Example 4 — A Tiny Ed25519 World

Understanding elliptic-curve signatures on a toy scale

—

1. Background: What Ed25519 Really Does

Ed25519 isn't used for encryption like RSA — it's used for **digital signatures**. That means you can:

- Prove you wrote a message (authenticity),
- Prove it hasn't been changed (integrity),
- Do it without sharing your private key (non-repudiation).

Ed25519 builds on **elliptic-curve math**, which feels weird at first, but here's the idea: you pick a point G on a special curve, and your public key is just

$$A = k \times G,$$

where k is your private number.

—

2. The Tiny Curve Playground (Toy Example)

To make this idea visible, let's imagine a miniature "curve world" where we work modulo 17. (Real Ed25519 works modulo $2^{255} - 19$ — a massive prime — but ours will fit on one page.)

$$\text{Field size: } p = 17$$

We'll use the simple curve equation:

$$y^2 = x^3 + 2x + 2 \pmod{17}.$$

—

3. The Base Point G

In our world, one valid point on this curve is:

$$G = (5, 1)$$

We'll use G as the "starting point" for all public keys.

—

4. Generating a Key Pair

Let's choose a private key:

$$k = 7$$

Then compute:

$$A = k \times G$$

In the real Ed25519 algorithm, $k \times G$ means adding G to itself k times on the curve. We'll imagine this as taking "steps" on a circular track — every step depends on the curve's shape.

After adding G to itself 7 times, we reach:

$$A = (6, 3)$$

$$\boxed{\text{Private key } k = 7, \quad \text{Public key } A = (6, 3)}$$

—

5. Signing a Message

Let's sign the message "OK".

1. Hash the message: $H(\text{OK}) = 5$ (toy example). 2. Pick a random number $r = 4$. 3. Compute $R = r \times G = 4 \times (5, 1) = (9, 16)$. 4. Compute challenge $h = H(R, A, \text{OK}) = 2$. 5. Compute $S = r + h \times k = 4 + 2 \times 7 = 18 \equiv 1 \pmod{17}$.

$$\boxed{\text{Signature } (R, S) = ((9, 16), 1)}$$

—

6. Verifying the Signature

Anyone can verify without knowing k:

1. Compute $h = H(R, A, \text{OK}) = 2$. 2. Check if:

$$S \times G \stackrel{?}{=} R + h \times A$$

Left side:

$$S \times G = 1 \times G = (5, 1)$$

Right side:

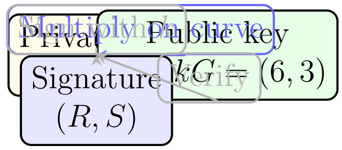
$$R + hA = (9, 16) + 2 \times (6, 3) = (5, 1)$$

They match!

$$\boxed{\text{Signature valid}}$$

—

7. Diagram: Key Generation and Signing Flow



—

8. What's Different from RSA?

— Feature — RSA — Ed25519 — ————-——————-— — Math idea — Multiplying and factoring — Adding points on a curve — — Security base — Integer factorization — Discrete logarithm on a curve — — Used for — Encryption & signatures — Signatures (auth + integrity) — — Key size — 2048–4096 bits — 256 bits — — Speed — Slower (big exponents) — Faster (curve arithmetic) — — Quantum resistance — Weak — Stronger (still vulnerable, but better) —

—

9. The Heart of the Matter

RSA says: ¿ "It's hard to go from n back to its prime factors."

Ed25519 says: ¿ "It's hard to go from A back to k when $A = kG$."

In both cases, you know the answer goes one way easily, but not backward. That's the soul of asymmetric cryptography — one-way doors that only the right key can open.

—

10. Final Thought

Elliptic curves are the poetry of number theory: smooth shapes hiding impossible problems. Where RSA uses massive steel walls, Ed25519 uses geometry — lightweight, elegant, and just as unbreakable (for now).

"RSA is arithmetic. Ed25519 is geometry. Both are trust made visible."