Cryptography
Homework #3
Fall 2018

Due Monday, December 5

(1) For this problem you will be using RSA encryption with $\boldsymbol{n = 11522869,\ e = 717409}$

(a) Start with the message
NEVERTRUSTACOMPUTERYOUCAN'TTHROWOUTAWINDOW

Convert this into a number using ASCII code. You want to encode this, but the number is larger than *n* (which is 8 digits). Break up the number into blocks of 7 digits. Now encode each block using RSA.

(b) Decode the message and convert back to characters.

(2) Use RSA with public key $\boldsymbol{n = 1889570071}$. To guard against transmission errors Alice has Bob encodes his message twice, with different values of the encryption exponent: $\boldsymbol{e_1 = 1021763679,\ e_2 = 519424709}$. Eve intercepts the two coded messages $\boldsymbol{c_1 = 1244183534,\ c_2 = 732959706}$. Assume Eve knows all of the numbers $\boldsymbol{n, e_1, e_{2,} c_1, c_2}$. Determine the original message that Bob used.

(3) Use the Miller-Rabin test for the following numbers. If you find 10 numbers that are not Miller-Rabin witnesses then conclude that the number is probably prime.

(a) $\boldsymbol{n = 104513}$

(b) $\boldsymbol{n = 406513}$

(4) Use Pollard's *p* – 1 method to factor each of the following.

(a) 1927

(b) 220459

(5) Samantha uses a RSA signature with primes $\boldsymbol{p = 541,\ q = 1223}$ and public verification exponent $\boldsymbol{e = 159853}$.

(a) Find Samantha's public modulus and private signing key.

(b) For the digital document $\boldsymbol{D = 630579}$ what is Samantha's signature?

(6) Prove that 1105 is a Carmichael number.

(7) For the elliptic curve $\boldsymbol{y^2 = x^3 - 2x + 4}$

(a) Sketch the graph of the curve.

(b) Compute the following points: $\boldsymbol{P + Q,\ P - Q,\ 2P,\ 2Q,\ 3P}$

(c) Display these points on your graph.

(8) For the elliptic curve $\boldsymbol{y^2 = x^3 + 2x + 3}$ over $\mathbb{F}_7$.

(a) How many points are on the curve?

(b) Write an addition table for the curve.

(9) Use the double and add algorithm to compute 23*P* for the elliptic curve $\boldsymbol{y^2 = x^3 + 143x + 367}$ over $\mathbb{F}_{\mathbf{613}}$ where $\boldsymbol{P = (195,9)}$.

(10) This problem deals with elliptic Diffie-Hellman. Suppose we have an elliptic curve $\boldsymbol{y^2 = x^3 + 171x + 853}$ over $\mathbb{F}_{\mathbf{2671}}$. Use point $\boldsymbol{P = (1980,431)}$.

(a) Alice sends Bob the point $\boldsymbol{Q_A = (2110,543)}$. Bob's secret multiplier is $\boldsymbol{n_B = 1943}$.

(b) What is their shared secret key?

(c) Compute Alice's secret multiplier $\boldsymbol{n_A}$.