AN EXAMPLE OF BREAKING DIFFIE-HELMAN USING BABY-STEP/GIANT-STEP

(1) Alice and Bob choose to exchange a key using the Diffie-Hellman key exchange system with prime modulus 269 and primitive root 109. Bob sends to Alice the the public key 91 and Alice sends to Bob the public key 210. Use the following data to determine the private keys of Alice and Bob and the common key that they share. Note: you should also be able to use the last column of the table to compute the common key since every power of 109 will be equivalent to 109^n for some $n < 17^2$. Then $109^n \equiv 109^{r+17q} \equiv 109^r \cdot 109^{17q}$ $(mod\ 269)$ for some r and q.

k	109^k $(mod\ 269)$	$91 \cdot 109^{-17k}$ $(mod\ 269)$	$210 \cdot 109^{-17k}$ $(mod\ 269)$	109^{17k} $(mod\ 269)$
0	1	91	210	1
1	109	45	228	8
2	45	241	163	64
3	63	131	54	243
4	142	50	74	61
5	145	208	211	219
6	203	26	60	138
7	69	205	142	28
8	258	261	85	224
9	146	268	246	178
10	43	168	98	79
11	114	21	214	94
12	52	238	94	214
13	19	97	79	98
14	188	113	178	246
15	48	115	224	85
16	121	48	28	142

NB: In class I had the modulus wrong (there was a typo of 257 rather than 269). Spoiler alert!!! common key = 252.

(2) Find all solutions to the following equations. A table of powers of the primitive root 2 is given to help you in your calculations.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2^k $(mod 61)$	2	4	8	16	32	3	6	12	24	48	35	9	18	36	11
k	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
2^k $(mod 61)$	22	44	27	54	47	33	5	10	20	40	19	38	15	30	60
k	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
2^k $(mod 61)$	59	57	53	45	29	58	55	49	37	13	26	52	43	25	50
k	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
2^k $(mod 61)$	39	17	34	7	14	28	56	51	41	21	42	23	46	31	1

(a) $22x \equiv 31$ $(mod\ 61)$
(b) $10x^7 \equiv 35$ $(mod\ 61)$
(c) $10x^6 \equiv 35$ $(mod\ 61)$
(d) $x^2 + 26x \equiv 10$ $(mod\ 61)$
(e) $x^2 + 13x \equiv 20$ $(mod\ 61)$

(f) $x^2 + 13x \equiv 10 \ (mod\ 61)$
(g) $55^x \equiv 2 \ (mod\ 61)$