CIS 3362 11/8/24

- analog of the Diffie-Hellmen Key Exchange via Elliptic Curves
- analog of the El Gamel Cryptosystem via Elliptic Curves
- online compiles to go through rest of the code

11/11 MON - VETERANTS DAY (NO CLASS)

11/13 WED - QUANTUM CRYPTO (CODE BOOK)

11/15 FRI - QUIZ 5 (JACOB + TRISTAN)

El Gamel via E.C.

Alice creates her private + public keys:

Public

Public elem
- $E_p(a,b)$
- G - point
- n - order

$n \times G = O$

Alice

Private key $1 < n_A < n$.

Public key $=$

Public key $= P_A = n_A \times G$.

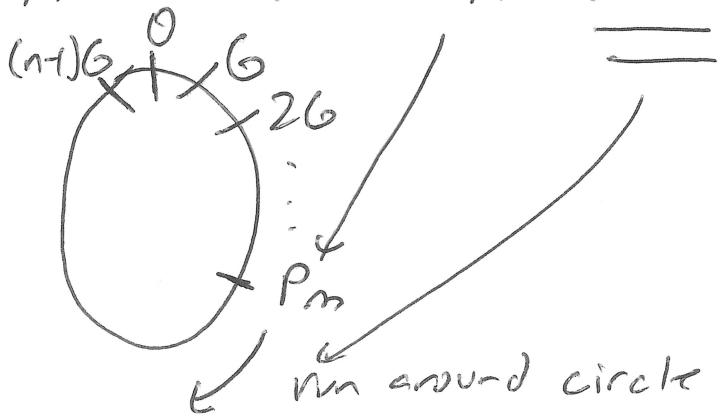
P_A: known but it's hard to figure out n_A.

G: known

Bob wants to send message to Alice

1. Bob Picks int $k < n$.
2. $C_1 = k \times G$ } if you know C_1, G, k is still difficult to figure out.
3. Let Plaintext message be P_m
4. $C_2 = P_m + k \times P_A$ → alice's public key
5. Bob sends (C_1, C_2).

$$C_2 = P_m + k \times P_A = P_m + (k \times n_A) \times G$$



To recover Plaintext, we must subtract $(k \times n_A) \times G$.

Notice $C_1 = k \times G$, so $n_A \times C_1 = (n_A \times k) \times G$
$= (k \times n_A) \times G$

Alice does $C_2 - n_A C_1 \Longrightarrow P_m$

$C_2 - n_A C_1 = P_m + k \times P_A - n_A C_1$
$= P_m + \underline{k \times n_A \times G} - \underline{n_A \times k \times G}$ } cancel
$= P_m$

We'll do an example with
$E_{23}(1,1)$, $G = (3,10)$, cycle info
6, 26, 36, ... 280
is in typed notes

Alice uses $n_A = 13$

Alice posted $P_A = 13 \times G = (1,7)$ from chart

Bob to send MSG

$P_m = MSG = (16,20)$ (116)

$k = 17 \longrightarrow$ $C_1 = 17G = (18,3)$ from chart

$C_2 = P_m + 17 \times (1,7)$

$= 116 + (17 \times 13) \times G$

$= 116 + 2216 = 2326$

$= 86 = (13,16)$

$28 \overline{)232}$ 8 R8
-224
8

Alice receives $C_1 = (18,3)$, $C_2 = (13,16)$

$C_2 - n_A \times C_1 = 86 - 13 \times 17G$

$= 86 - 221G$

$= -2136$

$= \boxed{116}$

$221 \equiv 8$

280
213
67
-56

Elliptic Curve Cryptography

Analog of Diffie-Hellman Key Exchange

We can use elliptic curves to exchange keys, very similar to the Diffie-Hellman Key Exchange.

The first public key will be an elliptic curve $E_p(a, b)$, for a large prime number p.

Next, pick a base point $G = (x_1, y_1)$ which has a very large order, n, on the curve. As you might expect, the order of a point, G, is the smallest positive integer n such that $nG = 0$, where 0 is the origin point.

Both the curve and the base point are the public keys for the system.

Alice and Bob can exchange keys as follows:

Alice picks a secret value $n_A < n$ and sends Bob the point $n_A \times G$.

Bob picks a secret value $n_B < n$, and sends Alice the point $n_B \times G$.

Alice takes the point Bob sends her and multiplies it by n_A.
Bob takes the point Alice sends her and multiplies it by n_B.

After this, both Alice and Bob have $n_A \times n_B \times G$ as their shared key.

Similar to the discrete log problem, when Eve sees either $n_A \times G$ or $n_B \times G$, she can not determine either n_A or n_B. Similarly, she can't use the two values $n_A \times G$ and $n_B \times G$ together to combine in some way to create $n_A \times n_B \times G$.

In class, we looked at the Elliptic Curve $E_{23}(1, 1)$ using the point P = (3, 10) as a base point. We found out that this point had order 28. Below is a list of each number from 1 to 28 multiplied by point P. The number to the left of the point represents what we are multiplying by:

1. (3, 10)
2. (7, 12)
3. (19, 5)
4. (17, 3)
5. (9, 16)
6. (12, 4)
7. (11, 3)
8. (13, 16)
9. (0, 1)
10. (6, 4)
11. (18, 20)
12. (5, 4)
13. (1, 7)
14. (4, 0)
15. (1, 16)
16. (5, 19)
17. (18, 3)
18. (6, 19)
19. (0, 22)
20. (13, 7)
21. (11, 20)
22. (12, 19)
23. (9, 7)
24. (17, 20)
25. (19, 18)
26. (7, 11)
27. (3, 13)
28. (0, 0)