WORKSHEET #11 – MATH 5405
SPRING 2016

Let's begin with some short answer questions.

(1) Suppose you are applying the $p-1$ method to factor a number n, using the recursive formula $a_i = a_{i-1}^i \bmod n$. What should you do with a_i in order to identify a factor of n?

(2) Draw a picture which illustrates how to add distinct points P and Q on an elliptic curve.

(3) If you are performing a quadratic sieve and discover that $x_i^2 \equiv_n 3^6 5^2$, how would you use that to find a factor of n?

(4) Suppose that $P \neq O$ is a point on an elliptic curve and that $6P = P$, what is the order of P in the elliptic curve group?

(5) Suppose Alice and Bob are using Diffie-Hellman to find a shared key. Alice chooses a prime p, generator/primitive root g and secret number a. What information will Alice share with Bob?

(6) Suppose you are given a byte (8 bits) $b_0b_1b_2b_3b_4b_5b_6b_7$. Represent it as an element of $\mathbb{F}_{2^8} = (\mathbb{Z}/2\mathbb{Z})[x]/(x^8 + x^4 + x^3 + x + 1)$ as you would if you were doing AES.

(7) The S-box in AES was constructed using the procedure. Fill in the blank. Take a byte, represent it as an element of $\mathbb{F}_{2^8}$, _____, then view it as a vector over $\mathbb{Z}/2\mathbb{Z}$ and apply a certain fixed linear transformation to it. This gives us a lookup table for where we see where every byte is sent in the S-box. What goes in the blank?

(8) How many points does the elliptic curve $y^2 = x^3 + 8$ have over the finite field $\mathbb{Z}/17\mathbb{Z}$.

(9) Use the $p+1$ method to find a factor of 15. Use the value $d=-1$ to do your work.

(10) Use Lenstra's elliptic curve method, and the elliptic curve $y^2 = x^3 + 3$ with point $P = (1, 2)$, to find a factor of 35.

(11) Use Pollard's rho (with the polynomial $x^2 + 1$) to find a factor of 15.

(12) Find all the points on the elliptic curve $y^2 = x^3 + 3$

(13) Let E be defined by $y^2 = x^3 + 3x$ over the finite field $\mathbb{Z}/5\mathbb{Z}$. Let $P = (1, 2)$. Compute $4P$.

(14) Alice is setting up an RSA encryption system. She chooses two primes $p = 3, q = 5$ so that $m = pq = 15$ and chooses $e = 5$.

(a) Compute d, the multiplicative inverse of e mod $\varphi(m)$.

(b) After publishing the numbers (m, e), Bob sends Alice the encrypted message 2. What number did Bob encrypt?

(15) Suppose Alice is setting up an ElGamal encryption system.

(a) She picks her prime $p = 7$ and generator $g = 3$. She publishes $(p, g, g^a = 6)$. Take the role of Eve and figure out what a is.

(b) Suppose Bob picks his own secret number b and sends Alice $(2 = g^b, 1 = c)$. If Bob is using ElGamal, what was the message he was sending to Alice?