Week 10 Tuesday

Summer Plans

Make sure you know your neighbors' names. Then discuss briefly:

What plans do you have for the summer? (It doesn't have to be just work or academic plans; feel free to discuss leisure plans!)

Reminder

We'll have some time for review on Thursday. If you have requests for topics you want to see, please mention them on Zulip under the topic `w10thu review requests`.

Elliptic Curve Diffie-Hellman

1. Alice and Bob agree to do a Diffie-Hellman key exchange with the elliptic curve mod $p = 11$ given by $y^2 = x^3 + x + 3$, using the point $P = (5, 1)$, which has order 18.

Alice must pick a secret integer a. From which range should this secret integer be chosen?

(A) $0 \leqslant a < 5$

(B) $0 \leqslant a < 11$

(C) $0 \leqslant a < 18$

(D) None of the above

2. Alice and Bob agree to do a Diffie-Hellman key exchange with the elliptic curve mod $p = 11$ given by $y^2 = x^3 + x + 3$, using the point $P = (5, 1)$, which has order 18.

Alice picks the secret integer $a = 11$. What does she send Bob?

(Just write down *a thorough outline* of how she'll do this calculation. You don't need to do this calculation out in full by hand; just convince yourself you know what all of the steps are and exactly what each step will look like.)

3. Alice and Bob agree to do a Diffie-Hellman key exchange with the elliptic curve mod $p = 11$ given by $y^2 = x^3 + x + 3$, using the point $P = (5, 1)$, which has order 18.

Alice picks the secret integer $a = 11$. She receives $Q_b = (10, 10)$ from Bob. What is her shared secret with Bob?

(Again, just write down *a thorough outline* of how she'll do this calculation.)