Summer School – Number Theory for Cryptography, Warwick
Exercises for lectures by D. J. Bernstein and T. Lange, June 24, 2013

1. Write a Sage program to do RSA encryption. Make sure to test your program on large RSA moduli to make sure you're doing the modular reductions inside the exponentiation.

2. Users A, B, C, D, and E are friends of S. They have public keys

$$\begin{aligned}(e_A, N_A) &= (5, 62857),\\ (e_B, N_B) &= (5, 64541),\\ (e_C, N_C) &= (5, 69799),\\ (e_D, N_D) &= (5, 89179),\\ (e_E, N_E) &= (5, 82583).\end{aligned}$$

   You know that S uses schoolbook RSA (no padding, no randomness). One day you observe the ciphertexts $c_A = 11529, c_B = 60248, c_C = 27504, c_D = 43997$, and $c_E = 44926$ and get the extra information that S sent the same message to all of them. What was the message?

3. The public RSA computations get faster when e is small. If proper padding is used (and thus problems as in the previous exercise are avoided) there is no harm to using small e. Small d would be dangerous – an attacker could try all small values.

   How can one use the knowledge of p and q to speed up the secret computation, i.e., the computation $x^d \pmod N$?

4. Show how to obtain m from X, Y in OAEP.

5. Alice uses the clock cryptosystem Clock($\mathbb{F}_{1000003}$) with base point $(1000, 2)$. With 30 clock additions she computed $n(1000, 2) = (947472, 736284)$ for some 6-digit n. Can you figure out n?

6. The method of sending aP, bP to establish the shared secret abP is called *Diffie-Hellman key exchange*. This method works over any group.
   The integer $p = 1009$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key exchange in a cyclic subgroup of $(\mathbb{Z}/p, +)$ with generator $g = 123$. You observe $h_a = 234$ and $h_b = 456$. What is the shared key of Alice and Bob?

7. Bosma and Lenstra proved in 1995 that "The smallest cardinality of a complete system of addition laws on E equals two". The critical step is to compute, for each addition law, a nonempty finite set Δ of points on E such that the addition law successfully adds P and Q exactly when $P - Q \notin \Delta$. How is it possible for a single addition law, the Edwards addition law, to be complete?

8. (a) How many multiplications are required for clock doubling? (b) How many of those multiplications can be squarings? (c) What about clock addition? (d) Show that Edwards doubling in $\mathbf{P}^2$ takes only $3\mathbf{M} + 4\mathbf{S}$. (e) Show that Edwards addition in $\mathbf{P}^2$ takes only $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$.

9. Curve25519 is the Montgomery curve $y^2 = x^3 + 486662x^2 + x$ modulo $2^{255} - 19$. Write a Sage function to compute $x(nP)$ given n and $x(P)$ for P on this curve. How fast is the function? Check, for random m, n, P, that computing $x(nP)$ from n and $x(P)$, and then computing $x(mnP)$ from m and $x(nP)$, produces the same result as using m and n in the opposite order. Does this check convince you that the function works?