4. (a) Compute $J(13, 4819)$, the Jacobi symbol of 13 and 4819.

   (b) Compute $13^{2409} \bmod 4819$. (Hint: $13^{39} = 1 \bmod 4819$)

   (c) Is 4819 prime? Why or why not.

3. (a) Compute $(\frac{13}{29})$, the Legendre symbol of 13 and 29.

   (b) Is there a value x such that $x^2 = 13 \bmod 29$? Explain.

(4) Factor 69689 given that $277^2 \equiv 17529^2 \equiv 7040 \pmod{69689}$.

(5) Determine if

$$x^2 + 12x + 10 \equiv 0 \pmod{53}$$

has a solution. Hint: complete the square.

k	1	2	3	4	5	6	7	8	9	10	11	12	13
$2^k \pmod{53}$	2	4	8	16	32	11	22	44	35	17	34	15	30

k	14	15	16	17	18	19	20	21	22	23	24	25	26
$2^k \pmod{53}$	7	14	28	3	6	12	24	48	43	33	13	26	52

k	27	28	29	30	31	32	33	34	35	36	37	38	39
$2^k \pmod{53}$	51	49	45	37	21	42	31	9	18	36	19	38	23

k	40	41	42	43	44	45	46	47	48	49	50	51	52
$2^k \pmod{53}$	46	39	25	50	47	41	29	5	10	20	40	27	1

(2) Alice and Bob decided to communicate using a key arrived at from the Diffie-Hellman key exchange system. They first agree on a modulus of 53 and a primitive root of 22. Alice sends to Bob her public key of 19 and Bob sends to Alice his public key of 37. You intercept these exchanges. Use the table of powers of 2 below to help recover their secret keys S_A and S_B and their common key $22^{S_A S_B} (mod\ 53)$.

(3) Using the same primitive root and modulus, Alice sends Bob the message $(Y, Z) = (19, 39)$ using the ElGamal system. What was the message sent to Bob?

(1) Say that we use a Feistel cipher with an 8 bit input (4 left bits and 4 right bits). The f function for this cipher is given by the 8×8 lookup table below, the R bits determine the row and the key bits K determine the column and the output of $f(R, K)$ is the corresponding entry in the table.

$R \backslash K$	0	1	2	3	4	5	6	7
0	5	0	1	0	4	5	4	7
1	7	6	1	1	2	5	4	2
2	3	1	4	4	6	3	6	1
3	2	3	3	1	1	1	7	0
4	7	6	7	1	6	7	5	6
5	7	7	0	4	6	2	1	7
6	6	4	6	4	3	5	2	7
7	2	5	7	2	0	4	4	2

(a) Using as input $(L, R) = 110\ 001$ and a key of $K = 011$, determine the output of this Feistel cipher after one round.

(b) Using the key $K = 100$ you find that the output after one round of this Feistel cipher is 011 111, determine the 8 input bits.

4. Suppose we use a Knapsack encryption system with sequence

$$a = \{1, 4, 11, 23, 48\}$$

with modulus $m = 101$ and multiplier $x = 9$.

(a) Encrypt the message 10101

(b) Decrypt the message 76.