Homework 5

4.2 Moving backwards:

$R_i = L_{i+1}$

and

$L_i = R_{i+1} \oplus f(R_i, K_i)$

If we follow this pattern, we are left with L_0 & R_0.

4.4

2b	28	ab	09	a0	88	23	2a	42	7a	59	73	38	47	1c	68	ef	a8	b6	0b	84	7c	ca	11	68	11	0b	ca	4c	5f	84	4c
7c	ae	f7	cf	fa	54	a3	6c	02	96	35	59	80	16	23	7a	44	52	71	06	01	83	f2	f9	88	06	f9	00	54	5f	ab	ab
15	02	13	4f	fc	2c	39	76	95	69	80	f6	47	fc	7e	88	a5	5b	25	a0	cb	9b	b8	15	a3	3c	86	93	f7	09	4f	dc
16	ab	08	3c	17	b1	39	05	f2	43	7a	7f	7d	3e	44	3b	41	7f	3b	00	f8	87	bc	bc	7a	fd	41	f8	0c	c3	b2	4f

...	ca	b5	31	7f	ac	19	28	57	d0	e9	d1	b6
	d2	8d	2b	8d	77	fa	d1	5c	14	ee	3f	63
	73	ba	f5	29	66	dc	29	00	f9	25	0c	0c
	21	02	b0	2f	f3	21	41	be	a8	89	a6	a6

5.1

5.7a