1 Modern Cryptography

(Continued from previous notes.)

1.1 Elliptic Curve Diffie-Hellman

Suppose Alice and Bob publicly agree to fix a prime p, an elliptic curve E mod p (specified by integers a, b such that the Weierstrass equation $y^2 = x^3 + ax + b$ is nonsingular mod p), and a point $P \in E$. To ensure security, we need for $\text{ord}_P(E)$ to be large. The data (p, E, P) is all shared publicly.

Alice can choose a secret integer $0 \leq k_a < \text{ord}_E(P)$ and send Bob $Q_a = k_aP$. She can compute this value quickly using binary multiplication. Similarly, Bob can choose a secret integer $0 \leq k_b < \text{ord}_E(P)$ and send Alice $Q_b = k_bP$. Alice computes $R = k_aQ_b$ and Bob computes $R = k_bQ_a \pmod p$. The two values of R that Alice and Bob compute are the same since

$$k_aQ_b = k_a(k_bP) = k_ak_bP = k_b(k_aP) = k_bQ_a.$$

Thus, Alice and Bob now share a secret point R on the elliptic curve.

(Exercise.) Suppose Alice and Bob publicly agree to use the elliptic curve $y^2 = x^3 + 17 \pmod p = 7$ and the point $P = (1, 2)$.

(a) Suppose Alice picks the number $k_a = 4$. What is the message Q_a that she sends Bob?

We know that

$$Q_a = k_aP = 4P.$$

Given this, we need to compute $4P$. Let's begin with $2P = P + P$. We know that $P = P$ and $y_1 = 2$ is invertible mod 7, so we define

$$\lambda = (3(1)^2 + 0)(2(2))^{-1} \pmod 7 = (3)((4)^{-1} \pmod 7).$$

Computing the inverse of 4 mod 7 gives us 2, so

$$\lambda = 3(2) \pmod 7 = 6 \pmod 7.$$

Then, we have

$$\nu = 2 - 6(1) = -4 \pmod 7 = 3$$

$$x_3 = 6^2 - 1 - 1 = 34 \pmod 7 = 6$$

$$y_3 = 6(6) + 3 = 39 \pmod 7 = 4.$$

Therefore, we can define $R = (6, 4)$ and thus $P + P = -R = (6, -4 \pmod 7)) = (6, 3)$. Now that we have $2P$, we can compute $4P = 2P + 2P$. We know that $y_1 = 3$ is invertible mod 7, so

$$\lambda = (3(6)^2 + 0)(2(3))^{-1} \pmod 7 = (108)(6)^{-1} \pmod 7.$$

Computing the inverse of 6 mod 7 gives us 6, so

$$\lambda = 108(6) \pmod 7 = 4.$$

Then, we have

$$\nu = 3 - 4(6) \pmod 7 = 0$$

$$x_3 = 4^2 - 6 - 6 \pmod 7 = 4$$

$$y_3 = 4(4) + 0 \pmod 7 = 2.$$

Therefore, we can define $R = (4, 2)$ and thus $2P + 2P = -R = (4, -2 \pmod 7)) = (4, 5)$.

(b) Suppose Alice receives the point $Q_b = (5, 3)$ from Bob. What is her shared secret with Bob?

We know that
$$R = k_a Q_b = k_a(5, 3).$$

(Exercise.) Suppose Alice and Bob publicly agree to use the elliptic curve $y^2 = x^3 + 17 \pmod{p} = 7$ and the point $P = (1, 2)$. This point has order 13, which is too small to be secure. Suppose Eve intercepts Alice and Bob's message: she sees that Alice sent Bob $Q_a = (3, 3)$ and that Bob sent Alice $Q_b = (6, 4)$. What is Alice and Bob's shared secret?

1.2 Interlude: Quadratic Residues

A familiar feature of the real numbers is that some numbers do not have square roots (e.g., the negatives). The same thing happens when you mod an integer. For example, let $n = 5$. We know that the integer is congruent to 0, 1, 2, 3, or 4 mod 5. This means that any square must be congruent to $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 \equiv 4 \pmod 5$, or $4^2 \equiv 1 \pmod 5$. In other words, only 0, 1, or 4 have square roots mod 5, and 2 and 3 do not.

Definition 1.1: Quadratic Residue

Fix a positive integer n. We say that an integer a is a **quadratic residue mod** n if it has a square root mod n, i..e, if there exists an integer x such that $x^2 \equiv a \pmod n$.

(Exercise.) Find all quadratic residues mod the following integers.

(a) $n = 3$

(b) $n = 7$

(c) $n = 11$

We'll see below that it will be useful to quickly determine whether an integer a is a quadratic residue mod a prime $p \geq 3$. It turns out that there is a good way to do this; let's introduce the following notation.

Definition 1.2: Legendre Symbol

Let $p \geq 3$ be prime. For any integer a, define the Legendre symbol (a/n) by

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod p \\ 1 & \text{if } a \not\equiv 0 \pmod p \text{ and } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \not\equiv 0 \pmod p \text{ and } a \text{ is not a quadratic residue mod } p \end{cases}$$

For example, we saw above that 4 is a quadratic residue mod 5, so

$$\left(\frac{4}{5}\right) = 1$$

and we saw that 2 is not a quadratic residue mod 5, so

$$\left(\frac{2}{5}\right) = -1.$$

We can now rephrase our goal: we would like a quick way of computing Legendre symbols. This is provided to us by combining binary exponentiation with the following:

Lemma 1.1: Euler's Criterion

Let $p \geq 3$ be prime. For any integer a,

$$\left(\frac{a}{n}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Euler's Criterion means that we have an efficient algorithm for determining whether something is a quadratic residue: we simply use binary exponentiation to compute $a^{(p-1)/2} \pmod{p}$ and we can read off the answer.

(Example.) Suppose we want to know if $a = 37$ is a quadratic residue mod $p = 97$. We have $(p-1)/2 = 96/2 = 48$, so we compute $a^{(p-1)/2} = 37^{48} \pmod{97}$ using binary exponentiation, and we find that it is $96 \equiv -1 \pmod{97}$. Euler's Criterion says that

$$\left(\frac{37}{97}\right) \equiv 37^{(97-1)/2} = 37^{48} \equiv -1 \pmod{97}.$$

Therefore, 37 is not a quadratic residue mod 97.

(Exercise.) Use Euler's Criterion to determine whether or not the following integers a are quadratic residues mod $p = 19$.

(a) $a = 3$

(b) $a = 5$

(c) $a = 11$

1.3 Elliptic Curve Elgamal

There is a variant of the Elgamal cryptosystem using elliptic curves that can be used to exchange messages, but there is a nontrivial encoding step. To make Elgamal work with elliptic curves, we first need a way to encode a plaintext message as a point on an elliptic curve E mod p.

For this, there's a probablistic algorithm that encodes plaintext as x-coordinate of a plain (but note that not every integer will occur as the x-integer of a point on an elliptic curve mod p). Specifically, if E is given by $y^2 = x^3 + ax + b$ and if $P = (x, y)$ is a point on the curve, then the x-coordinate must have the property that $x^3 + ax + b$ is a quadratic residue mod p.

1.3.1 The Process

Suppose Bob wants to receive messages of length N.

1. Bob will fix a positive integer s. We'll see that, the larger Bob chooses the integer, the higher the probability that encoding will succeed.

2. Bob will then choose a prime $p > s26^N$ and an elliptic curve E mod p (defined by integers a, b such that the integral Weierstrass equation $y^2 = x^3 + ax + b$ is nonsingular mod p), and a point $P \in E$.
3. He then computes $\text{ord}_E(P)$.
4. Then, Bob chooses a secret integer $0 \leq k < \text{ord}_E(P)$ to serve as his private key. He computes $Q = kP$, and this value is part of his public key.

In other words, Bob will share all of the data $(s, E, P, \text{ord}_E(P), Q)$ publicly, and keep only the integer k secret.

Suppose now that Alice wants to send Bob a message.

1. She converts her message into an integer m using the same base 26 idea we used for RSA.
2. She will then iterate through values of $r = 0, 1, 2, \ldots, s - 1$ until she finds the first value of $x = sm + r$ such that[1]
$$\left(\frac{x^3 + ax + b}{p}\right) \neq -1.$$
Note that the maximum possible value of m is $26^N - 1$, so
$$x = sm + r < s(26^N - 1) + s = s26^N < p$$
since Bob chose p to be larger than $s26^N$. There is a roughly $1/2$ chance that an integer in $[0, p)$ is not a quadratic residue mod p, and here we are iterating through s integers in the range $[0, p)$, so there is a $\left(\frac{1}{2}\right)^s$ chance that $x^3 + ax + b$ is not a quadratic residue for any of the s possible values of $x = sm + r$. If none of the s integers are quadratic residues, encoding fails. However, if Bob chose s to be even moderately large, encoding failure is very unlikely. If encoding does fail, Alice can just modify her message slightly[2] and try encoding again.
3. Once Alice finds a value of x such that $x^3 + ax + b$ is a quadratic residue mod p, then there is an integer y such that $y^2 \equiv x^3 + ax + b \pmod{p}$, so the point $M = (x, y)$ is on E. This will be the <u>encoding</u> of her plaintext.

This is not the ciphertext, but she can now encrypt the encoded message using a process very similar to the Elgamal cryptosystem we discussed earlier.

1. First, Alice chooses an "ephemeral key" h such that $0 \leq h < \text{ord}_E(P)$.
2. She computes $S = hQ$, $R_1 = hP$, and $R_2 = M + S$. The pair, (R_1, R_2), is the ciphertext she sends to Bob.

To decrypt the ciphertext (R_1, R_2), Bob uses his private key k to compute $S = kR_1$. Observe that
$$kR_1 = k(hP) = khP = h(kP) = hQ,$$
so Bob has found the same value of S that Alice had, even though he does not know the value of the ephemeral key h. He can then compute $-S$ by negating the y-coordinate, and he then calculates
$$R_2 - S = R_2 + (-S) = (M + S) + (-S) = M + (S + (-S)) = M + O = M.$$
He has thus recovered Alice's encoded plaintext.

Finally, Bob just needs to decode M. If $M = (x, y)$, he can extract the first coordinate x. The quotient when he divides this by s is the integer m that represents the message in base 26, so he then finishes off by converting back to text using the same process we used for RSA above.

1.3.2 Encoding and Decoding

[1] Remember that this is the **Legendre Symbol**!
[2] Rephrasing slightly or adding a nonsense letter.

(Exercise.) Suppose Bob's public key has $s = 2$, $p = 97$, $a = 31$, and $b = 20$. The elliptic curve E is then the one given by $y^2 = x^3 + 31x + 20 \pmod{p = 97}$.

(a) What is the encoding of the plaintext message `B`? Follow the process above to find the corresponding point $M \in E$.

First, we encode `B` into base 26; this gives us $m = 1$. Then, we need to iterate through all r such that $0 \leq r \leq 2 - 1 = 1$. We find that

- For $r = 0$, we have $x = 2(1) + 0 = 2$ and
$$\begin{aligned}\left(\frac{2^3 + 31(2) + 20}{97}\right) &= \left(\frac{90}{97}\right) \\ &= 90^{\frac{97-1}{2}} \pmod{97} \\ &= 90^{\frac{96}{2}} \pmod{97} \\ &= 90^{48} \pmod{97}.\end{aligned}$$
With this in mind, we find that $90^{48} \equiv 96 \equiv -1 \pmod{97}$, so $r = 0$ is not an option.
- For $r = 1$, we have $x = 2(1) + 1 = 3$ and
$$\begin{aligned}\left(\frac{3^3 + 31(3) + 20}{97}\right) &= \left(\frac{140}{97}\right) \\ &= 140^{\frac{97-1}{2}} \pmod{97} \\ &= 140^{48} \pmod{97} \\ &= 1 \pmod{97}.\end{aligned}$$
Here, we find that $r = 1$ and thus $x = 3$ *is* the option.

Now that we have $x = 3$, we can compute
$$y^2 \equiv 3^3 + 31(3) + 20 \pmod{97}.$$
We find that $y \equiv 25$. Thus,
$$M = (3, 25).$$

(b) Show that the encoding fails for the letter `K`.

Encoding `K` gives us $m = 10$. Then, iterating through all $0 \leq r \leq 2 - 1 = 1$, we have

- For $r = 0$, we have $x = 2(10) + 0 = 20$ and

$$\begin{aligned} \left(\frac{20^3 + 31(20) + 20}{97}\right) &= \left(\frac{8640}{97}\right) \\ &= 8640^{\frac{97-1}{2}} \pmod{97} \\ &= 8640^{48} \pmod{97} \\ &= 7^{48} \pmod{97} \\ &= 96 \pmod{97}. \end{aligned}$$

  This gives us $8640^{48} \equiv 96 \equiv -1 \pmod{97}$, so $r = 0$ is not an option.

- For $r = 1$, we have $x = 2(10) + 1 = 21$ and

$$\begin{aligned} \left(\frac{21^3 + 31(21) + 21}{97}\right) &= \left(\frac{9933}{97}\right) \\ &= 9933^{\frac{97-1}{2}} \pmod{97} \\ &= 9933^{48} \pmod{97} \\ &= 39^{48} \pmod{97} \\ &= 96 \pmod{97}. \end{aligned}$$

  Once again, this gives us $9933^{48} \equiv 96 \equiv -1 \pmod{97}$, so $r = 1$ is not an option.

Because we got -1 for all valid r, encoding is not possible.

(c) Follow the process described above to find the plaintext message that results from decoding the point $(25, 30) \in E$.

TODO