Crypto HW #6 -- Discrete Log Attacks

1) Please use the Baby-Step Giant-Step algorithm to solve the equations $5^x = 111$ and $5^x = 123$ in Z/167Z.

2) Please use the Pohlig-Hellman algorithm to solve the equation $7^x = 22$ in Z/151Z.

3) Please use Index Calculus with the factor base {2, 3, 5, 7} to solve the equation $5^x = 33$ in Z/167Z.

4) Please use your favorite method to break the encrypted message $(x = m*g^{ab}, g^b) = (503, 192)$ encrypted with the El Gamal Public Key $(p, g, g^a) = (647, 5, 466)$.

5) Suppose you have a personal computer which takes exactly 100 bytes to store any number of size $< 10^{200}$, has a gigabyte of internal memory, and can do about a billion multiplications per second.

   a) In about how much time can you break a well-chosen El Gamal Public key (with prime p) of size 10^{10}? of size 10^{30}?

   b) In about how much time can you break a well-chosen RSA Public Key (with n = pq) of size 10^{10}? of size 10^{30}?

   c) Which cryptosystem offers more security?

6) Please use the Chinese Remainder Theorem Algorithm to simultaneously solve the three congruences $x = 4 \pmod{49}$, $x = 11 \pmod{81}$, $x = 13 \pmod{125}$.

7) Your friend has recently learned about the RSA Cryptosystem from the internet, and knows that typically keys with n=pq of size 10^{200} offer good security. However they dream of making an awesomely unbreakable key, and so they search the internet for the largest possible prime numbers.

   a) They find that the largest known prime numbers are Mersenne primes, which are prime numbers p of the form $p = 2^k - 1$ for some k. The largest two primes are when k = 431120609 and k = 42643801. Please discuss the feasibility and security of this choice.

   b) Among the list of top 100 primes, there are also many primes of the form $p = p' * 2^k + 1$ where p' is a small prime number. The largest of these is where p' = 19249 and k = 13018586. How does allowing the use of such large primes affect the security of your RSA Key?

   c) How do (a) and (b) change if we use the El GamalCryptosystem instead of RSA?