Elliptic Curve Cryptography

Justin Findlay
jfindlay@gmail.com

2016 January 6

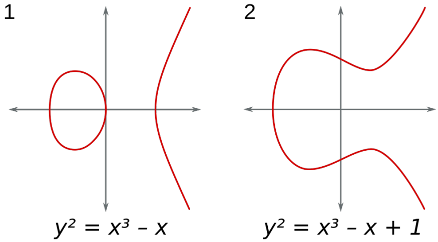
Elliptic Curves

Weierstrass equation[1]:

$$y^2 = x^3 + ax + b$$

where

$$\forall a, b \in \mathbb{R} \qquad \text{and} \qquad \Delta = -16(4a^3 + 27b^3) \neq 0$$



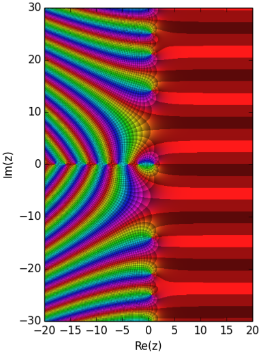
[1] https://en.wikipedia.org/wiki/Elliptic_curve

Utility of Elliptic Curves

Elliptic curves are related to:

- Riemann ζ function[2]

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-1}$$
$$= \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$
$$= \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{x^{s-1}}{e^x - 1} \mathrm{d}x$$



[2] And consequently the Riemann hypothesis: `https://en.wikipedia.org/wiki/Riemann_hypothesis#Consequences_of_the_Riemann_hypothesis`

Utility of Elliptic Curves

Elliptic curves are related to:

- Fermat's last theorem

$$\forall\ x, y, z \in \mathbb{Z}, \quad \nexists\ n \in \mathbb{Z} \quad \text{such that} \quad x^n + y^n = z^n$$

- Birch and Swinnerton-Dyer conjecture
- Langlands Program: Galois groups $\leftrightarrow$ automorphic forms, representation theory, *etc.*
- Galois Theory
- Lie Theory
- *etc.*

Groups

A group is a 2-tuple consisting of a set G and an operation $*$ having a list of properties.
Consider the set of integers and the addition operation, $(\mathbb{Z}, +)$.
For any $a, b, c \in \mathbb{Z}$:

- Closure: $a + b \in \mathbb{Z}$
- Associativity: $(a + b) + c = a + (b + c)$
- Identity: $\exists\ 0 \in \mathbb{Z}$ such that $a + 0 = a$
- Inverse: $\exists\ -a \in \mathbb{Z}$ such that $a + (-a) = 0$
- (Commutativity: $a + b = b + a$, only for abelian groups)

Fields

A field is a 3-tuple consisting of a set G and two operations $\dagger, *$ having a list of properties.
Consider the set of rational numbers and the addition and multiplication operations, $(\mathbb{Q}, +, \times)$. For any $a, b, c \in \mathbb{Q}$:

- the 2-tuple $(\mathbb{Q}, +)$ is an abelian group
- the 2-tuple $(\mathbb{Q} \setminus \{0\}, \times)$ is an abelian group
- Distributivity: $a \times (b + c) = a \times b + a \times c$

Vector Spaces

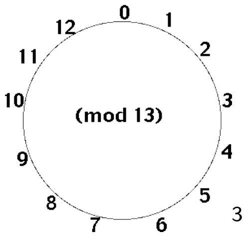
A vector space is a 3-tuple of a cartesian product of identical sets and two operations.

Consider the three copies of the set of integers $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^3$, vector addition and scalar multiplication, $(\mathbb{Z}^3, +, \cdot)$. For any $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \mathbb{Z}^3$ and $a, b \in \mathbb{Z}$:

- the 2-tuple $(\mathbb{Z}^3, +)$ is a group
- Compatibility: $a \cdot (b \cdot \boldsymbol{v}) = (ab) \cdot \boldsymbol{v}$
- Scalar Identity: $1 \cdot \boldsymbol{v} = \boldsymbol{v}$
- Field Distributivity: $(a + b) \cdot \boldsymbol{v} = a \cdot \boldsymbol{v} + b \cdot \boldsymbol{v}$
- Vector Distributivity: $a \cdot (\boldsymbol{v} + \boldsymbol{u}) = a \cdot \boldsymbol{v} + a \cdot \boldsymbol{u}$

Modular Arithmetic and Finite Fields

A finite group or a finite field is a group or a field whose set is finite.



[3]

Examples:

$$7 + 8 = 15 \equiv 2 \mod 13$$
$$10 \times 10 = 20 \equiv 7 \mod 13$$

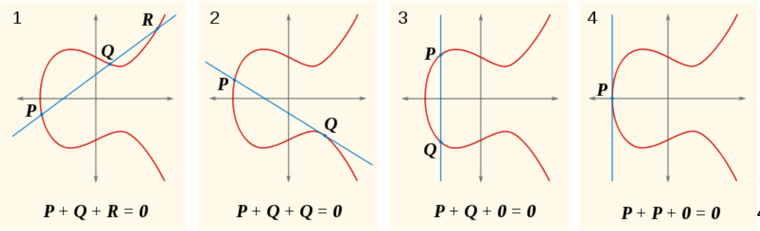
[3] http://pajhome.org.uk/crypt/rsa/maths.html

Projective Plane

The projective plane (the set $\mathbb{R}^2 + \{P\}$, where P is the point at infinity):

- $\forall$ points $a, b \in \mathbb{P}$, $\exists$ exactly one line $L \subset \mathbb{P}$ such that $a, b \in L$
- $\forall$ lines $K, L \in \mathbb{P}$, $\exists$ exactly one point $a \in \mathbb{P}$ such that $a \in L$ and $a \in K$
- $\forall a, b, c, d \in \mathbb{P}$, $\exists$ no line $L \subset \mathbb{P}$ such that more than two points $\in L$

Projective Plane



[4]

The projective plane is needed to do algebra over the points on an elliptic curve. The point at infinity serves as the identity element.

[4] https://en.wikipedia.org/wiki/File:ECClines.svg

Discrete Logarithm

- The discrete logarithm[5]:

$$n^k \mod p \qquad\qquad k, n, p \in \mathbb{Z}$$

- The discrete logarithm problem:

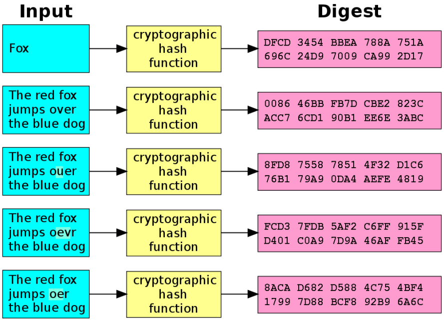
$$n^k \mod p = N \equiv m$$

  Is there a polynomial time algorithm that can find k by knowing N? Whereas finding N by knowing k is easy.
- (n is known as a generator of the group $\mathbb{Z}_p$)

[5] Also see:
https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/discrete-logarithm-problem

Hashing

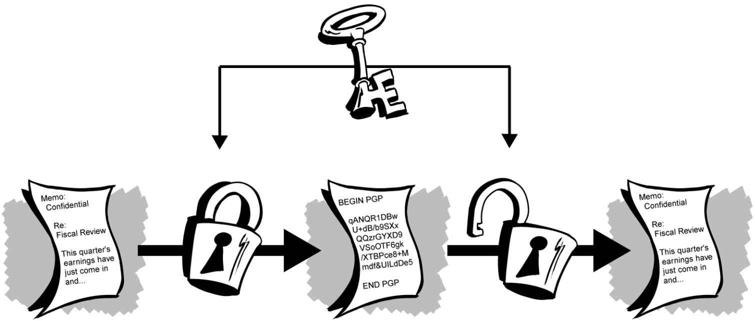
A hash is a function that maps strings of bytes of arbitrary length into a set of strings of bytes that have relatively short and identical lengths.



[6]

[6] https://commons.wikimedia.org/wiki/File:Cryptographic_Hash_Function.svg

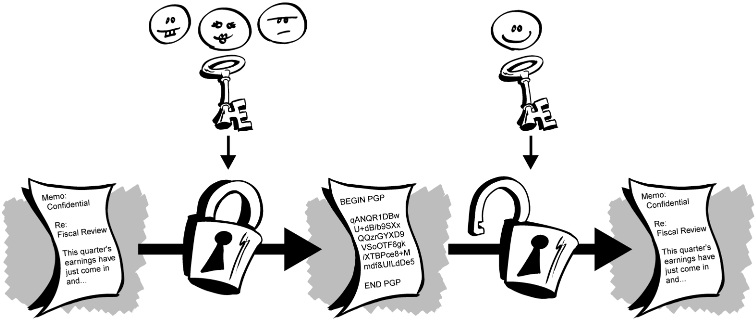
Symmetric Keys



[7]

[7] http://fisher.osu.edu/~muhanna.1/pdf/crypto.pdf

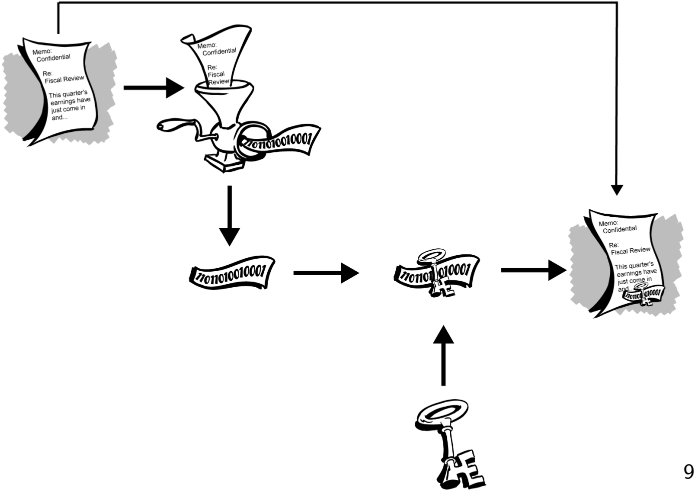
Asymmetric Keys



[8]

[8] http://fisher.osu.edu/~muhanna.1/pdf/crypto.pdf

Signing



[9]

[9] http://fisher.osu.edu/~muhanna.1/pdf/crypto.pdf

Libraries

- NaCl
  - NaCl: `http://nacl.cr.yp.to/`
  - tweetNaCl: `http://tweetnacl.cr.yp.to/`
  - libsodium: `https://github.com/jedisct1/libsodium`
- libnacl
  - home: `https://github.com/saltstack/libnacl`
  - docs: `https://libnacl.readthedocs.org/en/latest/`
- PyNaCl
  - home: `https://github.com/pyca/pynacl`
  - docs: `https://pynacl.readthedocs.org/en/latest/`
- pure_pynacl: `https://github.com/jfindlay/pure_pynacl`