Lab 3: DES Block Cipher Internals & Modes of Use

2019年10月10日

一、实验目的

- 1. 熟悉 DES 加密内部过程。
- 2. 熟悉 CBC 和 CTR 两种加密模式的过程。

二、实验环境

DES block cipher calculator (注意: 此工具中 key length 为 64 位,即 16 个 16 进制的数,与明文和密文的长度相同)

三、实验背景知识

DES 是经典的分组密码,加密 64bit 的数据块,得到 64bit 的密文。由于其密钥空间为 2⁵⁶,容易遭受穷举式攻击(exhaustive search attack),因此被 3DES 或 AES 代替。

DES 使用 Feistel 加密模式,由于其结构的特点,可以使用任意的函数构造出可逆的函数。DES 的核心是 Feistel function 的设计,如图 1 所示。

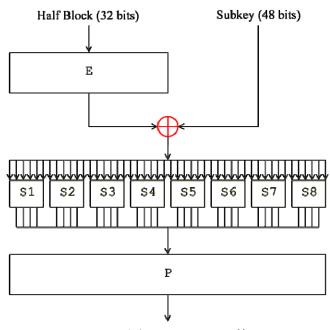
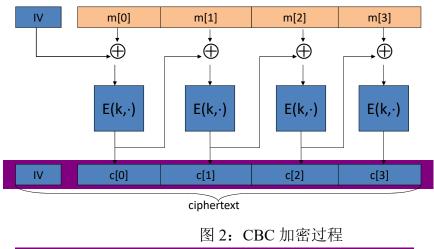


图 1: Feistel 函数

可以参考如下网页来获取 E 扩展、S-box 表格等,或参考后面的图 5、图 6。 https://www.cnblogs.com/songwenlong/p/5944139.html

为了使用 DES 密钥重复加密多块消息,需要设计分组密码的加密模式。简单的 ECB 电子密码本已被证明不安全。经常使用的加密模式为 CBC 模式,如图 2,3 所示,和 CTR 模式,如图 4 所示。



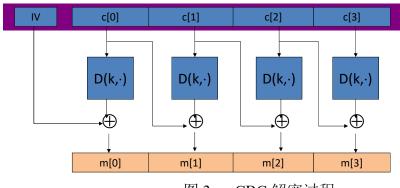


图 3: CBC 解密过程

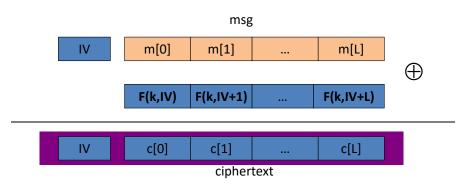


图 4: CTR 模式加密过程

四、实验内容与要求

统一说明:实验中所需的密钥、明文与密文都可以自己构造。

1. 验证 DES 的可逆性与扩散性。

Key: 5B5A57676A56676E

Plaintext: 675A69675E5A6B5B Ciphertext: 974AFFBF86022D1F

密钥、明文与密文都可以自己设置,但要保证为64bits(16个16进制数)。

- a. 输入 key 与明文,点击加密,得到密文。
- b. 输入 key 与密文,点击解密,得到对应的明文。
- c. 将明文或密钥中的一个比特翻转,查看密文的变化情况。(Diffusion,扩散性)

2. 熟悉 DES 内部加密过程。

Key: 5B5A57676A56676E

Plaintext: 675A69675E5A6B5A

选由 DES calculator 由的 trace level.

Trace Level: ○ 0: none ○ 1: calls ⊙ 2: +rounds

依据实验背景知识中提供的参考资料,手算第二轮(round 2)的 feistel 函数结果,并验证结果。

注意: SK 后面数字是 48 位的扩展密钥 (8 组 6 位的数), 如 38 \rightarrow 11 1000, 09— \rightarrow 001001, 1b \rightarrow 011011

3. 熟悉 CBC 与 CTR 的过程。

(1) CBC 模式

构造一个 24 字节的消息, 假设 IV = 0, Key: 5B5A57676A56676E

- a. 用 CBC 模式对消息进行加密,得到密文。
- b. 用 CBC 模式对消息进行解密,得到明文。
- (2) CTR 模式

构造一个 24 字节的消息, 假设 IV = 0, Key: 5B5A57676A56676E

- c. 用 CTR 模式对消息进行加密,得到密文。
- d. 用 CTR 模式对消息进行解密,得到明文。

注意:异或运算可以使用老师提供的 java 小程序,也可以使用 online calculator,如:

http://www.jdejong.net/tools/bitwisecalculator.php

24 字节消息的构造举例:

yuanyi's message yuanyi's message

a	b	c	d	e	f	g	h	i	j	k	l	m	n	0	p	q	r	S	t	u	v	w	X	y	Z
61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a

': 27, 空格: 20

注意:消息可以自己构造,对应的十六进制数可以查表1。

表 1: ASCII 表

ASCII 码		字符	ASCII 码		字符	ASC	II 码	字符	ASC	字符	
十进制	十六进制	1.10	十进制	十六进制	1.1.1	十进制	十六进制	1.17	十进制	十六进制	1.01
032	20		056	38	8	080	50	Р	104	68	h
033	21	1	057	39	9	081	51	Q	105	69	i
034	22	п	058	3A	:	082	52	R	106	6A	j
035	23	#	059	3B	;	083	53	S	107	6B	k
036	24	\$	060	3C	<	084	54	Т	108	6C	1
037	25	%	061	3D	=	085	55	U	109	6D	m
038	26	&	062	3E	>	086	56	V	110	6E	n
039	27	1	063	3F	?	087	57	W	111	6F	0
040	28	(064	40	@	088	58	X	112	70	р
041	29)	065	41	Α	089	59	Y	113	71	q
042	2A	340	066	42	В	090	5A	Z	114	72	r
043	2B	+	067	43	С	091	5B	[115	73	s
044	2C	,	068	44	D	092	5C	1	116	74	t
045	2D	10	069	45	Е	093	5D]	117	75	u
046	2E	SO. 0	070	46	F	094	5E	^	118	76	V
047	2F	1	071	47	G	095	5F	ter	119	77	W
048	30	0	072	48	Н	096	60	•	120	78	Х
049	31	1	073	49	I	097	61	а	121	79	У
050	32	2	074	4A	J	098	62	b	122	7A	Z
051	33	3	075	4B	K	099	63	С	123	7B	{
052	34	4	076	4C	L	100	64	d	124	7C	
053	35	5	077	4D	М	101	65	e	125	7D	}
054	36	6	078	4E	N	102	66	f	126	7E	~
055	37	7	079	4F	0	103	67	g	127	7F	

图 5 Expansion function (E)

S-boxes

S ₁	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0уууу0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0уууу1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1уууу0	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
1yyyy1	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S ₂	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0уууу0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
0уууу1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
1уууу0	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
1yyyy1	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S ₃	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
	x0000x	x0001x	x0010x 9	x0011x	x0100x	x0101x	x0110x 15	x0111x 5	x1000x	x1001x 13	x1010x 12	x1011x 7	x1100x	x1101x	x1110x	x1111x 8
S ₃																
S ₃	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	
S ₃ 0yyyy0 0yyyy1	10	7	9	14	6	3	15 6	5 10	1 2	13	12 5	7 14	11	4 11	2 15	8
S ₃ 0yyyy0 0yyyy1 1yyyy0	10 13 13	0 7 6	9 0 4	14 9 9	6 3 8	3 4 15	15 6 3	5 10 0	1 2 11	13 8 1	12 5 2	7 14 12	11 12 5	4 11 10	2 15 14	8 1 7
S ₃ 0yyyy0 0yyyy1 1yyyy0 1yyyy1	10 13 13 1	0 7 6 10	9 0 4 13	14 9 9	6 3 8 6	3 4 15 9	15 6 3 8	5 10 0 7	1 2 11 4	13 8 1 15	12 5 2 14	7 14 12 3	11 12 5 11	4 11 10 5	2 15 14 2	8 1 7 12
S ₃ 0yyyy0 0yyyy1 1yyyy0 1yyyy1 S ₄	10 13 13 1 x0000x	0 7 6 10 x0001x	9 0 4 13 x0010x	14 9 9 0 x0011x	6 3 8 6 x0100x	3 4 15 9 x0101x	15 6 3 8 x0110x	5 10 0 7 x0111x	1 2 11 4 x1000x	13 8 1 15 x1001x	12 5 2 14 x1010x	7 14 12 3 x1011x	11 12 5 11 x1100x	4 11 10 5 x1101x	2 15 14 2 x1110x	8 1 7 12 x1111x
S ₃ 0yyyy0 0yyyy1 1yyyy0 1yyyy1 S ₄ 0yyyy0	10 13 13 1 x0000x	0 7 6 10 x0001x 13	9 0 4 13 x0010x 14	14 9 9 0 x0011x 3	6 3 8 6 x0100x	3 4 15 9 x0101x 6	15 6 3 8 x0110x 9	5 10 0 7 x0111x 10	1 2 11 4 x1000x 1	13 8 1 15 x1001x 2	12 5 2 14 x1010x 8	7 14 12 3 x1011x 5	11 12 5 11 x1100x	4 11 10 5 x1101x 12	2 15 14 2 x1110x 4	8 1 7 12 x1111x 15

S ₅	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
ОууууО	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
0уууу1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
1уууу0	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
1уууу1	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S ₆	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0уууу0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
0уууу1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
1уууу0	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
1yyyy1	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S ₇	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	1100			
							AUTTOR	AUTITIA	XIOOOX	XIOUIX	XIOIOX	XIUIIX	x1100x	x1101x	x1110x	x1111x
0уууу0	4	11	2	14	15	0	8	13	3	12	9	7	5	x1101x 10	x1110x 6	x11111 x
0yyyy0 0yyyy1	13	11	2	14 7	15 4											
					-	0	8	13	3	12	9	7	5	10	6	1
0уууу1	13	0	11	7	4	9	8	13 10	3 14	12	9	7	5 2	10 15	6	1
0yyyy1 1yyyy0	13	0 4	11	7 13	4 12	9	8 1 7	13 10 14	3 14 10	12 3 15	9 5 6	7 12 8	5 2 0	10 15 5	6 8 9	1 6 2
0yyyy1 1yyyy0 1yyyy1	13 1 6	0 4 11	11 11 13	7 13 8	4 12 1	0 9 3 4	8 1 7 10	13 10 14 7	3 14 10 9	12 3 15 5	9 5 6 0	7 12 8 15	5 2 0 14	10 15 5 2	6 8 9 3	1 6 2 12
0yyyy1 1yyyy0 1yyyy1 S ₈	13 1 6 x0000x	0 4 11 x0001x	11 11 13 x0010x	7 13 8 x0011x	4 12 1 x0100x	0 9 3 4 x0101x	8 1 7 10 x0110x	13 10 14 7 x0111x	3 14 10 9 x1000 x	12 3 15 5 x1001x	9 5 6 0 x1010x	7 12 8 15 x1011x	5 2 0 14 x1100x	10 15 5 2 x1101x	6 8 9 3 x1110 x	1 6 2 12 x1111x
0yyyy1 1yyyy0 1yyyy1 S ₈ 0yyyy0	13 1 6 x0000x	0 4 11 x0001x 2	11 11 13 x0010x 8	7 13 8 x0011x 4	4 12 1 x0100x 6	0 9 3 4 x0101x 15	8 1 7 10 x0110x 11	13 10 14 7 x0111x	3 14 10 9 x1000x 10	12 3 15 5 x1001x 9	9 5 6 0 x1010x 3	7 12 8 15 x1011x	5 2 0 14 x1100x 5	10 15 5 2 x1101x 0	6 8 9 3 x1110x	1 6 2 12 x1111x 7

图 6 S-box

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

图 7 P 盒置换

- 1. 实验报告由小组完成。
- 2. 实验报告成绩评分标准:
 - 实验报告提交及时(10分)
 - 实验过程翔实(40分)
 - 语言表达清晰(20分)
 - 实验结果合理(20分)
 - 实验体会(10)
- 3. 实验报告提交截止日期等老师通知。