A sample communication with the elliptic curve version of El Gamal cryptosystems

- Alice chooses finite field: $\mathbb{F}_5$.
- Alice chooses basepoint $B = (1,2)$

$\Rightarrow y^2 = x^3 + ax + b$ with $x = 1$, $y = 2$

Alice tries $a = 1$:

$$b = y^2 - x^3 - ax = 4 - 1 - 1 = 2$$

$$4a^3 + 27b^2 = 4 + 27 \cdot 4 = 112 \not\equiv 0 \text{ in } \mathbb{F}_5$$

$\Rightarrow$ Alice has found the elliptic curve $y^2 = x^3 + x + 2$ over $\mathbb{F}_5$, and sends it to Bob, together with $B = (1,2)$.

- Alice chooses secret number $A = 2$, Bob chooses secret key $k = 4$

- Alice computes public key $A \cdot B = 2 \cdot B = B + B$

$$x_3 = \left(\frac{3 \cdot 1^2 + 1}{2 \cdot 2}\right)^2 - 2 \cdot 1 = -1 \equiv 4 \bmod 5$$

$$y_3 = -y_1 + \frac{3x_1^2 + a}{2y_1}(x_1 - x_3) = -2 + \frac{3 \cdot 1^2 + 1}{2 \cdot 2}(1 - 4) \equiv 0 \bmod 5,$$

sends $(4,0)$ to Bob, as her public key.

- Bob computes his public key, $k \cdot B$ $= 4B = 2B + 2B = (x_3, y_3)$ with

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 = \frac{3 \cdot 4^2 + 1}{2 \cdot 0} - 2 \cdot 4 = \mathcal{O}$$

This public key is unsafe, because it will encipher clear text to clear text!

So Bob chooses a new secret key, $k = 3$.

Bob computes his public key, $k \cdot B = 3 \cdot B = 2B + B$,

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 = \left(\frac{2-0}{1-4}\right)^2 - 4 - 1$$

As $\frac{2}{-3} \equiv \frac{2}{2}$ in $\mathbb{F}_5$, $x_3 = 1$.

$$y_3 = -y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) = 0 + \frac{2-0}{1-4}(4-1) = 3$$

and sends $(1,3)$ to Alice.

- Bob computes the common secret key,

$$k \cdot (A \cdot B) = k \cdot (4,0) = 3 \cdot (4,0) = (4,0) + \underbrace{((4,0) + (4,0))}_{4B = \mathcal{O}}$$

$$= \underline{\underline{(4,0)}}.$$

- A sample message block of Bob is $\mathcal{O}$.

Bob sends $P_m + k \cdot (A \cdot B) = \mathcal{O} + (4,0) = (4,0)$.

- Alice deciphers the message block with her secret key $A = 2$:

$$
\begin{aligned}
2\cdot(\text{public key of Bob}) &= 2\cdot(1,3)\\
&= 2\cdot(-(1,2))\\
&= -2\cdot(1,2)\\
&= -(4,0)\\
&= (4,0)\\
&= \text{common secret key}
\end{aligned}
$$

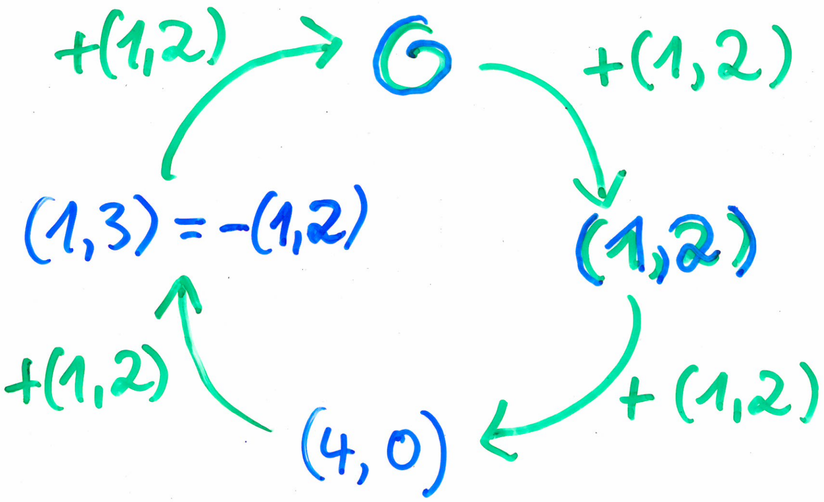
- Alice substracts the common secret key from the cipherblock $P_m + k\cdot(A\cdot B)$:

$$(4,0) - (4,0) = \mathcal{O}.$$

Note that the point $\mathcal{O}$ at the horizon is allowed as a message block, but not as a public key.

<u>Homework</u>: Encipher the above communication by starting with the parameter $a = 2$, and then going through all of the above steps. If you obtain $\mathcal{O}$ as a public key, then change the secret number on its side.

Group structure of Alice's curve



The curve $y^2 = x^3 + x + 2$ over $\mathbb{F}_5$.
It has structure C_4.

Permutations of the points on the curve obtained with the possible keys:

Element of alphabet	$\mathcal{O}$	$(1,2)$	$(4,0)$	$(1,3)$
Encrypted by $+(1,2)$	$(1,2)$	$(4,0)$	$(1,3)$	$\mathcal{O}$
Encrypted by $+(4,0)$	$(4,0)$	$(1,3)$	$\mathcal{O}$	$(1,2)$
Encrypted by $+(1,3)$	$(1,3)$	$\mathcal{O}$	$(1,2)$	$(4,0)$

Decryption is done using the inverse (negative) of the encryption point. The point $\mathcal{O}$ appears in the alphabet, but must not be used as encryption key.

Of course, we need curves with much more points to construct a reasonable cryptosystem.