Public Key Cryptography

Two public-key algorithms:

both with relatively large key sizes!

Diffie-Hellman

Relies on the difficulty of the **discrete logarithm problem**

RSA

Relies on the difficulty of **prime factorization**

In part, keys must be large because we know a lot about these problems

Elliptic Curve Cryptography

An elliptic curve is defined by a formula

$$y^2 = x^3 + \mathrm{A}x + \mathrm{B}$$

or sometimes

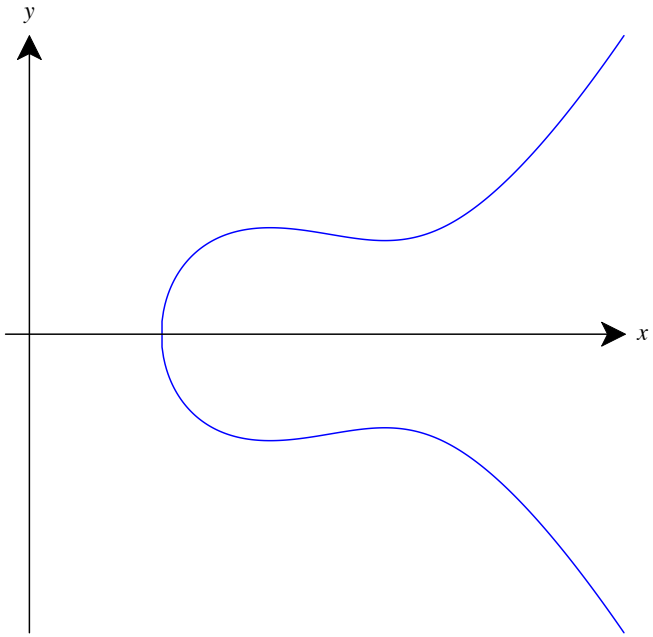
$$y^2 = x^3 + \mathrm{A}x^2 + \mathrm{B}x + \mathrm{C}$$

or even more generally

$$y^2 + \mathrm{D}yx = x^3 + \mathrm{A}x^2 + \mathrm{B}x + \mathrm{C}$$

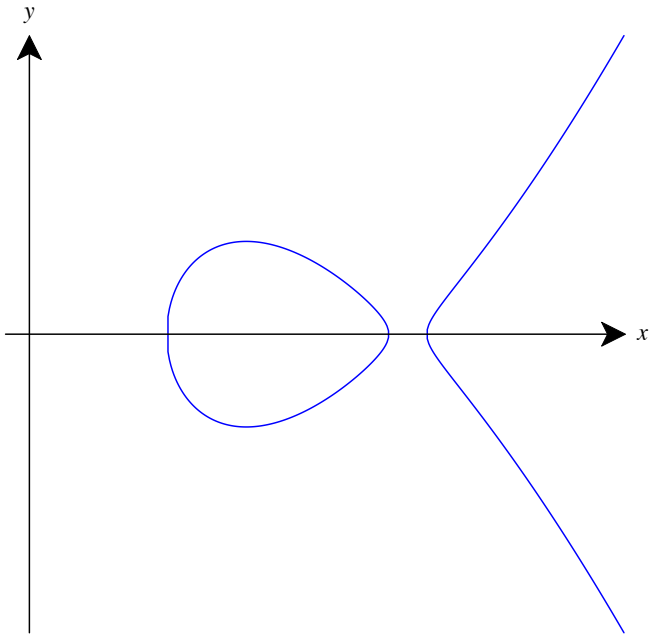
Elliptic Curves

$$y^2 = x^3 - x + 3$$



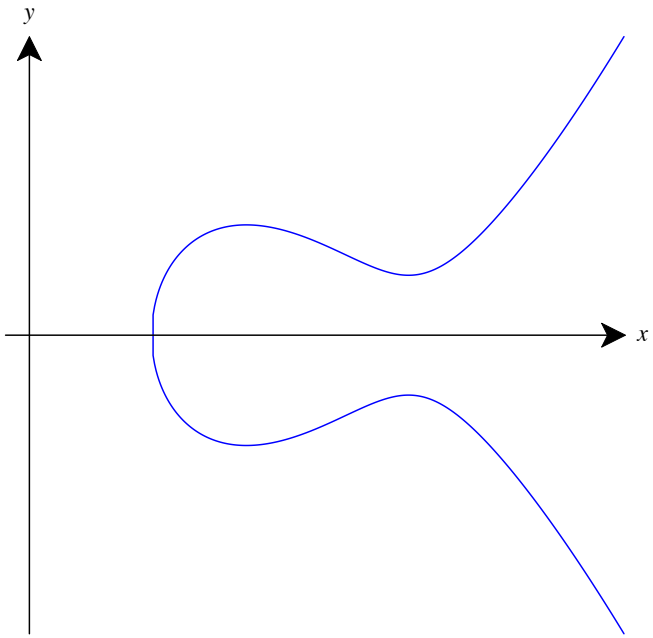
Elliptic Curves

$$y^2 = x^3 - 2x + 1$$

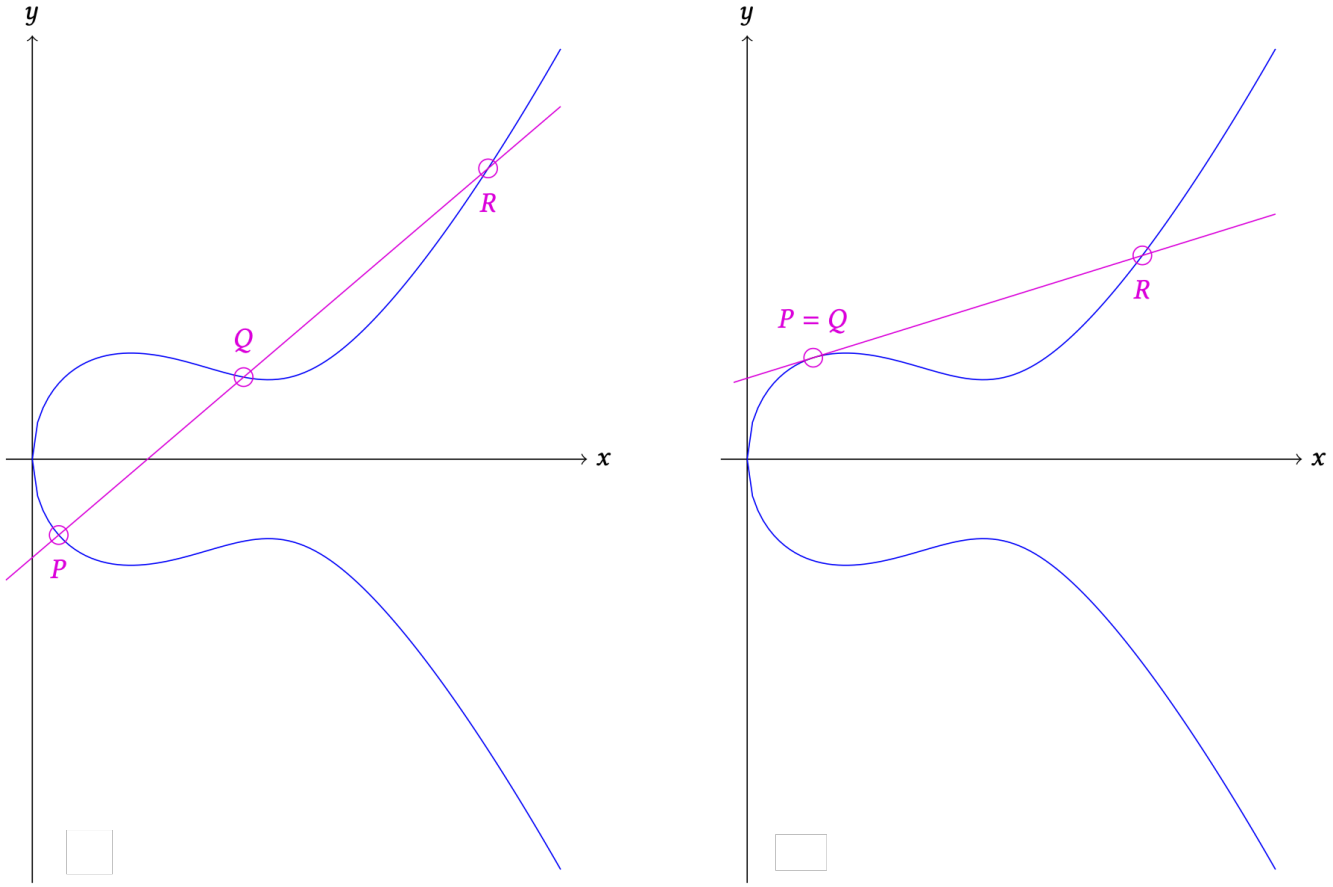


Elliptic Curves

$$y^2 = x^3 - 2x + 2$$

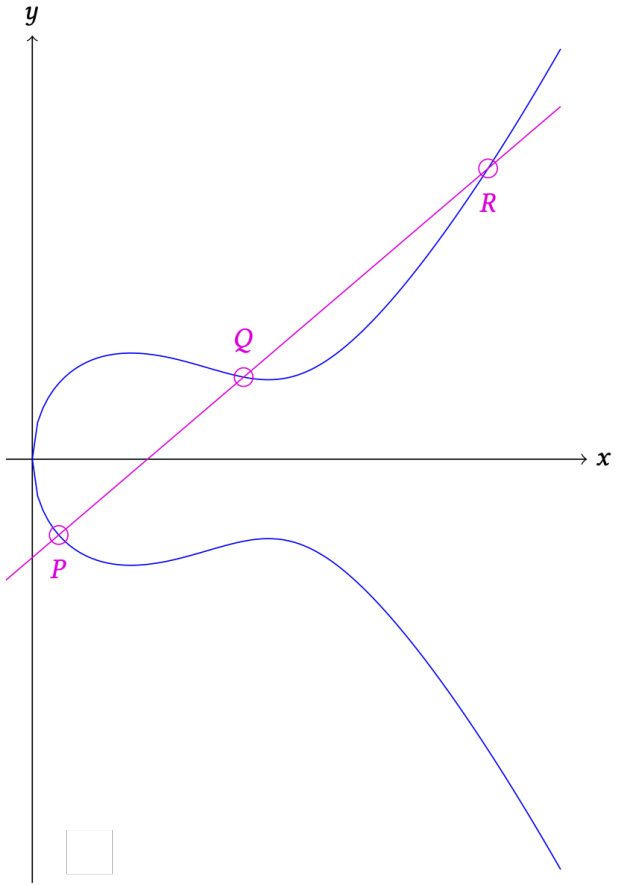


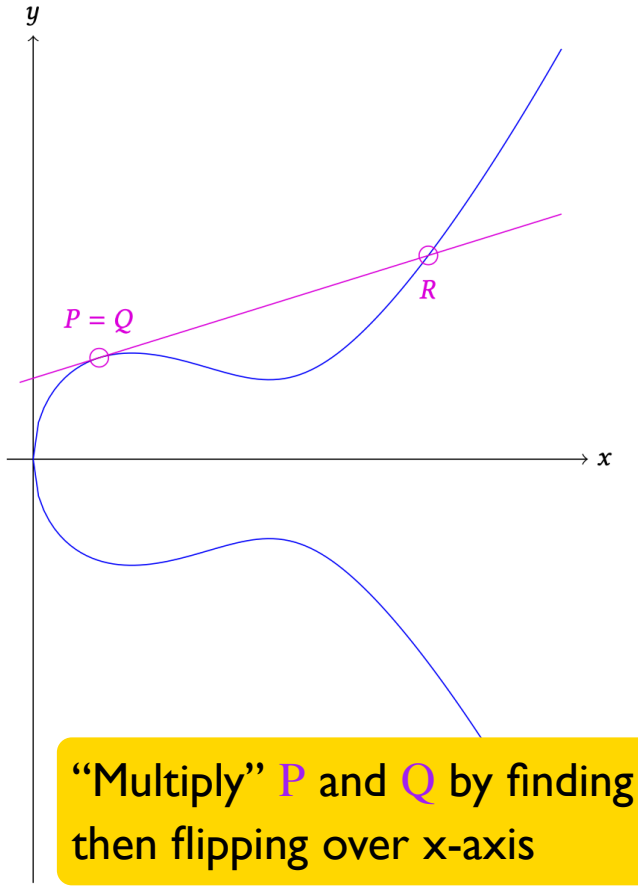
P and Q to R on an Elliptic Curve



Martin Kleppmann, "Implementing Curve25519/X25519: A Tutorial on Elliptic Curve Cryptography"

P and Q to R on an Elliptic Curve

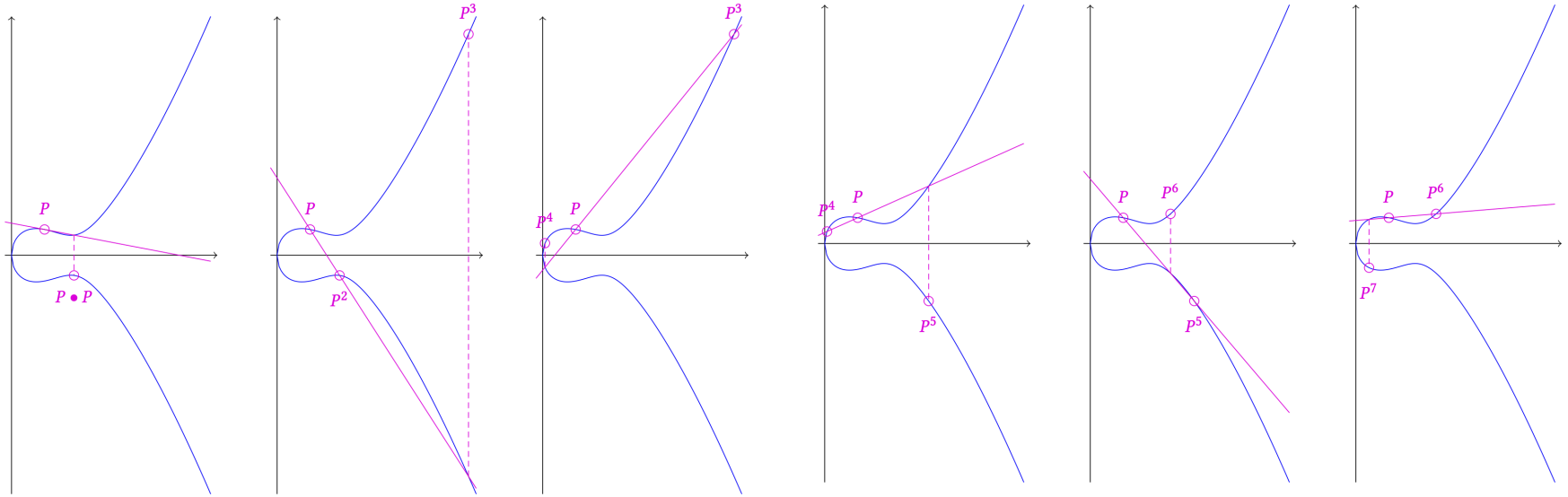




"Multiply" P and Q by finding R, then flipping over x-axis

Martin Kleppmann, "Implementing Curve25519/X25519: A Tutorial on Elliptic Curve Cryptography"

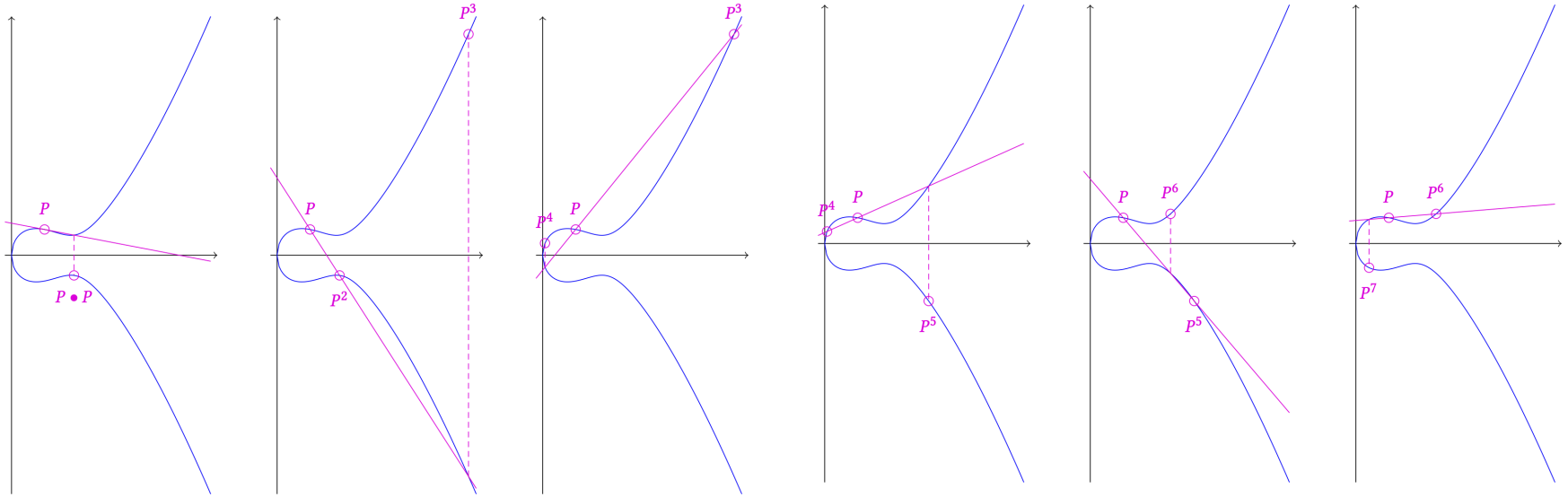
Power of P on an Elliptic Curve



Pictures show intuition with the field $\mathbb{R}$ of real numbers

To actually compute: use a discrete, finite field with modulo integers

Power of P on an Elliptic Curve



Using the finite field, taking N steps to get P^N is fast,
but reversing from P^N back to N is infeasible

Elliptic Curve Diffie-Hellman (ECDH)

Alice's secret key is a, public key is $A = P^a$

Bob's secret key is b, public key is $B = P^b$

P followed by a steps followed by b steps

=

P followed by b steps followed by a steps

A followed by b steps

=

B followed by a steps

Some Standard Curves

prime192v1 $y^2 = x^3 + Ax + B$

A = `0xfffffffffffffffffffffffffffffffefffffffffffffffc`

B = `0x64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1`

sect193r2 $y^2 + yx = x^3 + Ax^2 + B$

A = `0x0163f35a5137c2ce3ea6ed8667190b0bc43ecd69977702709b`

B = `0x00c9bb9e8927d4d64c377e2ab2856a5b16e3efb7f61d4316ae`

K-283 $y^2 + yx = x^3 + B$

$B = 1$

X25519

Curve25519 is defined as $y^2 = x^3 + 486662x^2 + x$

X25519 uses that curve with P at $x = 9$

256-bit keys

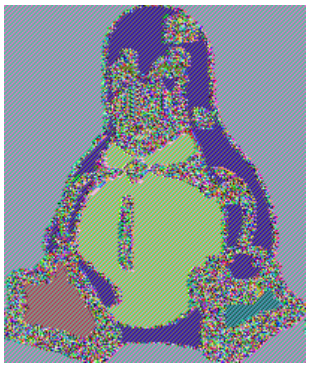
20× faster than 2048-bit RSA

See `x25519.c`

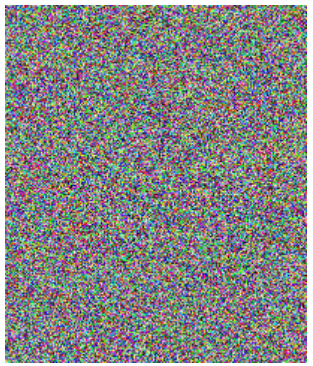
Block Cipher Mode of Operation

Recall that we need use a block cipher with a **mode of operation**

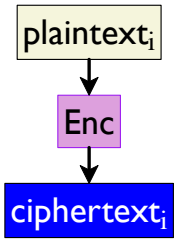
original

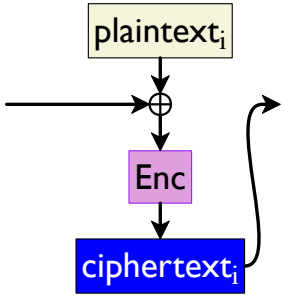


AES



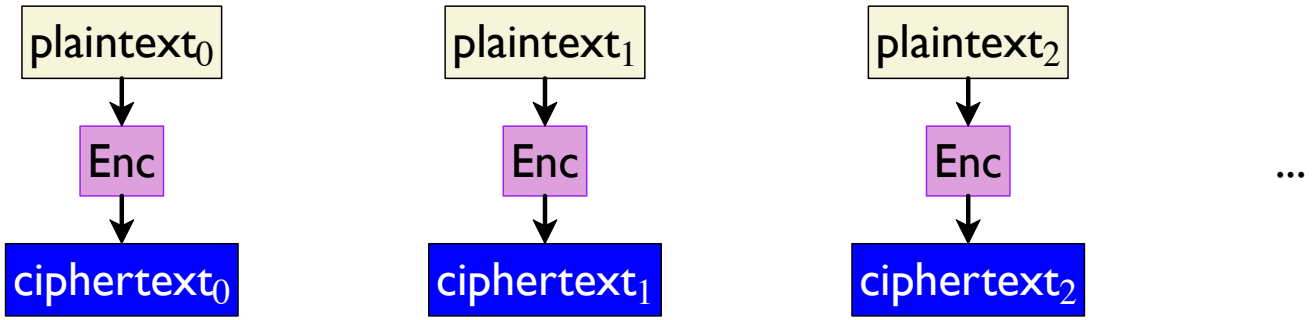
AES plus chaining





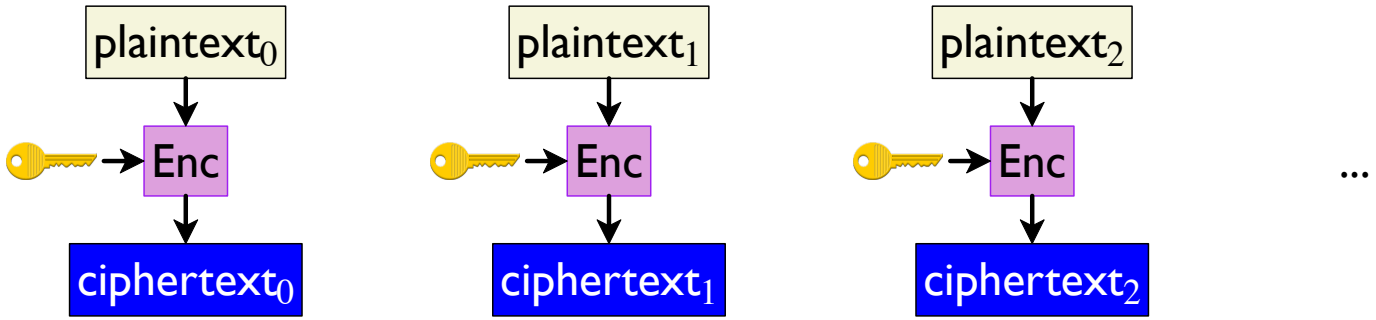
Electronic Cookbook

Electronic Cookbook (ECB) refers to using a block cipher separately on each block (i.e., naively)



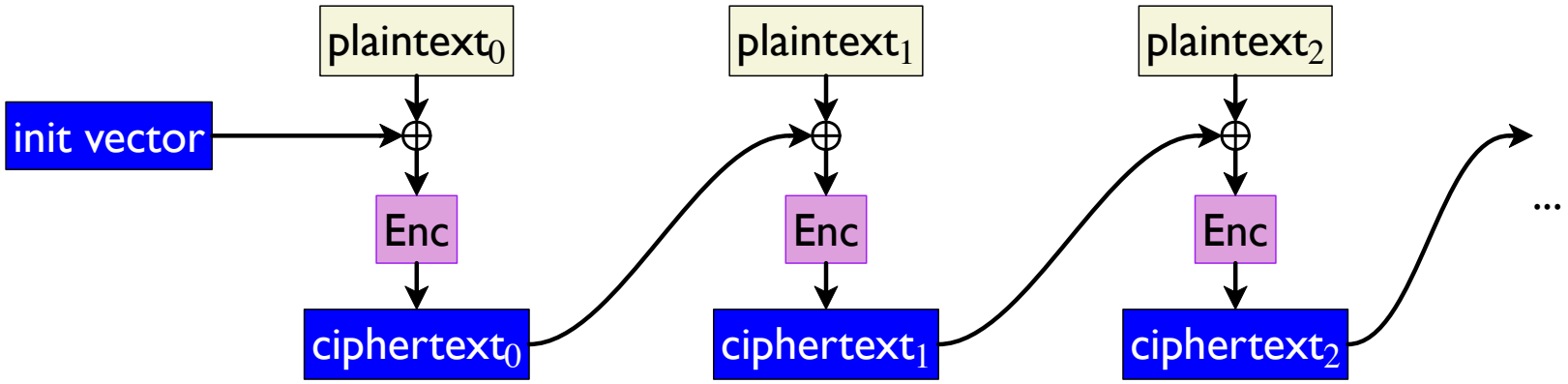
Electronic Cookbook

Electronic Cookbook (ECB) refers to using a block cipher separately on each block (i.e., naively)



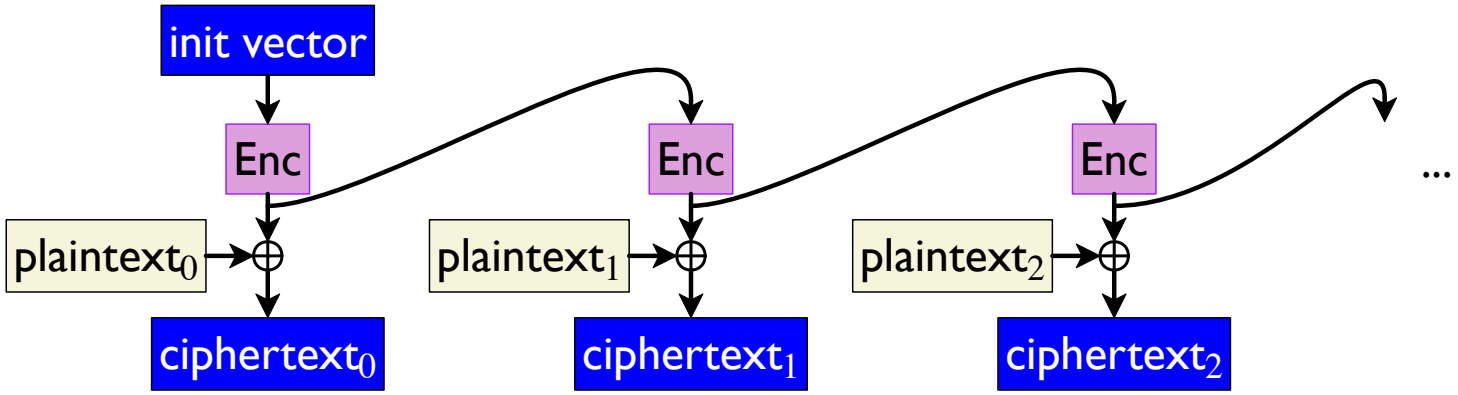
Cipher Block Chaining

Cipher Block Chaining (CBC) adds each previous ciphertext to plaintext before encoding



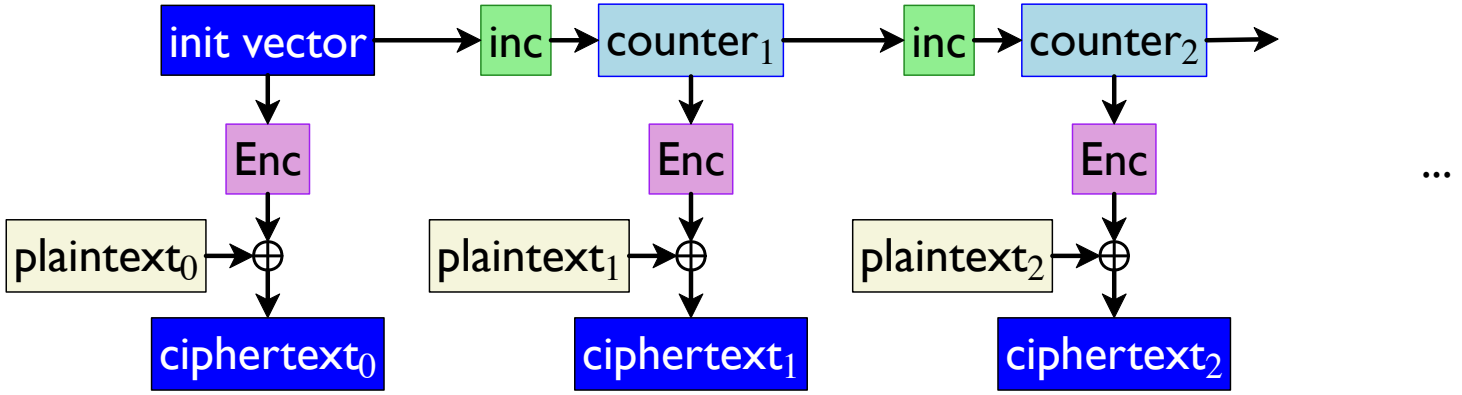
Output Feedback

Output Feedback (OFB) turns a block cipher intro a stream cipher



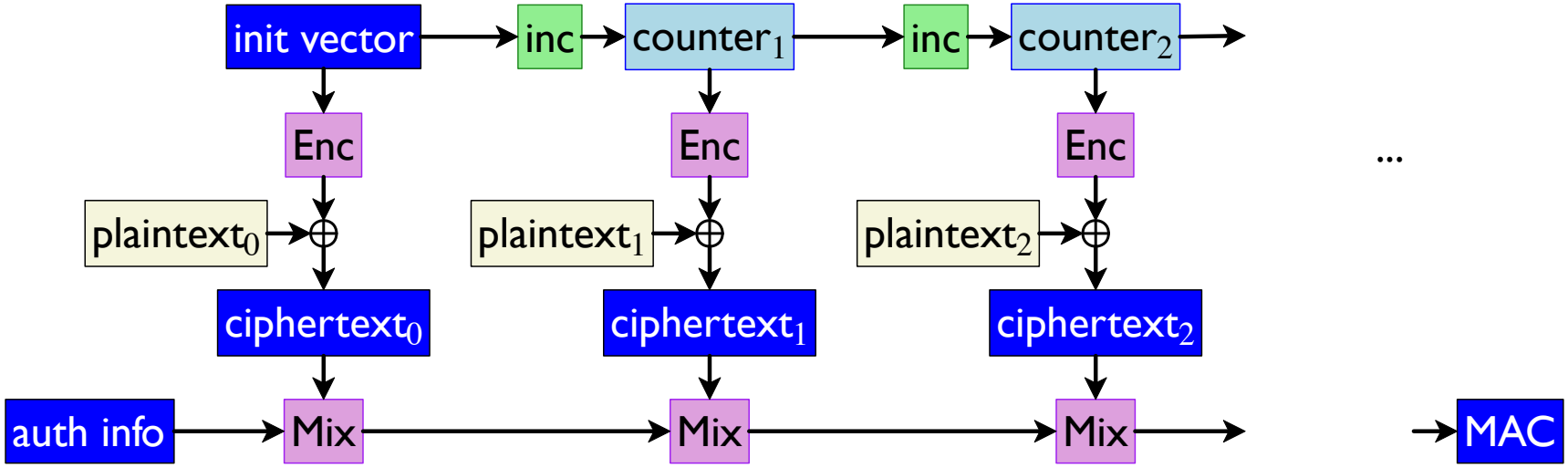
Counter

Counter (CTR) also turns a block cipher intro a stream cipher, but using a counter as input to the cipher



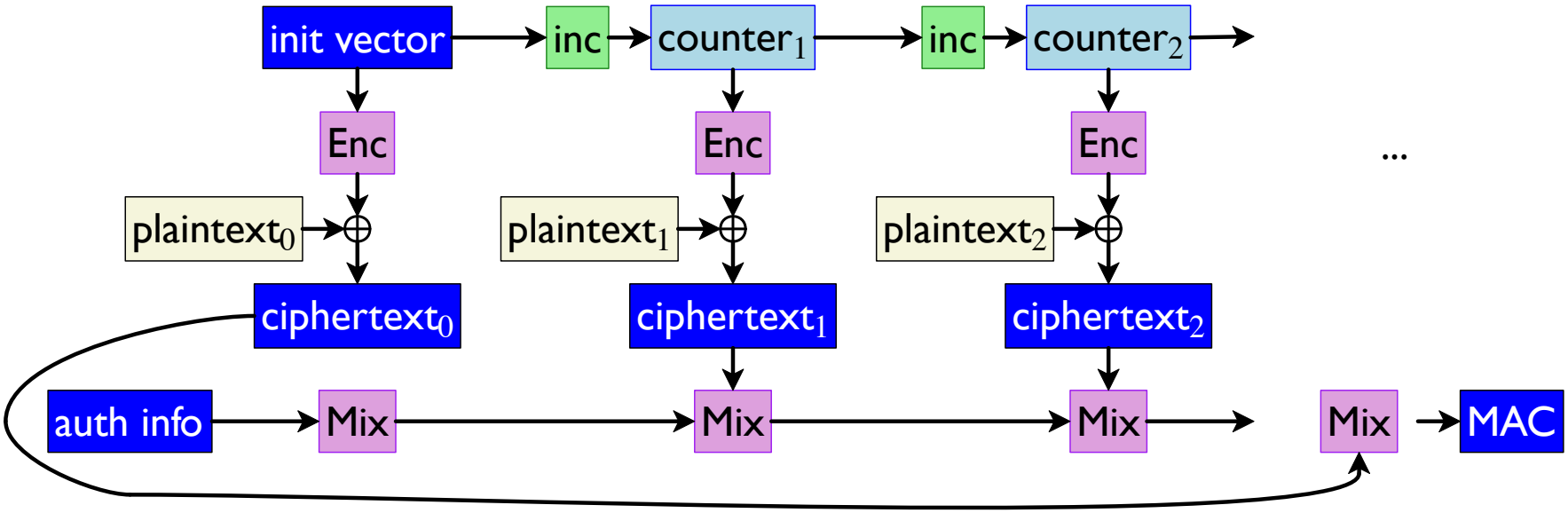
Galois/Counter

Galois/counter (GCM) builds on CTR by computing a MAC, which can used for both integrity and authorization



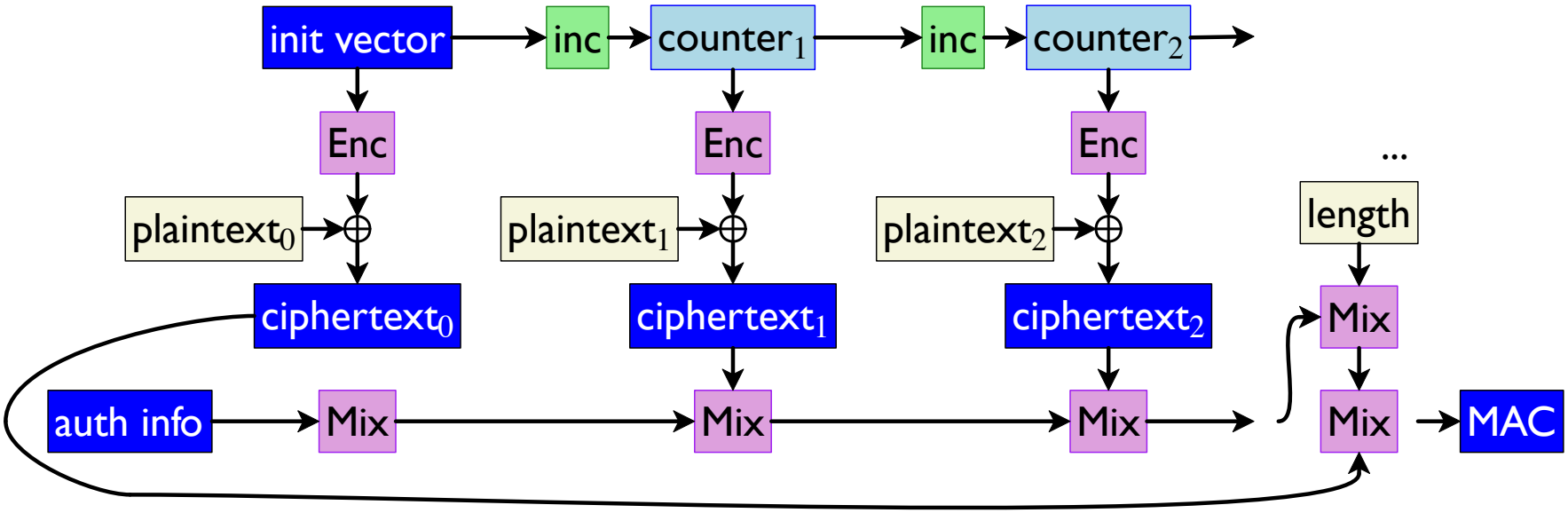
Galois/Counter

Galois/counter (GCM) builds on CTR by computing a MAC, which can used for both integrity and authorization



Galois/Counter

Galois/counter (GCM) builds on CTR by computing a MAC, which can used for both integrity and authorization



Summary

Elliptic key cryptography is an alternative to the traditional number-theory choice of encoding

Same protocol as Diffie-Hellman ⇒ **ECDH**

There are several **modes of operation** possible for block ciphers

Galois/counter (GCM) is a good choice