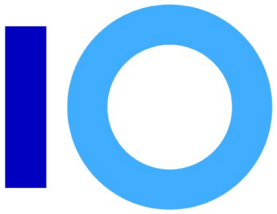


"Ss. Cyril and Methodius" University in Skopje
FACULTY OF COMPUTER
SCIENCE AND ENGINEERING

Лабораториска вежба бр. 2 по предметот

"Криптографија"

DES block cipher

Изработил:

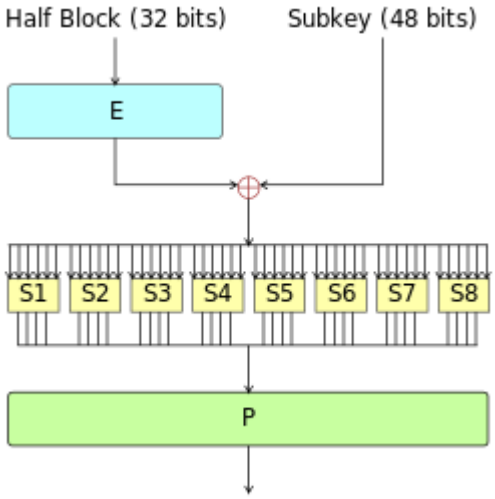
Мартин Костадинов

Број на индекс:

161159

ВОВЕД

Во оваа документација ќе биде прикажан начинот на кој е имплементиран DES алгоритмот за шифрирање и дешифрирање на пораки. DES е блоковски алгоритам за криптирање кој обработува блокови од 64 битна големина и користи клуч со големина на 56 бита (+8 parity bits и најчесто се отфрлуваат). Овој алгоритам е базиран на дизајнот на Horst Feistel и ја користи Feistel-ова функција при криптирање од оригинален текст во шифриран текст. Работи на начин така што најпрвин има иницијална пермутација што ги меша битовите па потоа ја имаме Feistel-овата функција и на крајот имаме уште една, додатна финална пермутација. За време на Feistel-овата функција, пораката се дели на два блока од по 32 бита и на секој блок се прави XOR со 48 битен подклуч и на овој начин пораката се проширува на 48 бита. Потоа пораката се дели на 8 блокови од по 6 бита (6*8=48) односно во 8 S-Boxes. Секој од овие S-Boxes прави нелинеарна трансформација на 6 битната информација во 4 битна и како таква ја дава на излез. Откако сите трансформации ќе завршат, се вади 32 битен блок и се предава на P-Box кој прави пермутација на битовите, се со цел да не се појават исти битови во наредните рунди на S-Boxes.



1. Имплементација

За оваа вежба беше користена готова имплементација на DES алгоритмот, правена во програмскиот јазик Java. Автори на овој код се Jonathan Poltak Samosir и Goodwin Lam, кодот е достапен на https://github.com/poltak/DataEncryptionStandard.

Самата имплементација во себе содржи 4 класи и тоа:

- DES (методи потребни за функционалност на алгоритмот, енкрипција, декрипција и сл.);
- FeistelFunction (методи потребни за функционалност на Feistel-ова функција);
- RoundKeyGenerator (метода потребна за генерирање на клуч во секоја рунда);
- DESInterface (главната main функција каде се вршени проверките во интерес на вежбата).

1. Користејќи некоја од готовите имплементации на блок шифрувачот DES во програмски јазик по желба да се провери дали соодветно работат енкрипцијата и декрипцијата над дадена порака M со ист клуч K. Користете ја оваа имплементација за да може да се одговорат следните прашања:

а) кој е излезот од првата рунда на DES алгоритамот кога пораката и клучот се составени само од 0-ли. Испечатете ги рундовските клучеви.

- Ако во DES класата го сетираме бројот на рунди да биде 1, излезот е следен:

Key for round 0: 0

0000010000000100000000001010101010101010000000101010100010101010

б) кој е излезот од првата рунда на DES алгоритамот кога пораката и клучот се составени само од 1-ци. Испечатете ги рундовските клучеви.

- Сите единици значи да енкриптираме порака од обликот на 111...111. Со оглед на тоа што DES алгоритмот работи со **long** променливи, 1111...111 ќе биде максималната вредност на оваа променлива. Излезот е следен:

Key for round 0: 281474708275199

0110101111111011101111111011101010101111111111101111101110101010

Додека Long.MAX_VALUE изнесува 9223372036854775807

в) кој е излезот од првата рунда на DES алгоритамот кога пораката под а) се променила во еден бит (на било која позиција ставете бит 1, а сите останати нека останат 0), а клучот останал ист како и претходно (се состои од сите 0-ли). Пробајте повеќе варинати за позиции на битот 1. Може ли да изведете некој заклучок?

-

0	0000010000000100000000010101010101010101000000010101010001010101
2	0000010001000100000001010101010001000101000100010101010001010111
4	0000010000000100000000010101010101010101000000010101010001010001
8	0100010000000100000000010101010101010101000000010100010101011100
16	0000010000000100000000010101010101010101000000010101010001000101
32	0000000000000100010000000100010101010100000000101010100011 10101
64	0000010000000100000000010101010101010101000000010101010000010101

Согласно местоположбата на битот, можеме да заклучиме дека на таа позиција имаме промена во обратниот бит (во поголемиот дел од случаевите).

г) колку битови се промениле на излез после првата рунда. Споредено со ситуацијата под а) има ли разлика? Колкав е авеланч ефектот тука?

- После првата рунда се има променено 1 бит (во поголемиот дел од случаевите). Avelanche ефектот е мал и на некој начин може да кажеме и дека не постои бидејќи за Avelanche ефект потребно е за една промена на бит во оригиналната порака да има промена на повеќе битови во шифрираниот текст.

д) споредете колку од S-box-овите (во втората рунда) сега имаат различен влез, споредено со ситуацијата под а)?

00000...000 (0)	0000000...000010 (2)
Key for round 0: 0 Runda: [0] 0 0 14 Runda: [1] 0 0 15 Runda: [2] 0 0 10 Runda: [3] 0 0 7 Runda: [4] 0 0 2 Runda: [5] 0 0 12 Runda: [6] 0 0 4 Runda: [7] 0 0 13 Key for round 1: 0 Runda: [0] 1 13 5 Runda: [1] 3 8 11 Runda: [2] 1 13 11 Runda: [3] 3 8 9 Runda: [4] 1 13 9 Runda: [5] 3 11 7 Runda: [6] 3 11 15 Runda: [7] 3 12 3	Key for round 0: 0 Runda: [0] 0 0 14 Runda: [1] 0 0 15 Runda: [2] 0 0 10 Runda: [3] 0 0 7 Runda: [4] 0 0 2 **Runda: [5] 1 0 10** **Runda: [6] 0 8 3** Runda: [7] 0 0 13 Key for round 1: 0 Runda: [0] 1 13 5 **Runda: [1] 3 10 7** **Runda: [2] 1 14 15** **Runda: [3] 1 8 4** Runda: [4] 1 13 9 **Runda: [5] 3 15 13** **Runda: [6] 2 11 8** **Runda: [7] 3 4 4**

Во првата рунда имаме промена во 2 S-Boxes додека пак во втората рунда имаме промена на дури 6 S-Boxes.

ѓ) наведете кои точно S-box-ови се засегнати од оваа промена на битот, односно да се покаже патот на промена на S-box-овите низ сите 16 рунди на DES алгоритамот.

00000...000 (0)	0000000...000010 (2)
Key for round 0: 0 Runda: [0] 0 0 14 Runda: [1] 0 0 15 Runda: [2] 0 0 10 Runda: [3] 0 0 7 Runda: [4] 0 0 2 Runda: [5] 0 0 12 Runda: [6] 0 0 4 Runda: [7] 0 0 13 Key for round 1: 0 Runda: [0] 1 13 5 Runda: [1] 3 8 11 Runda: [2] 1 13 11 Runda: [3] 3 8 9 Runda: [4] 1 13 9 Runda: [5] 3 11 7	Key for round 0: 0 Runda: [0] 0 0 14 Runda: [1] 0 0 15 Runda: [2] 0 0 10 Runda: [3] 0 0 7 Runda: [4] 0 0 2 **Runda: [5] 1 0 10** **Runda: [6] 0 8 3** Runda: [7] 0 0 13 Key for round 1: 0 Runda: [0] 1 13 5 **Runda: [1] 3 10 7** **Runda: [2] 1 14 15** **Runda: [3] 1 8 4** Runda: [4] 1 13 9 **Runda: [5] 3 15 13**

Runda: [6] 3 11 15 Runda: [7] 3 12 3 Key for round 2: 0 Runda: [0] 2 14 5 Runda: [1] 0 7 4 Runda: [2] 3 3 0 Runda: [3] 3 10 5 Runda: [4] 1 14 8 Runda: [5] 0 13 7 Runda: [6] 3 4 1 Runda: [7] 1 15 2 Key for round 3: 0 Runda: [0] 1 5 2 Runda: [1] 3 11 12 Runda: [2] 3 15 12 Runda: [3] 2 10 3 Runda: [4] 1 6 13 Runda: [5] 1 11 14 Runda: [6] 2 10 6 Runda: [7] 0 6 11 Key for round 4: 0 Runda: [0] 3 5 9 Runda: [1] 2 14 2 Runda: [2] 0 4 6 Runda: [3] 1 5 15 Runda: [4] 2 14 0 Runda: [5] 0 2 10 Runda: [6] 0 5 0 Runda: [7] 2 7 2 Key for round 5: 0 Runda: [0] 1 8 10 Runda: [1] 0 11 13 Runda: [2] 3 1 10 Runda: [3] 2 9 1 Runda: [4] 3 7 13 Runda: [5] 3 11 7 Runda: [6] 2 14 9 Runda: [7] 1 0 1 Key for round 6: 0 Runda: [0] 1 15 8 Runda: [1] 3 13 5 Runda: [2] 3 14 2 Runda: [3] 1 9 7	**Runda: [6] 2 11 8** **Runda: [7] 3 4 4** Key for round 2: 0 Runda: [0] 2 7 11 Runda: [1] 2 5 4 Runda: [2] 2 0 13 Runda: [3] 1 1 8 Runda: [4] 2 15 14 Runda: [5] 3 1 3 Runda: [6] 3 11 15 Runda: [7] 2 15 8 Key for round 3: 0 Runda: [0] 2 13 10 Runda: [1] 2 5 4 Runda: [2] 3 5 9 Runda: [3] 3 13 7 Runda: [4] 3 15 3 Runda: [5] 2 8 7 Runda: [6] 0 6 8 Runda: [7] 1 7 4 Key for round 4: 0 Runda: [0] 0 13 9 Runda: [1] 3 1 8 Runda: [2] 2 14 14 Runda: [3] 1 1 8 Runda: [4] 2 12 6 Runda: [5] 0 2 10 Runda: [6] 0 0 4 Runda: [7] 1 6 7 Key for round 5: 0 Runda: [0] 2 12 3 Runda: [1] 1 5 2 Runda: [2] 2 14 14 Runda: [3] 1 2 11 Runda: [4] 0 15 9 Runda: [5] 3 1 3 Runda: [6] 2 8 10 Runda: [7] 1 1 15 Key for round 6: 0 Runda: [0] 3 3 2 Runda: [1] 3 8 11 Runda: [2] 0 8 1 Runda: [3] 1 2 11

Runda: [4] 3 8 6 Runda: [5] 0 9 13 Runda: [6] 3 4 1 Runda: [7] 1 10 6 Key for round 7: 0 Runda: [0] 1 1 15 Runda: [1] 3 9 6 Runda: [2] 3 13 5 Runda: [3] 2 15 4 Runda: [4] 3 0 11 Runda: [5] 0 11 4 Runda: [6] 3 5 4 Runda: [7] 2 12 15 Key for round 8: 0 Runda: [0] 0 9 10 Runda: [1] 2 0 0 Runda: [2] 1 7 10 Runda: [3] 2 10 3 Runda: [4] 0 1 12 Runda: [5] 3 3 12 Runda: [6] 2 15 2 Runda: [7] 3 0 2 Key for round 9: 0 Runda: [0] 1 8 10 Runda: [1] 0 8 9 Runda: [2] 1 1 7 Runda: [3] 2 9 1 Runda: [4] 3 0 11 Runda: [5] 0 12 14 Runda: [6] 0 5 0 Runda: [7] 3 0 2 Key for round 10: 0 Runda: [0] 0 2 13 Runda: [1] 1 5 2 Runda: [2] 2 13 10 Runda: [3] 2 1 6 Runda: [4] 2 5 13 Runda: [5] 2 1 14 Runda: [6] 3 7 7 Runda: [7] 2 12 15 Key for round 11: 0 Runda: [0] 0 15 7 Runda: [1] 3 3 1	Runda: [4] 1 14 8 Runda: [5] 0 13 7 Runda: [6] 2 6 7 Runda: [7] 0 1 2 Key for round 7: 0 Runda: [0] 2 0 4 Runda: [1] 1 2 4 Runda: [2] 1 9 8 Runda: [3] 3 8 9 Runda: [4] 0 9 5 Runda: [5] 3 7 10 Runda: [6] 3 12 14 Runda: [7] 0 9 9 Key for round 8: 0 Runda: [0] 0 8 3 Runda: [1] 1 0 3 Runda: [2] 0 11 7 Runda: [3] 2 6 7 Runda: [4] 0 6 11 Runda: [5] 0 0 12 Runda: [6] 0 3 14 Runda: [7] 3 0 2 Key for round 9: 0 Runda: [0] 0 15 7 Runda: [1] 3 7 2 Runda: [2] 3 12 11 Runda: [3] 1 11 12 Runda: [4] 2 12 6 Runda: [5] 0 1 1 Runda: [6] 2 4 12 Runda: [7] 1 6 7 Key for round 10: 0 Runda: [0] 2 12 3 Runda: [1] 1 4 15 Runda: [2] 0 10 12 Runda: [3] 1 0 13 Runda: [4] 1 13 9 Runda: [5] 3 11 7 Runda: [6] 2 13 5 Runda: [7] 3 7 13 Key for round 11: 0 Runda: [0] 1 1 15 Runda: [1] 3 12 0

Runda: [2] 3 14 2 Runda: [3] 1 15 9 Runda: [4] 2 9 9 Runda: [5] 2 1 14 Runda: [6] 3 7 7 Runda: [7] 3 14 6 Key for round 12: 0 Runda: [0] 0 9 10 Runda: [1] 3 6 4 Runda: [2] 0 14 2 Runda: [3] 1 3 5 Runda: [4] 2 9 9 Runda: [5] 2 7 3 Runda: [6] 2 1 4 Runda: [7] 3 2 14 Key for round 13: 0 Runda: [0] 1 5 2 Runda: [1] 2 10 12 Runda: [2] 1 5 4 Runda: [3] 3 13 7 Runda: [4] 2 10 12 Runda: [5] 0 3 15 Runda: [6] 3 4 1 Runda: [7] 0 10 3 Key for round 14: 0 Runda: [0] 0 0 14 Runda: [1] 1 5 2 Runda: [2] 3 8 4 Runda: [3] 1 12 1 Runda: [4] 1 10 15 Runda: [5] 0 13 7 Runda: [6] 3 0 6 Runda: [7] 0 10 3 Key for round 15: 0 Runda: [0] 1 11 11 Runda: [1] 3 11 12 Runda: [2] 3 14 2 Runda: [3] 0 10 8 Runda: [4] 1 0 14 Runda: [5] 1 13 11 Runda: [6] 2 12 0 Runda: [7] 1 2 13	Runda: [2] 0 15 8 Runda: [3] 3 2 0 Runda: [4] 1 11 10 Runda: [5] 2 10 4 Runda: [6] 1 3 7 Runda: [7] 2 12 15 Key for round 12: 0 Runda: [0] 3 12 10 Runda: [1] 0 15 10 Runda: [2] 2 3 9 Runda: [3] 2 2 9 Runda: [4] 0 5 10 Runda: [5] 2 4 2 Runda: [6] 1 7 10 Runda: [7] 3 13 5 Key for round 13: 0 Runda: [0] 3 13 0 Runda: [1] 2 9 8 Runda: [2] 3 5 9 Runda: [3] 3 10 5 Runda: [4] 0 11 15 Runda: [5] 3 5 5 Runda: [6] 3 13 2 Runda: [7] 3 13 5 Key for round 14: 0 Runda: [0] 3 6 1 Runda: [1] 0 10 2 Runda: [2] 1 3 9 Runda: [3] 2 14 8 Runda: [4] 1 6 13 Runda: [5] 1 9 1 Runda: [6] 2 13 5 Runda: [7] 2 5 12 Key for round 15: 0 Runda: [0] 2 11 7 Runda: [1] 2 6 13 Runda: [2] 1 4 3 Runda: [3] 1 14 14 Runda: [4] 0 9 5 Runda: [5] 3 4 9 Runda: [6] 1 11 12 Runda: [7] 3 15 11

- Промената во првите две рунди е иста како и под д) а во наредните рунди веќе имаме сосема различни вредности на S-Воховите (вредноста на S-Воховите е последната).

2. Изгенерирајте си сите слаби клучеви за DES алгоритамот и покажете преку примери зошто овие клучеви не треба да се користат.

- Потребно е да се избегнуваат слаби клучеви при DES енкрипција поради тоа што при формирањето на подклучевите за енкрипција, се формираат 16 идентични подклучеви. Додатно, имаме слаби клучеви што голем дел од својата вредност ја префрлаат во другата рунда или воопшто не се менуваат. Како пример за слаби клучеви се:

а) 0x0000000000000000 (сите нули)

б) 0xFFFFFFFFFFFFFFFF (сите единици)

в) 0xE1E1E1E1F0F0F0F0

г) 0x1E1E1E1E0F0F0F0F

Клуч = 0x0000000000000000	Клуч = 0xFFFFFFFFFFFFFFFF
Key for round 0: 0 Key for round 1: 0 Key for round 2: 0 Key for round 3: 0 Key for round 4: 0 Key for round 5: 0 Key for round 6: 0 Key for round 7: 0 Key for round 8: 0 Key for round 9: 0 Key for round 10: 0 Key for round 11: 0 Key for round 12: 0 Key for round 13: 0 Key for round 14: 0 Key for round 15: 0	Key for round 0: **28147**4708275199 Key for round 1: 281200098803711 Key for round 2: **28147**0681743359 Key for round 3: **2814749**59933439 Key for round 4: 280375465082879 Key for round 5: **28147**2829227007 Key for round 6: 263882790666239 Key for round 7: **2814749**76710655 Key for round 8: 281337537757183 Key for round 9: **2814**57796841471 Key for round 10: 211106232532991 Key for round 11: 280925220896767 Key for round 12: **2814749**43156223 Key for round 13: 246290604621823 Key for round 14: **2814749**76710655 Key for round 15: **28147**3902968831