Lab 3: DES Block Cipher Internals & Modes of Use

2017 年 3 月 28 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 2^{56}，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。

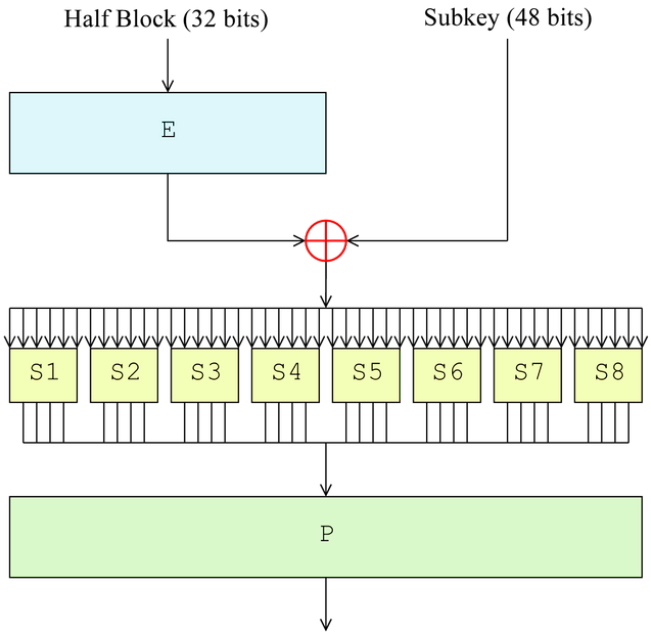


图 1：Feistel 函数

可以参考如下网页来了解 DES Feistel function 的细节：

https://en.wikipedia.org/wiki/Data_Encryption_Standard

Feistel 函数中的 E 扩展、S-box 表格等可以查看：

https://en.wikipedia.org/wiki/DES_supplementary_material

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。

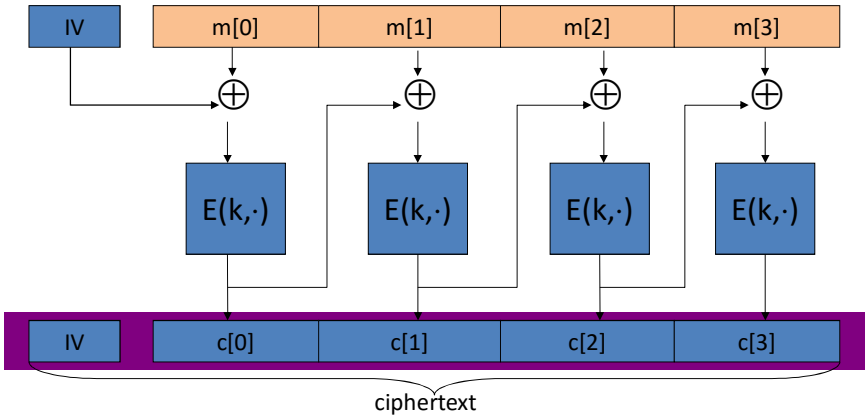


图 2：CBC 加密过程

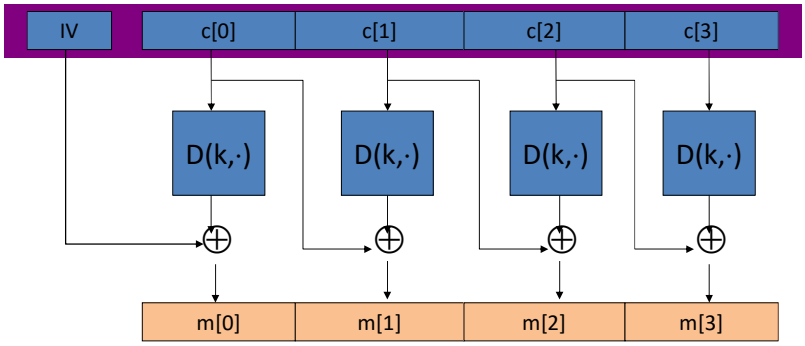


图 3： CBC 解密过程

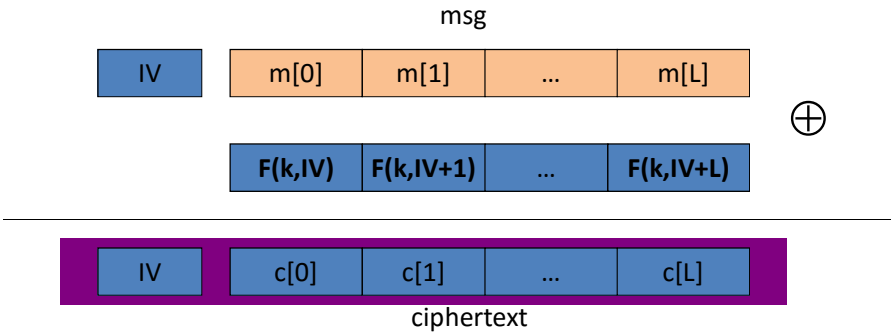


图 4：CTR 模式加密过程

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：675A69675E5A6B5A

   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。

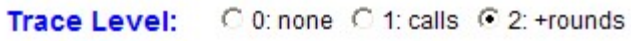
   c. 将明文或密钥中的一个比特翻转，查看密文的变化情况。（Diffusion，扩散性）

2. 熟悉 DES 内部加密过程。

   Key：5B5A57676A56676E

   Plaintext：675A69675E5A6B5A

选中 DES calculator 中的 trace level：



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 –〉11 1000，09—〉001001，1b –〉 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	o	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 十进制	ASCII 码 十六进制	字符	ASCII 码 十进制	ASCII 码 十六进制	字符	ASCII 码 十进制	ASCII 码 十六进制	字符	ASCII 码 十进制	ASCII 码 十六进制	字符
032	20		056	38	8	080	50	P	104	68	h
033	21	!	057	39	9	081	51	Q	105	69	i
034	22	"	058	3A	:	082	52	R	106	6A	j
035	23	#	059	3B	;	083	53	S	107	6B	k
036	24	$	060	3C	<	084	54	T	108	6C	l
037	25	%	061	3D	=	085	55	U	109	6D	m
038	26	&	062	3E	>	086	56	V	110	6E	n
039	27	'	063	3F	?	087	57	W	111	6F	o
040	28	(	064	40	@	088	58	X	112	70	p
041	29	)	065	41	A	089	59	Y	113	71	q
042	2A	*	066	42	B	090	5A	Z	114	72	r
043	2B	+	067	43	C	091	5B	[	115	73	s
044	2C	,	068	44	D	092	5C	\	116	74	t
045	2D	-	069	45	E	093	5D	]	117	75	u
046	2E	.	070	46	F	094	5E	^	118	76	v
047	2F	/	071	47	G	095	5F	_	119	77	w
048	30	0	072	48	H	096	60	`	120	78	x
049	31	1	073	49	I	097	61	a	121	79	y
050	32	2	074	4A	J	098	62	b	122	7A	z
051	33	3	075	4B	K	099	63	c	123	7B	{
052	34	4	076	4C	L	100	64	d	124	7C	|
053	35	5	077	4D	M	101	65	e	125	7D	}
054	36	6	078	4E	N	102	66	f	126	7E	~
055	37	7	079	4F	O	103	67	g	127	7F	⌂

五、实验报告

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： 2017 年 4 月 11 日。