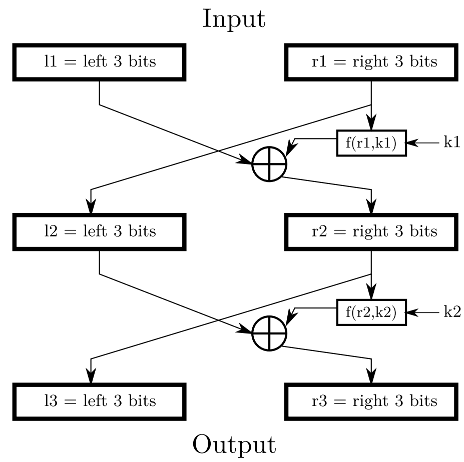
(1) At the beginning of the second round in DES R_1 begins in the six bits 110110 and ends in the six bits 010010. Moreover K_2 begins in the 6 bits 110101 and ends in 011001. What are the 6 input bits and the 4 output bits from the last (eighth) S-box of that round?

(2) A three letter message is encoded with a double Feistel cipher as given in the following diagram.



The left and right bits correspond to integer values 0 through 7 (the normal binary ordering) which will be used in the function f. The input and output are uppercase and lowercase letters, the digits 0 through 9 and the punctuation . and , (64 characters in all) which are encoded with a 6 digit binary number given by the table below.

The key of this system are two numbers k_1 and k_2 which take on the values 0 through 7. The function f is given by the following table:

$r\backslash k$	0	1	2	3	4	5	6	7
0	4	3	2	1	0	7	6	5
1	5	6	7	0	7	6	2	5
2	1	2	3	4	4	1	3	0
3	4	3	2	1	2	7	6	5
4	0	7	6	5	0	1	4	3
5	1	2	3	4	5	6	7	0
6	5	6	7	0	1	2	3	4
7	0	7	6	5	4	3	2	1

Three letters are encoded with $k_1 = 2$ and $k_2 = 5$. What is the plaintext if the ciphertext is ℓ6h?

Hint: the answer is a common three letter word so it is likely you will know if you have the right answer at the end of the problem.

0	000000	1	000001	2	000010	3	000011	4	000100	5	000101	6	000110	7	000111
8	001000	9	001001	A	001010	B	001011	C	001100	D	001101	E	001110	F	001111
G	010000	H	010001	I	010010	J	010011	K	010100	L	010101	M	010110	N	010111
O	011000	P	011001	Q	011010	R	011011	S	011100	T	011101	U	011110	V	011111
W	100000	X	100001	Y	100010	Z	100011	.	100100	a	100101	b	100110	c	100111
d	101000	e	101001	f	101010	g	101011	h	101100	i	101101	j	101110	k	101111
ℓ	110000	m	110001	n	110010	o	110011	p	110100	q	110101	r	110110	s	110111
t	111000	u	111001	v	111010	w	111011	x	111100	y	111101	z	111110	,	111111

(3) Using the Knapsack encryption system with a public modulus of 137 and a public key of

$$55 \;-\; 1 \;-\; 29 \;-\; 113 \;-\; 116 \;-\; 123$$

the message $50, 17, 63, 107, 100, 121$ was sent. Given that the first number of the private key is 1, what was the message? The encoding for the letters is given on the previous page.

(4) The ElGamal system is used with modulus 79 and 39 as a primitive root. Bob publishes his public key as 33. You may use the table of powers of 3 (mod 79) below to complete the computation.

(a) What is Bob's secret key?

(b) Alice sends the message $(52, 17), (57, 14), (13, 74)$. What three letter words does this message represent? Use the encoding $A \to 0, B \to 1, C \to 2$, etc.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
3^k	1	3	9	27	2	6	18	54	4	12	36	29	8	24	72	58	16	48
k	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
3^k	65	37	32	17	51	74	64	34	23	69	49	68	46	59	19	57	13	39
k	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
3^k	38	35	26	78	76	70	52	77	73	61	25	75	67	43	50	71	55	7
k	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71
3^k	21	63	31	14	42	47	62	28	5	15	45	56	10	30	11	33	20	60
k	72	73	74	75	76	77												
3^k	22	66	40	41	44	53												

(5) Find all of the solutions to the following equations. You may use the table of powers of 3 (mod 79) on the previous page to help you.

(a) $33x \equiv 10 \ (mod\ 79)$

(b) $10^{33} \equiv x \ (mod\ 79)$

(c) $x^{11} \equiv 33 \ (mod\ 79)$

(d) $x^{33} \equiv 10 \ (mod\ 79)$

(e) Show that the equation

$$x^4 + 14x^2 + 43 \equiv 0 \ (mod\ 79)$$

has no solutions.

(6) The integer 4667875 factors into primes as $107 \cdot 349 \cdot 5^3$.

(a) Calculate $\phi(4667875)$

(b) Calculate

$$7^{3688888} \ (mod\ 4667875)$$