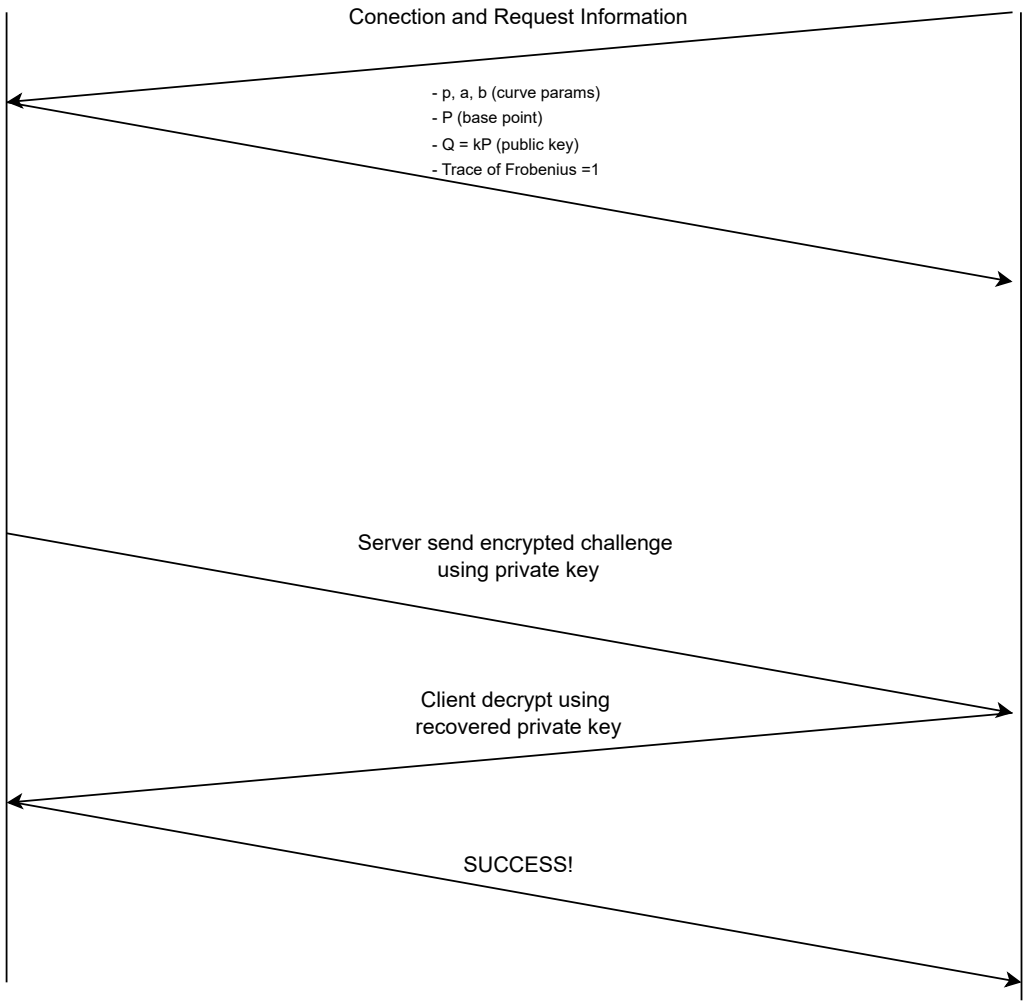
Server
ECC Curve Trace of Frobenius = 1
Server generates:
- private key (k)
- public key (Q = kP)

Client



Step 1: Vulnerability Check:
- Verify trace of Frobenius = 1
=> Curve is vulnerable!

Step 2: Lift to p-adic field
$E \rightarrow E(Q_p)$
$P \rightarrow P' \in E(Q_p)$

Step 3: Scale Points
$G' = pP'$
$Q' = pQ'$

Step 4: Compute Discrete Log
$k = (Q'_x/Q'_y)/(G'_x/G'_y)$

=> private key (k) recovered

Step 5: Verification
Check: kP=Q