Elliptic Curve Diffie-Hellman (ECDH) Key Exchange

A selects an integer X_A to serve as his/her private key. A then generates $Y_A = X_A \times G$ to serve as his/her public key. A makes publicly available the public key Y_A.

B designates an integer X_B to serve as his/her private key. As was done by A, B also calculates his/her public key by $Y_B = X_B \times G$.

In order to create a shared secret key (that could subsequently be used for, say, a symmetric-key based communication link), both A and B now carry out the following operations:

– A calculates the shared session key by

$$K = X_A \times Y_B$$

– B calculates the shared session key by

$$K = X_B \times Y_A$$

$$
\begin{aligned}
K \text{ as calculated by } A &= X_A \times Y_B \\
&= X_A \times (X_B \times G) \\
&= (X_A \times X_B) \times G \\
&= (X_B \times X_A) \times G \\
&= X_B \times (X_A \times G) \\
&= X_B \times Y_A \\
&= K \text{ as calculated by } B
\end{aligned}
$$

$$y^2 \equiv x^3 + 2x + 9 \pmod{23}$$

$G = (0,3)$
$X_A = 3$
$X_B = 11$

$Y_A = 3 \times (0,3) = (8,10)$
$Y_B = 11 \times (0,3) = (4,14)$

$K = X_A P_B = 3 \times (4,14) = (5,12)$
$K = X_B P_A = 11 \times (8,10) = (5,12)$

$G = (19,11)$
$X_A = 8$
$X_B = 15$

$X_A = 15$
$X_B = 8$

$X_A = 7$
$X_B = 6$

K-?