Note Title 1/24/2012

P → I attack → 26

C → L d w w d f n

Plain text: I a t t a c k
Key: 2 3 4 2 3 4 2
Cipher text: K d x v d g m

(key is "234") → 26^3

	00	01	10	11
00	0011	0100	1111	0001
01	1010	0110	0101	1011
10	1110	1101	0100	0010
11	0111	0000	1001	1100

(a)

→

	0	1	2	3
0	3	8	15	1
1	10	6	5	11
2	14	13	4	2
3	7	0	9	12

(b)

Figure 8.3: A 4-bit S-box (a) An S-box in binary. (b) The same S-box in decimal. This particular S-box is used in the Serpent cryptosystem, which

"0110" → 0101