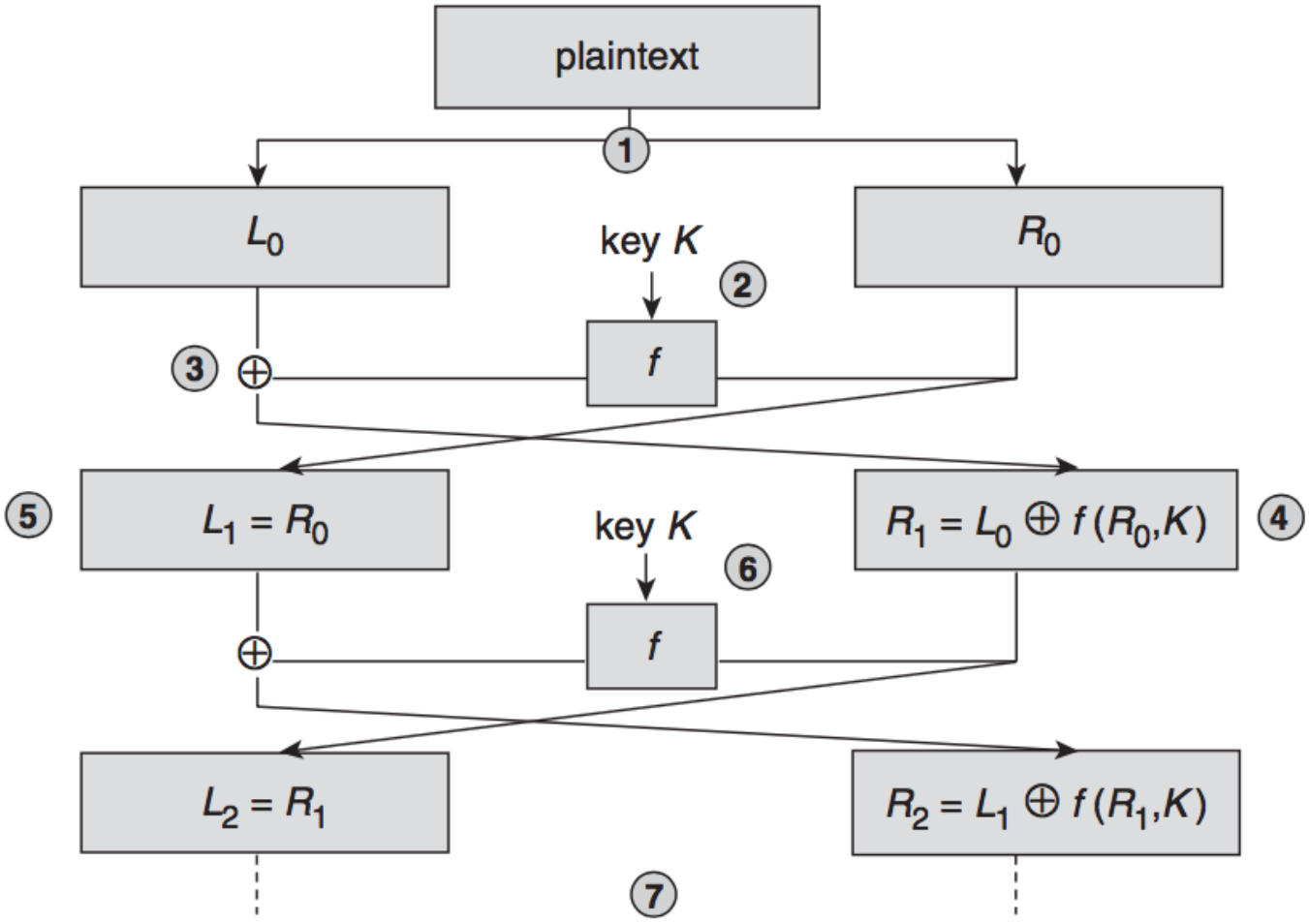
Фистел крипто-систем

Фистел (Feistel) је тип блок крипто-система. Наводимо неке његове основне особине

- Користи се алфабетом $\mathbb{Z}_2 = 0, 1$.
- Дужина блока је $2t$ за неко $t \in \mathbb{N}$.
- Енкипција се врши у $r \in \mathbb{N}$ етапа.
- За сваки кључ, формира се r **етапних кључева** $k_1, \ldots, k_r$ који се генеришу и користе редом током одвијања алгоритма.

Водећи представник Фистел крипто-система је DES.

ДЕС - илустрација Фистеловог система



Архитектура Фистел крипто-система

Процес енкрипције у Фистеловом крипто-систему почиње тако што се блок основне поруке m подијели на два дијела, сваки по t битова.

Општи алгоритам

1. Нека је L_0 лијева, а R_0 десна половина, односно $m = (L_0, R_0)$.
2. Низ парова (L_i, R_i) за $i = 1, \ldots, r$ се даље, рекурзивно, дефинише као

$$(L_i, R_i) = (R_{i-1}, L_{i-1} \oplus f_{k_i}(R_{i-1}))$$

гдје је f_{k_i} одређена функција, зависна од кључа k_i у етапи i, за $i = 1, \ldots, r$.

Декрипција у Фистеловом крипто-систему

Укратко, енкрипцију у Фистеловом крипто-систему можемо описати као

$$E_k(m) = E_k(L_0, R_0) = (L_r, R_r).$$

Такође, примјетимо да из

$$\begin{aligned} (L_i, R_i) &= (R_{i-1}, L_{i-1} \oplus f_{k_i}(R_{i-1})), \text{ слиједи} \\ (L_i, R_i \oplus f_{k_i}(R_{i-1})) &= (R_{i-1}, L_{i-1}) \end{aligned}$$

а пошто је $L_i = R_{i-1}$ онда

$$\begin{aligned} (L_i, R_i \oplus f_{k_i}(L_i)) &= (R_{i-1}, L_{i-1}), \text{ односно,} \\ (L_{i-1}, R_{i-1}) &= (R_i \oplus f_{k_i}(L_i), L_i). \end{aligned}$$

Декрипција у Фистеловом крипто-систему

- Полазећи од

$$(L_{i-1}, R_{i-1}) = (R_i \oplus f_{k_i}(L_i), L_i),$$

  $i = r, \ldots, 1$, видимо да је процес декрипције у суштини исти као и енкрипција, само што треба обрнути редослед етапа.
- Ова чињеница чини Фистелов крипто-систем веома погодним за имплементацију, како у софтверу, тако и у хардверу.

Детаљи DES крипто-система

- DES је типичан представник Фистеловог крипто-система са $t = 32$ и $r = 16$.
- Кључ DES крипто-система је дужине 64 бита, уз обавезу да последњи бит сваког бајта представља такозвани бит парности.

$$\mathcal{K} = \{(k_1, \ldots, k_{64}) \in \{0,1\}^{64}\}, \text{ уз услов да}$$

$$\sum_{i=1}^{8} k_{8j+i} \equiv 1 \pmod 2 \text{ за } j = 0, \ldots, 7.$$

- На тај начин, дужина DES кључа је заправо 56, чиме је величина домена кључа 2^{56}.

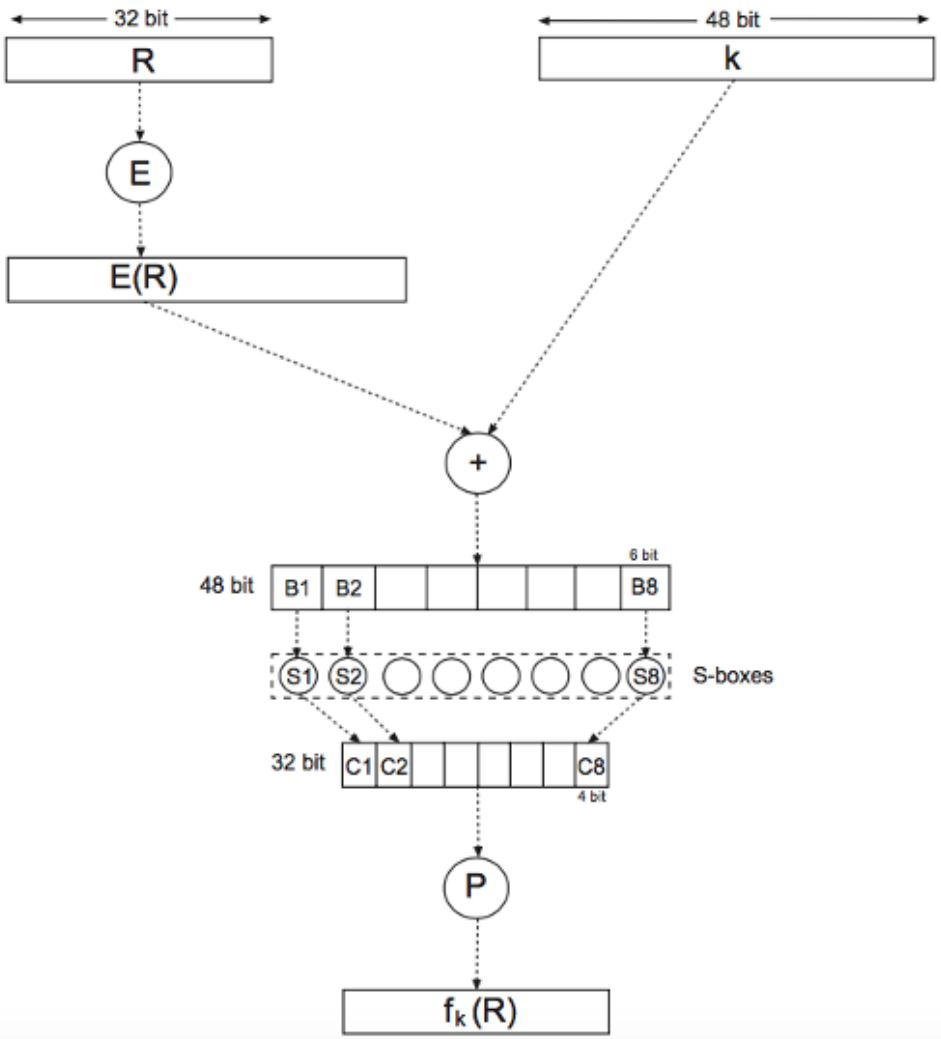
Детаљи ДЕС алгоритма

- Као што смо видјели, базично рачунање у свакој етапи Фистеловог крипто-система, а и ДЕС-а је

$$(L_i, R_i) = (R_{i-1}, L_{i-1} \oplus f_{k_i}(R_{i-1})).$$

- Дакле, једина непознаница је начин како се у појединим корацима (етапама) генеришу кључеви k_i из почетног кључа k, као и детаљи функције f_{k_i}.
- Начином генерисања "етапних" кључева k_i се нећемо бавити детаљније.
- Функцију f_{k_i} обично идентификујемо као С-кутије, које представљају срце ДЕС-а.

С-кутије "изнутра"



С-кутије "изнутра"

- Најприје, изводимо такозвану експанзиону обраду десне половине, односно R,

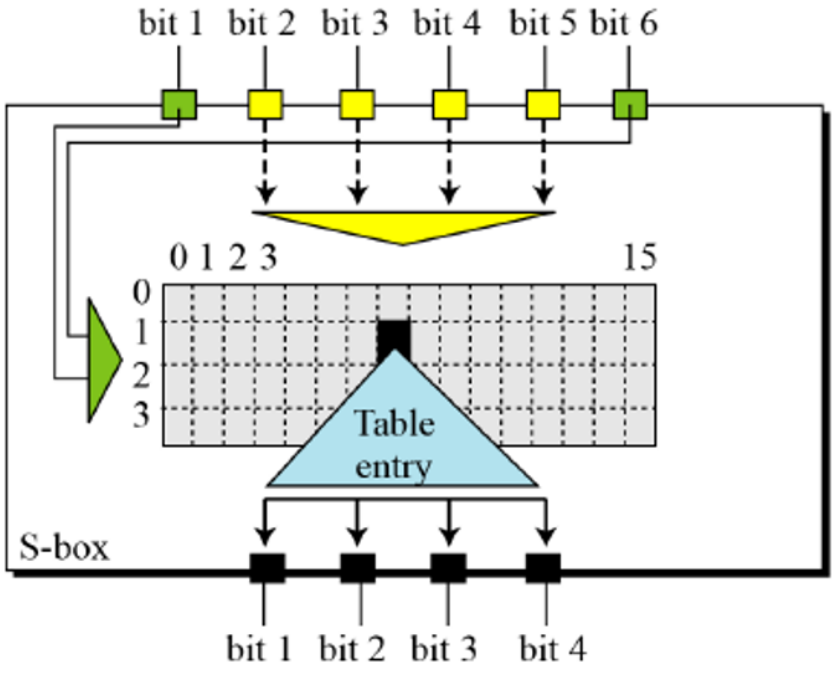
$$R = r_1 r_2 \ldots r_{32} \rightarrow E(R) = \underbrace{r_{32} r_1 r_{32} r_1 \ldots r_{32} r_1}_{\text{48 бита}}$$

- Након што добијемо резултат $E(R)$, врши се сабирање са етапним кључевима k_i (који се добијају по посебном алгоритму),

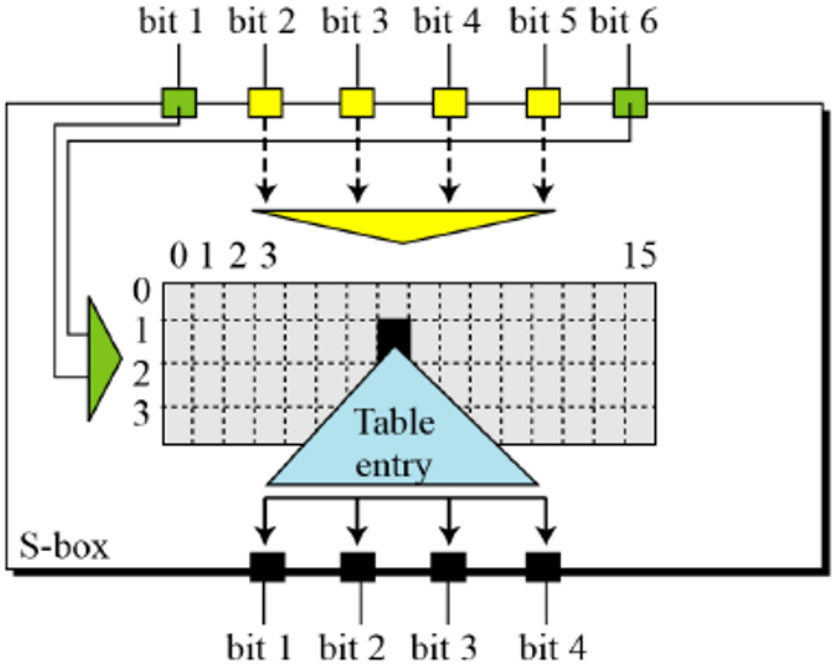
$$E(R) \oplus k_i = B_1 B_2 \ldots B_8,$$

гдје су B_i блокови по 6 бита.

- Потом се битови $B_i = b_1 b_2 b_3 b_4 b_5 b_6$ групишу у два блока $b_1 b_6$ и $b_2 b_3 b_4 b_5$ који представљају бројеве између 0 и 3, односно 0 и 15 респективно.
- Та два броја се користе као координате врсте и колоне за табелу $S-$ кутијама, као на слици



С-кутије "изнутра"

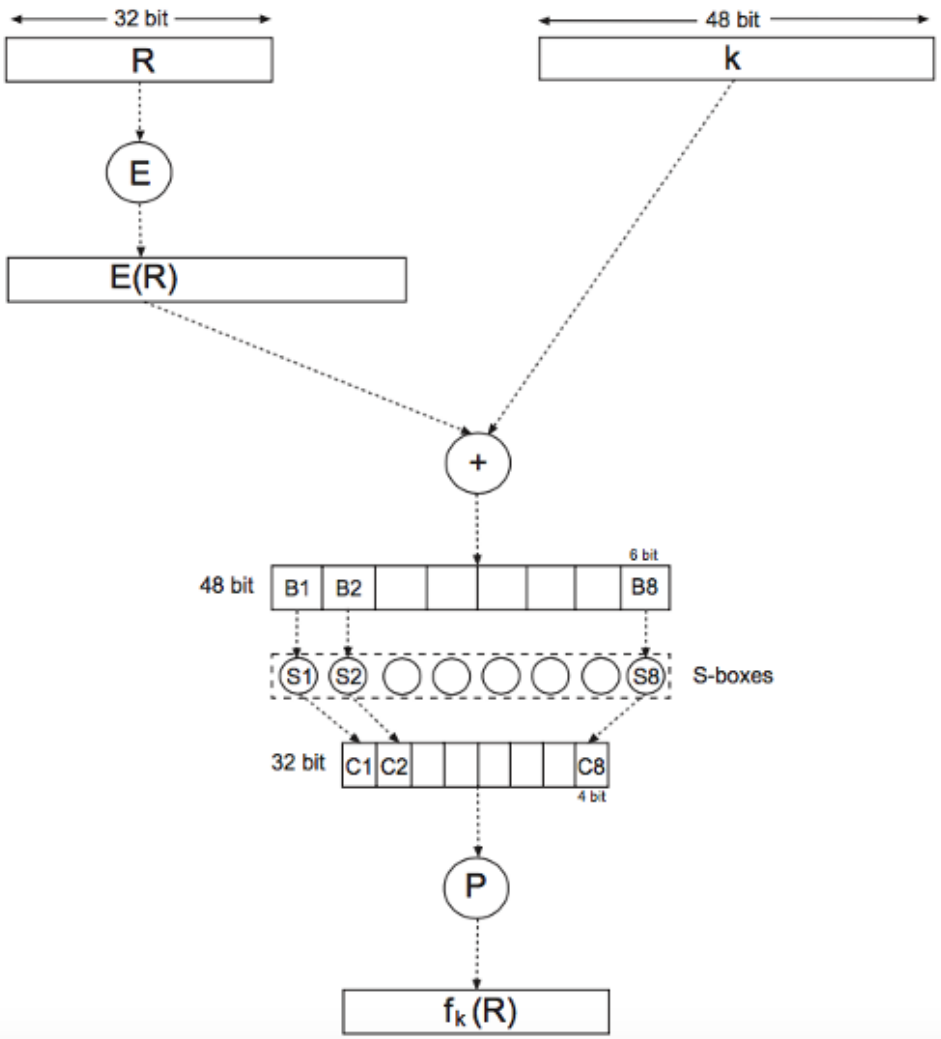


У "ћелијама" ове $S-$кутије се налазе 4-битни садржаји, па имамо

$$S(B_i) = C_i, \ \ i = 1, \ldots, 8.$$

Тиме добијамо низ од 32 бита $C = C_1 \ldots C_8$.

С-кутије "изнутра"



DES алгоритам - поглед из даљине

DES алгоритам се обавља у три корака

1. Улазна порука m се мијења иницијалном пермутацијом IP, чиме добијамо $m_1 = IP(m)$.
2. Потом се порука m_1 трансформише у 16 етапа Фистеловог крипто-система, чиме се на излазу добија (L_{16}, R_{16}).
3. Ако је излаз из претходног корака (L_{16}, R_{16}), онда се примјењује IP^{-1} на следећи начин

$$c = IP^{-1}(R_{16}, L_{16}).$$

ДЕС алгоритам

Улаз: (m, k)

$m \leftarrow IP(m)$

$L_0 =$ лијева половина поруке (32 бита)

$R_0 =$ десна половина поруке (32 бита)

for i=1 to 16 do

$$L_i \leftarrow R_{i-1}$$
$$R_i \leftarrow L_{i-1} \oplus f_{k_i}(R_{i-1})$$

$c \leftarrow IP^{-1}(R_{16}, L_{16})$

Излаз: c

Криптоанализа DES-а

Са практичног становишта, највећи проблем DES-а је мала дужина кључа, односно величина домена кључа. Постоји неколико теоријских и практичних резултата који се тичу крипто-анализе DES-а од којих издвајамо

- Michael J. Wiener је предложио хардверски дизајн 1993. године која би коштала $1,000,000$ US$ и била способна да нађе DES кључ за 3.5 сата у просјеку.
- Тек 1998. године је направљен специјализован хардверски систем за криптоанализу DES-а, назван **Deep Crack**, направљен од Electronic Frontier Foundation (EFF)

Криптоанализа DES-а

- Deep Crack је коштао 200,000 US$ и састојао се од 1,536 процесора, од којих је сваки био у стању провјере 60 милиона кључева у секунди.
- Међутим, да специјализован хардвер није неопхподан показао је пројекат на мрежи **distributed.net**, у јануару 1999.
- Заједничким напором више од 100,000 компјутера, успјели су да разбију DES кључ за само 23 сата. У том процесу, више од 250 милијарди кључева је провјеравано сваке секунде.

Више о DES крипто-систему можете пронаћи на интернету, као и у књизи ***Understanding Cryptography*** која се налази међу материјалима (Поглавље 3, стране 55-77).

Још о блок крипто-системима

Постоји неколико различитих модалитета енкрипције који се користе у блок крипто-системима. Наводимо најзаступљеније типове

- Electronic Code Book mode (ECB)
- Cipher Block Chaining mode (CBC)
- Output Feedback mode (OFB)
- Cipher Feedback mode (CFB)

Још о блок крипто-системима

Electronic Code Book mode (ECB)

- Дијелимо поруку на блокове дужине b бита и потом се врши редом, блок по блок, енкрипција.
- Једна од предности је то што јке могуће извршити енкрипцију блока $i+1$ чак и ако се не прими блок i, односно ако се прими погрешно.
- Коришћење истог кључа за различите блокова увећава вјероватноћу напада.
- Ако постоји "хедер" који се увијек шаље на почетку неког типа поруке, онда он увијек резултира истим криптограмом, па нападач увијек зна кад долази та одређена порука.

Још о блок крипто-системима

Супституциони напад на ЕСВ

Банка А пошиљалац	Рачун пошиљаоца	Банка Б прималац	Рачун примаоца	Износ средстава

- Ева отвара рачуне у банци А и Б.
- Неколико пута шаље износ од 1 евра са рачуна у банци А на рачун у банци Б.
- Претпоставка је да банке не мијењају често кључеве у међусобној комуникацији
- Ева прати трансфере из банке А у банку Б и на неколико инстанци само мијења поље 4 са оним што има снимљено у свом криптограму.

Још о блок крипто-системима

Cipher Block Chaining mode (CBC)

- Дијелимо текст на блокове од b бита. Нека су x_i, y_i и иницијални вектор IV блокови дужине b бита.
- Ако је e_k функција енкрипције, онда у овом моду енкрипцију вршимо на следећи начин

$$y_1 = e_k(x_1 \oplus IV),\ y_i = e_k(x_i \oplus y_{i-1}),\ i \geq 2.$$

- Сходно томе, декрипција је дата са

$$x_1 = e_k^{-1}(y_1) \oplus IV,\ x_i = e_k^{-1}(y_i) \oplus y_{i-1},\ i \geq 2.$$

Још о блок крипто-системима

Output Feedback mode (OFB)

- Дијелимо текст на блокове од b бита. Нека су x_i, y_i, s_i и IV блокови дужине b бита, а e_k функција енкрипције.
- Нека је $s_1 = e_k(IV)$, $y_1 = s_1 \oplus x_1$. Енкрипција у овом моду је
$$s_i = e_k(s_{i-1}),\ y_i = s_i \oplus x_i,\ i \geq 2.$$
- Сходно томе, декрипција је дата са $s_1 = e_k(IV)$, $x_1 = s_1 \oplus y_1$, а потом
$$s_i = e_k(s_{i-1}),\ x_i = s_i \oplus y_i,\ i \geq 2.$$

Још о блок крипто-системима

Cipher Feedback mode (CFB)

- Дијелимо текст на блокове од b бита. Нека су x_i, y_i и IV блокови дужине b бита, а e_k функција енкрипције.
- Нека је $y_1 = e_k(IV) \oplus x_1$. Енкрипција у овом моду је

$$y_i = e_k(y_{i-1}) \oplus x_i,\ i \geq 2.$$

- Сходно томе, декрипција је дата са $x_1 = e_k(IV) \oplus y_1$, а потом

$$x_i = e_k(y_{i-1}) \oplus y_i,\ i \geq 1.$$

Хвала на пажњи :)