Plan for Today

Bitcoin Wallets and Passwords

Asymmetric Cryptography Recap:

Transferring a Coin

Crash Course in Number Theory

Elliptic Curve Cryptography

Buying Bitcoin

CIRCLE

Hello, money.

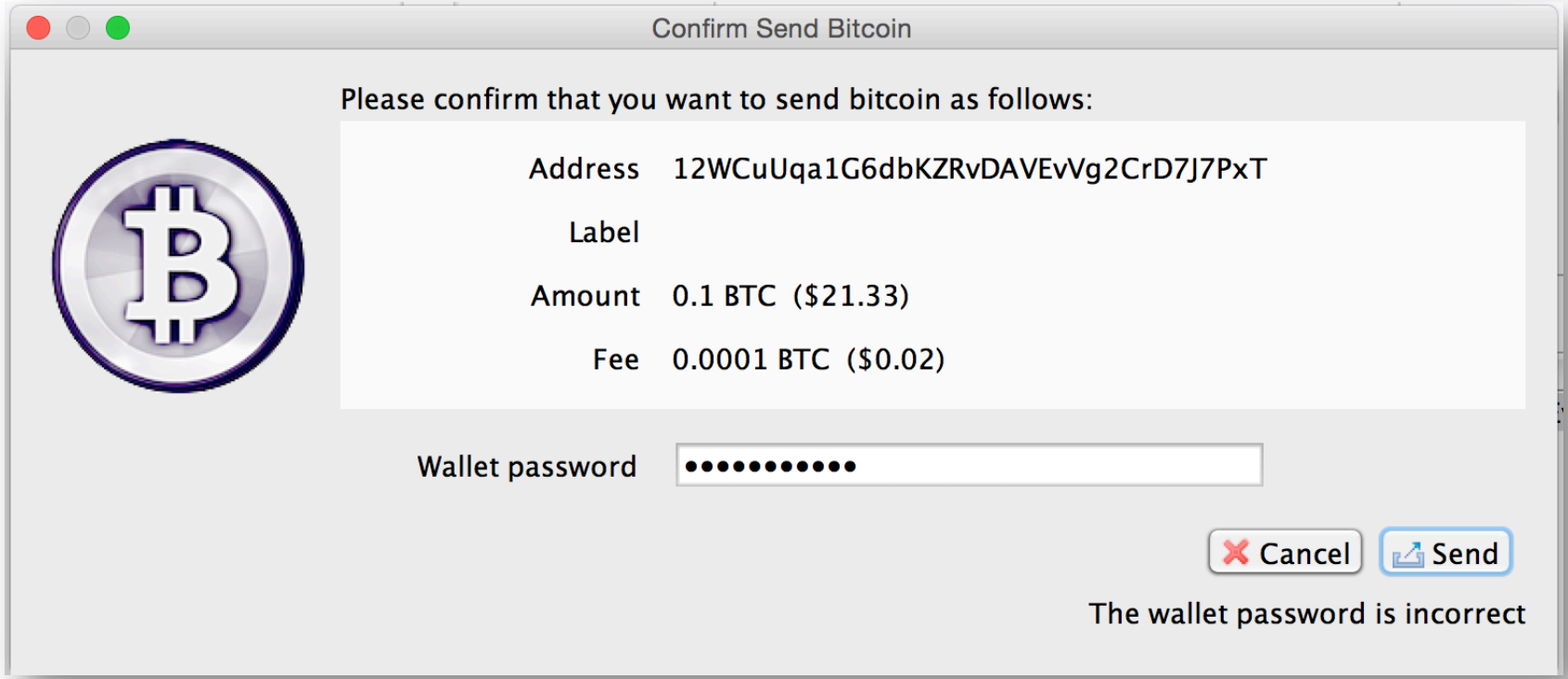
We make using money instant, secure, and free.
The way money should be.

coinbas

YOUR BITCOIN WALLET

Coinbase is the world's most popular bitcoin wallet. We make it easy to securely buy, use, and accept bitcoin currency.

HOW TO BUY BITCOIN


Confirm Send Bitcoin
Please confirm that you want to send bitcoin as follows:
Address 12WCuUqa1G6dbKZRvDAVEvVg2CrD7J7PxT
Label
Amount 0.1 BTC ($21.33)
Fee 0.0001 BTC ($0.02)
Wallet password
Cancel
Send
The wallet password is incorrect

RESPONSIBLE COMPUTING
UNIVERSITY of VIRGINIA

Use Strong Password Protection

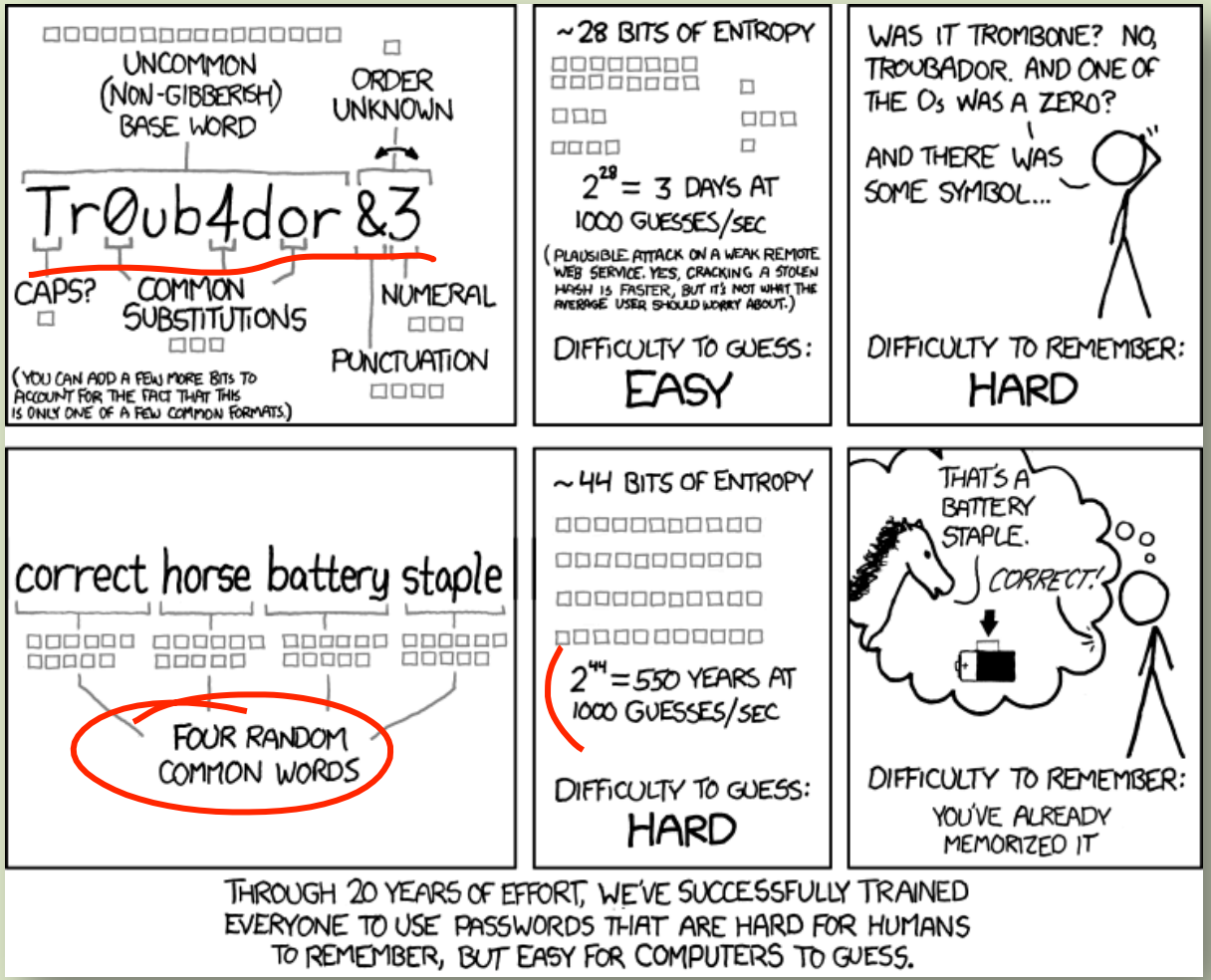
Some types of computer attacks aren't possible if the attacker can't guess your password. Unfortunately, hackers have too
password tips:

- Memorize the passwords you create, rather than writing them down.
- Don't share your passwords with others, ever.
- Change your passwords if you know or suspect they have been revealed to someone.
- Use different login names and passwords for your work accounts and your personal, non-work accounts.
- Learn what makes a strong password.

How to Make a Strong Password

Make sure your passwords:

- consist of 8 or more characters;
- use both uppercase (A-Z) and lowercase (a-z) letters;
- include one or more numbers (0-9);
- include one or more special characters, such as a question mark or an asterisk; and
- do not contain a name or a word found in the dictionary.


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

My Advice

Don't waste brainpower/space on passwords that don't matter

"silly" is a fine password for most things than need one

Don't follow any widely-available advice

password cracker authors can read too!

Humans cannot generate randomness and neither can you

Generate a random password

Share your password

(but only with people with whom you are willing to raise children)

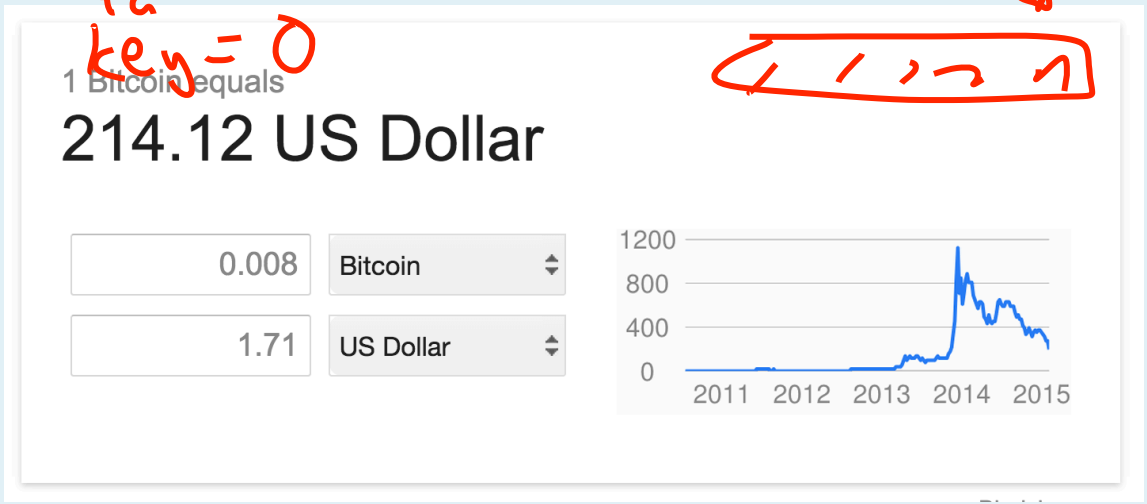
Write down your important passwords

Store them somewhere safe, and write down in a way that someone who steals it wouldn't be able to use.

Using Bitcoin in This Class

It is “real” money: try not lose (all of) it. (But you can do everything in this class with very small amounts.)

If you do, I’ll send you more (so long as you learned something from the loss). Everyone gets **one embarrassment-free transfer**.



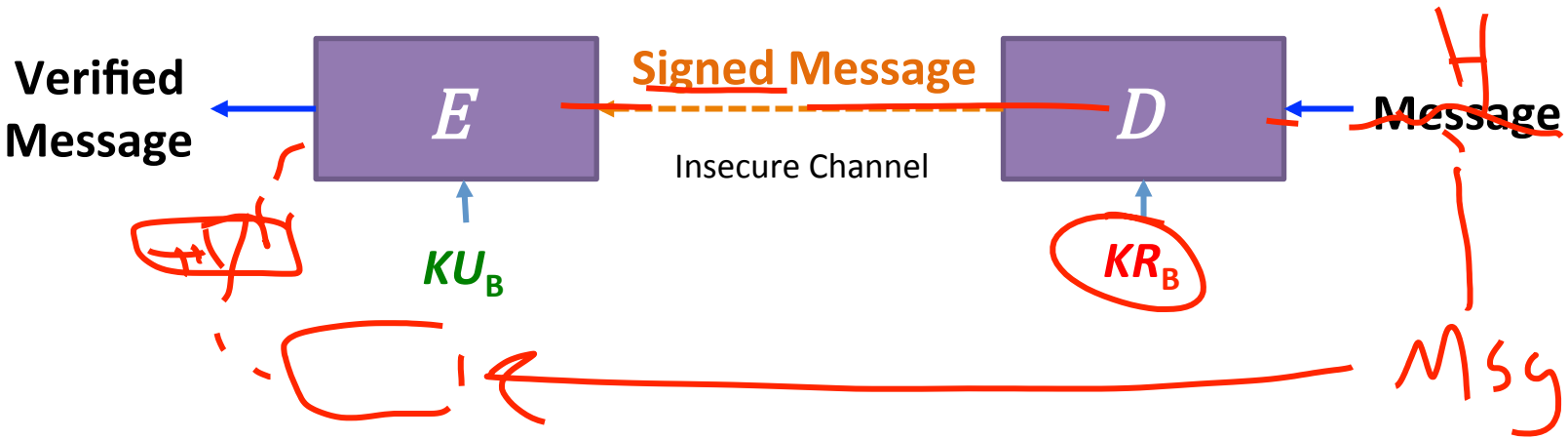
Using Asymmetric Crypto: **Signatures**

Anyone

Get KU_B from trusted provider

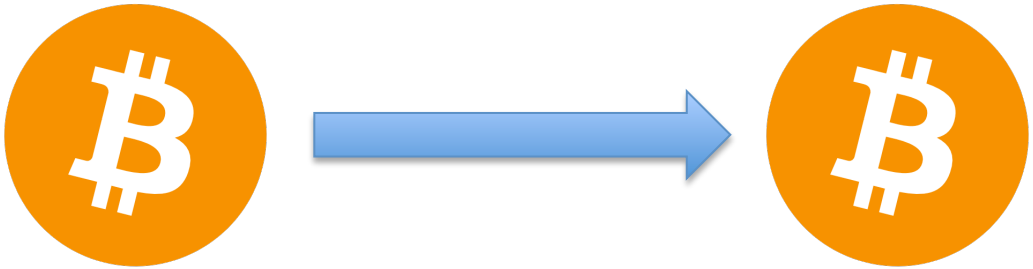
Bob

Generates key pair: KU_B, KR_B
Publishes KU_B



Transferring a Coin

Alice signs m_1 = { "I give coin $x = KU_A$, t to address KU_B."} with KR_A.

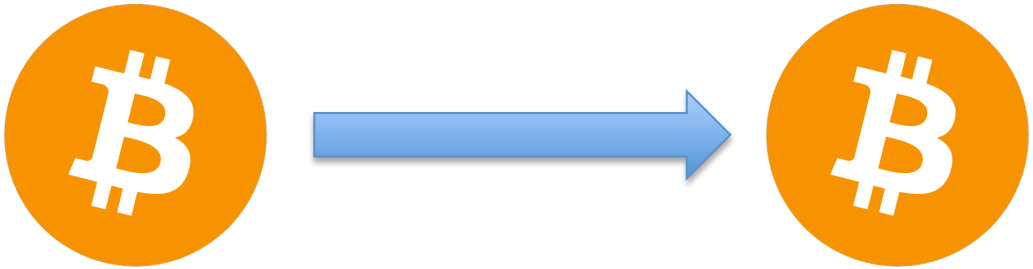


How does Bob transfer x to Colleen (KU_C)?

Transferring a Coin

Alice signs m_1 = { "I give coin $x = KU_A$, t to address KU_B."} with KR_A.

Bob signs m_2 = { "I give coin $x = KU_A$, t, given to me by $m_1$to address KU_C."} with KR_B.



Transferring a Coin

Alice signs m_1 = { "I give coin $x = KU_A$, t to address KU_B."} with KR_A.

Bob signs m_2 = { "I give coin $x = KU_A$, t, given to me by m_1 to address KU_C."} with KR_B.

Colleen signs m_2 = { "I give coin $x = KU_A$, t, given to me by m_2 to address KU_D."} with KR_C.

…

This does not prevent double spending! (Next week)

Asymmetry Required

Need a function f that is:

Easy to compute:

given x, **easy** to compute $f(x)$

Hard to invert:

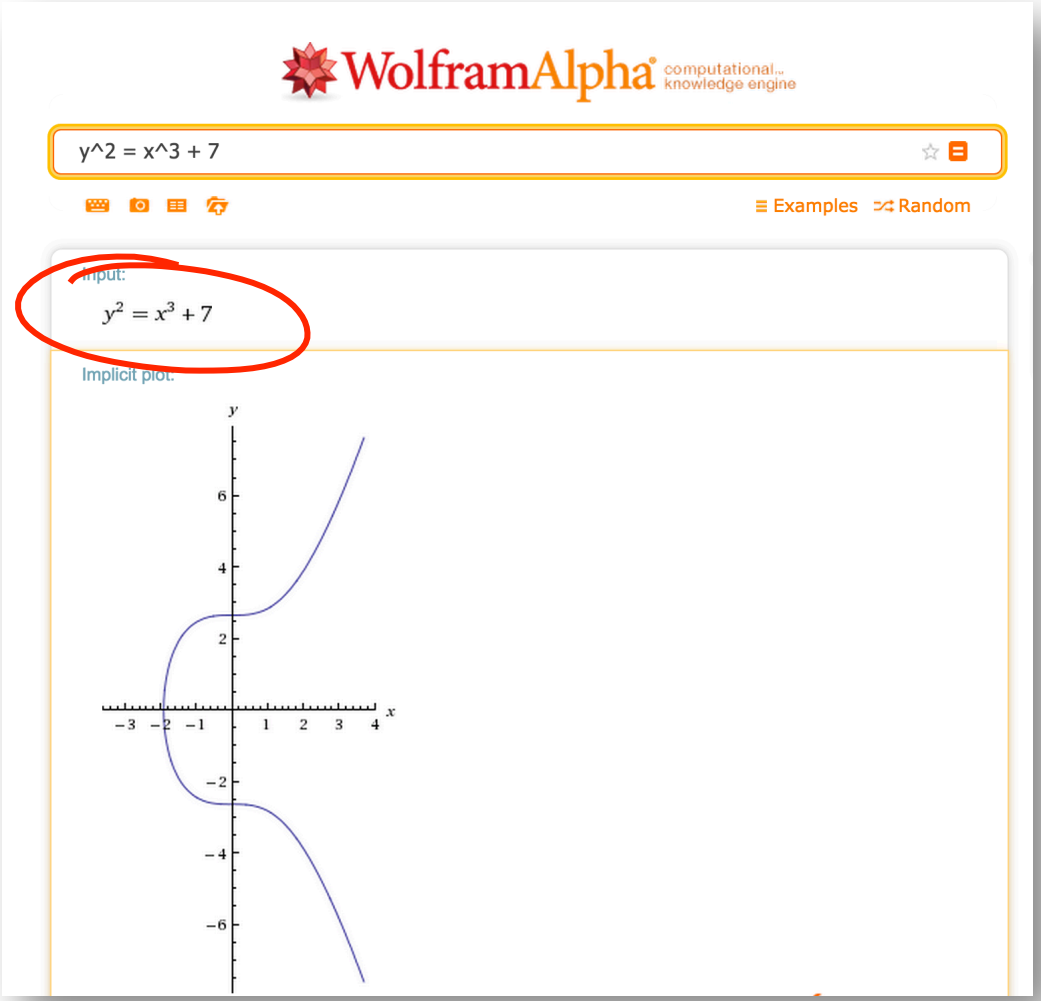
given $f(x)$, **hard** to compute x

Has a trap-door:

given $f(x)$ and t,

easy to compute x


Elliptic Curve Cryptography



$$y = \sqrt{x^3 + 7}$$

$$y = -\sqrt{x^3 + 7}$$

Real numbers are useless!

Groups

A **group** is a set, G, on which the operation $\oplus$ is defined with the following properties:

1. **Closure:** for all $a, b \in G$, $a \oplus b \in G$.
2. **Associative:** for all $a, b, c \in G$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. **Identity:** there is some element, $\mathbf{0} \in G$, such that:
   for all $a \in G$, $a \oplus \mathbf{0} = \mathbf{0} \oplus a = a$.
4. **Inverse:** for all $a \in G$, there exists an inverse, $-a \in G$, such that $a \oplus (-a) = 0$.

1. **Closure:** for all $a, b \in G$, $a \oplus b \in G$.
2. **Associative:** for all $a, b, c \in G$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. **Identity:** there is some element, $\mathbf{0} \in G$, such that:
   for all $a \in G$, $a \oplus \mathbf{0} = \mathbf{0} \oplus a = a$.
4. **Inverse:** for all $a \in G$, there exists an inverse, $-a \in G$, such that $a \oplus (-a) = 0$.

Is *Integers*, **+** a group?

✓ $0 = 0$

inverse = $-n$

1. **Closure:** for all $a, b \in G$, $a \oplus b \in G$.
2. **Associative:** for all $a, b, c \in G$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. **Identity:** there is some element, $\mathbf{0} \in G$, such that:
   for all $a \in G$, $a \oplus \mathbf{0} = \mathbf{0} \oplus a = a$.
4. **Inverse:** for all $a \in G$, there exists an inverse, $-a \in G$, such that $a \oplus (-a) = 0$.

Is *Naturals*, **+** a group?

No

1. **Closure:** for all $a, b \in G$, $a \oplus b \in G$.
2. **Associative:** for all $a, b, c \in G$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. **Identity:** there is some element, $\mathbf{0} \in G$, such that:
   for all $a \in G$, $a \oplus \mathbf{0} = \mathbf{0} \oplus a = a$.
4. **Inverse:** for all $a \in G$, there exists an inverse, $-a \in G$, such that $a \oplus (-a) = 0$.

Is *Rationals*, * a group?

$\frac{p}{q}$

Identity

1

Identity = 1

0 has no inverse!

$\mathbb{Q} - \{0\}$

Abelian Groups

A **group** is a set, G, on which the operation $\oplus$ is defined with the following properties:

1. **Closure:** for all $a, b \in G$, $a \oplus b \in G$.
2. **Associative:** for all $a, b, c \in G$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. **Identity:** there is some element, $\mathbf{0} \in G$, such that:
   for all $a \in G$, $a \oplus \mathbf{0} = \mathbf{0} \oplus a = a$.
4. **Inverse:** for all $a \in G$, there exists an inverse, $-a \in G$, such that $a \oplus (-a) = 0$.
5. **Commutative:** for all $a, b \in G$, $a \oplus b = b \oplus a$.

1. **Closure:** for all $a, b \in G$, $a \oplus b \in G$.
2. **Associative:** for all $a, b, c \in G$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. **Identity:** there is some element, $\mathbf{0} \in G$, such that:
   for all $a \in G$, $a \oplus \mathbf{0} = \mathbf{0} \oplus a = a$.
4. **Inverse:** for all $a \in G$, there exists an inverse, $-a \in G$, such that $a \oplus (-a) = 0$.
5. **Commutative:** for all $a, b \in G$, $a \oplus b = b \oplus a$.

Is $Rationals - \{0\}$, * an abelian group?

Finite Fields

A finite field is a set F of $N \geq 2$ elements on which the operators $\oplus$ and $\times$ are defined with these properties:

1. The set F is an abelian group with identity **0** under the $\oplus$ operation.
2. The set F - $\{ 0 \}$ is an abelian group with identity **1** under the $\times$ operation.
3. **Distributive:** For all $a, b, c \in F$,

$$(a \oplus b) \times c = (a \times c) \oplus (b \times c).$$

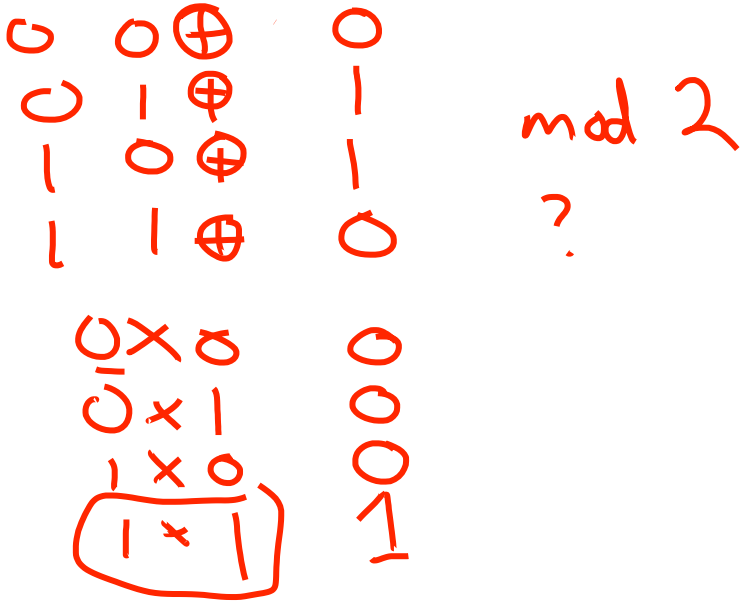
Know any finite fields?

A finite field is a set F of $N \geq 2$ elements on which the operators $\oplus$ and $\times$ are defined with these properties:

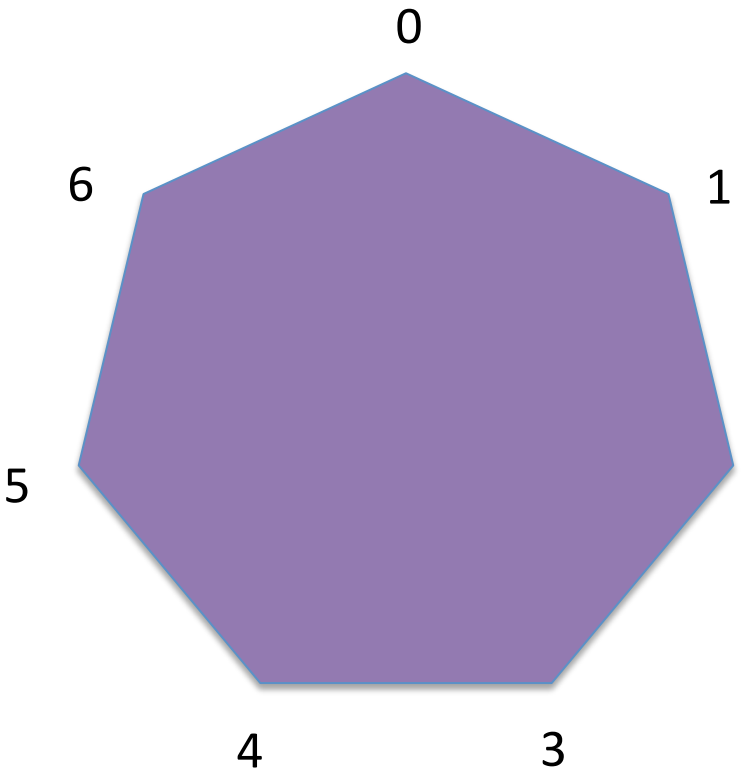
1. The set F is an abelian group with identity **0** under the $\oplus$ operation.
2. The set $F - \{ 0 \}$ is an abelian group with identity **1** under the $\times$ operation.
3. **Distributive:** For all $a, b, c \in F$, $(a \oplus b) \times c = (a \times c) \oplus (b \times c)$.

{0, 1}

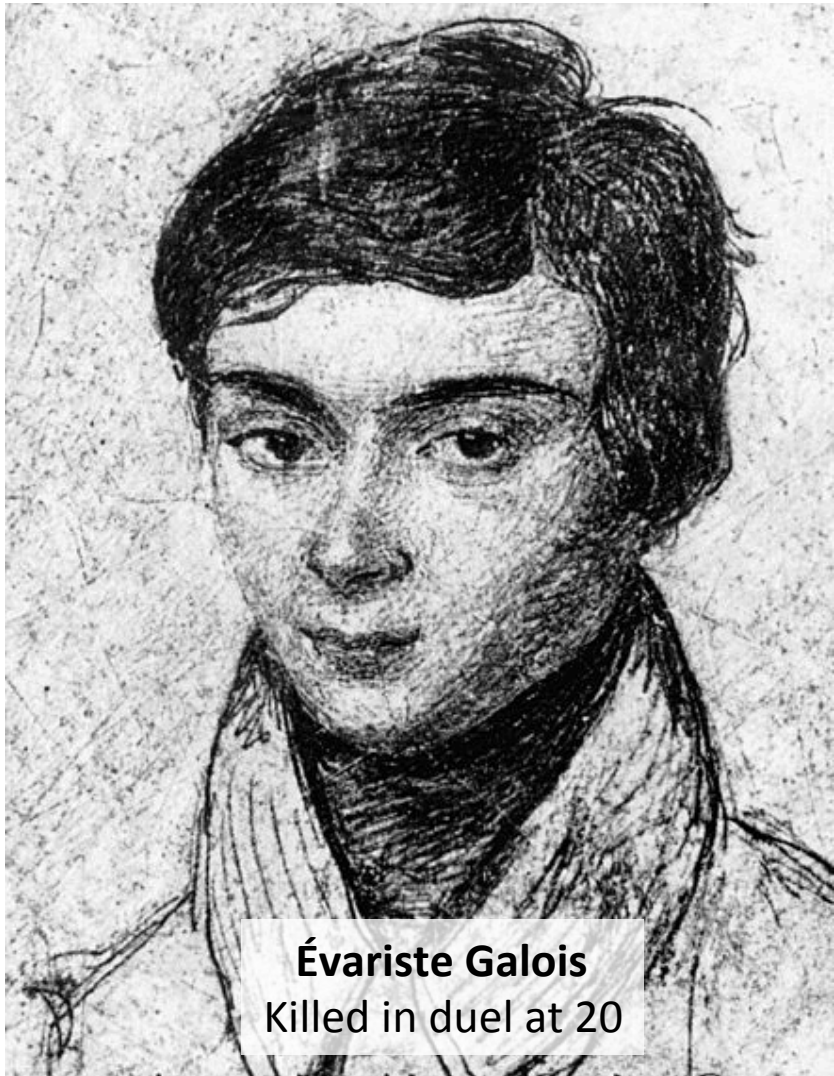
GF(2)



mod 2 ?



$GF(7)$



Prime Fields

Prime Field Theorem: For every prime number p, the set $\{ 0, 1, \ldots, p - 1 \}$ forms a finite field with the operations addition and multiplication modulo p.

GF(2)

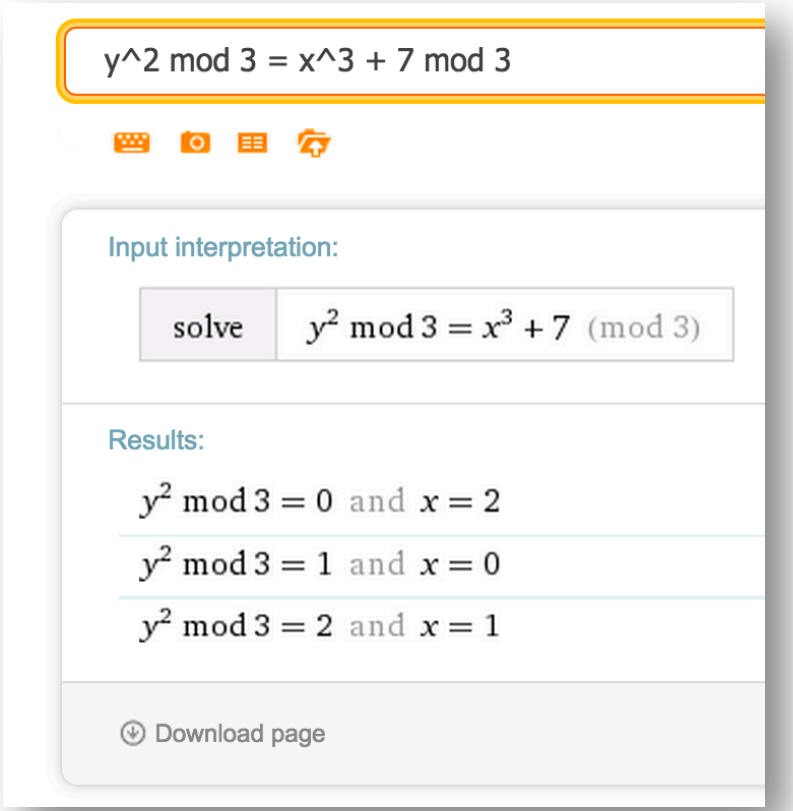
Elliptic Curves in Finite Fields

$y^2 = x^3 + 7$ in $GF(3)$

$1^2 = 0^3 + 1$ ✓

Elliptic Curves in Finite Fields

$y^2 = x^3 + 7$ in $GF(3)$

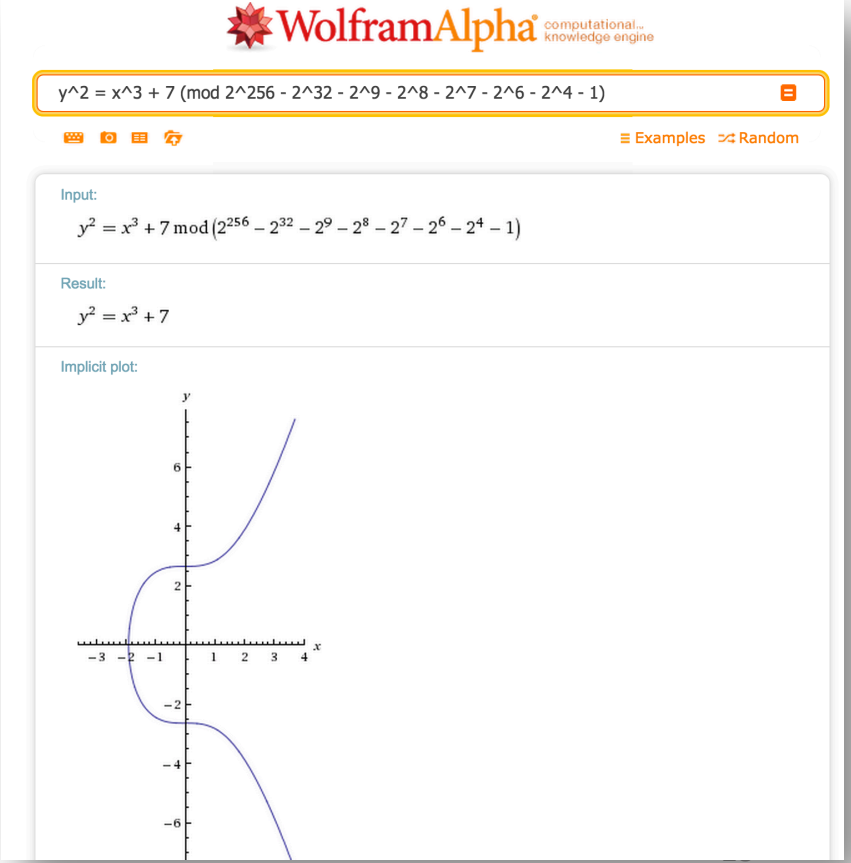


Elliptic Curves in Finite Fields

$$y^2 = x^3 + 7 \text{ in } GF(2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1)$$

$y^2 = x^3 + 7$ in $GF(2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1)$

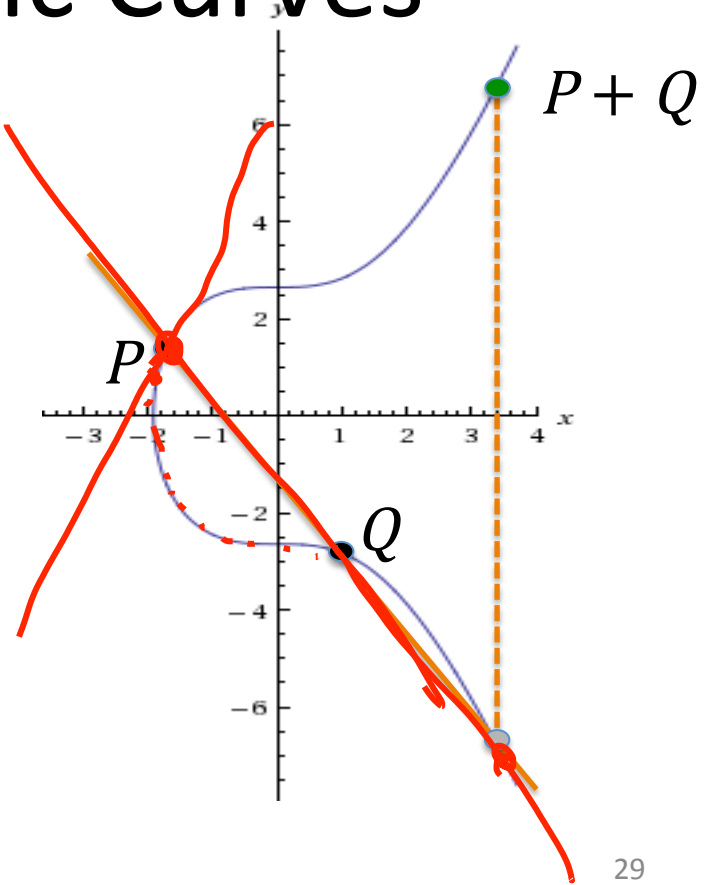
115 quattuorvigintillion 792 trevigintillion 89 duovigintillion 237 unvigintillion 316 vigintillion 195 novemdecillion 423 octodecillion 570 septendecillion 985 sexdecillion 8 quindecillion 687 quattuordecillion 907 tredecillion 853 duodecillion 269 undecillion 984 decillion 665 nonillion 640 octillion 564 septillion 39 sextillion 457 quintillion 584 quadrillion 7 trillion 908 billion 834 million 671 thousand 663
(0.0012 × the number of atoms in the visible universe)



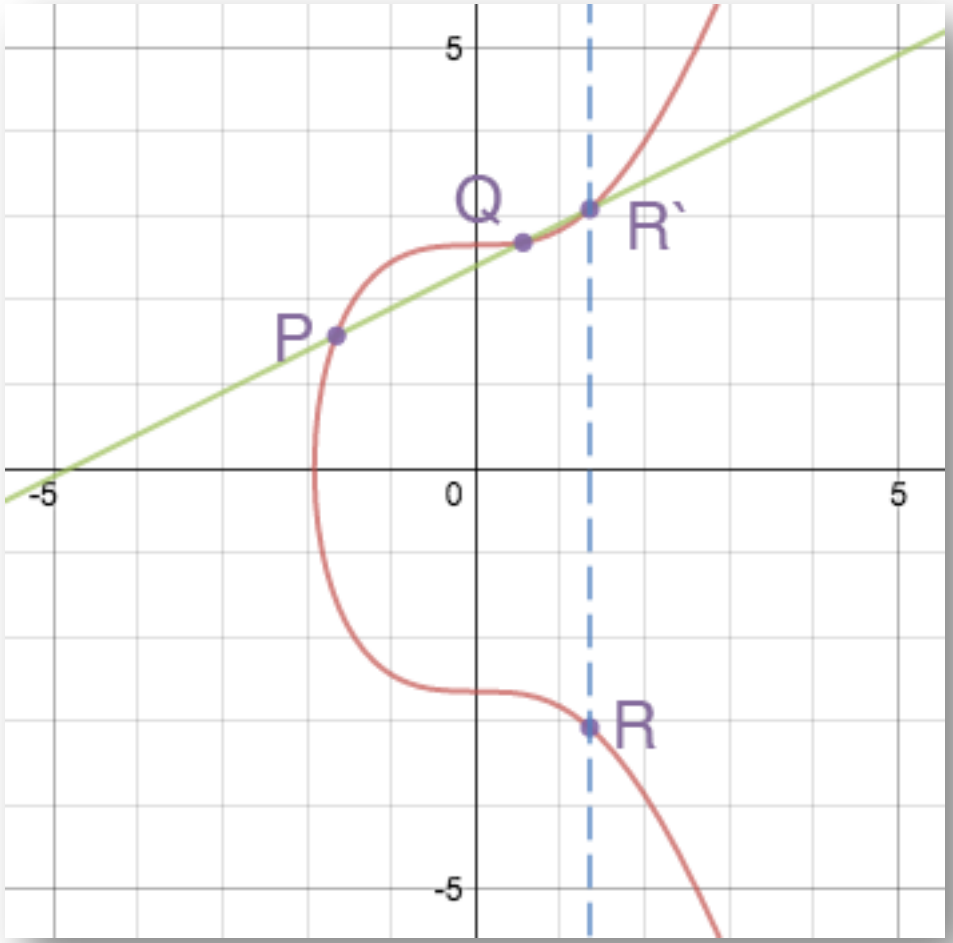
Addition on Elliptic Curves

$P + P$

$$y^2 = x^3 + 7 \pmod{p}$$



Addition: $P + Q$
= negate intersection of curve with line through P and Q

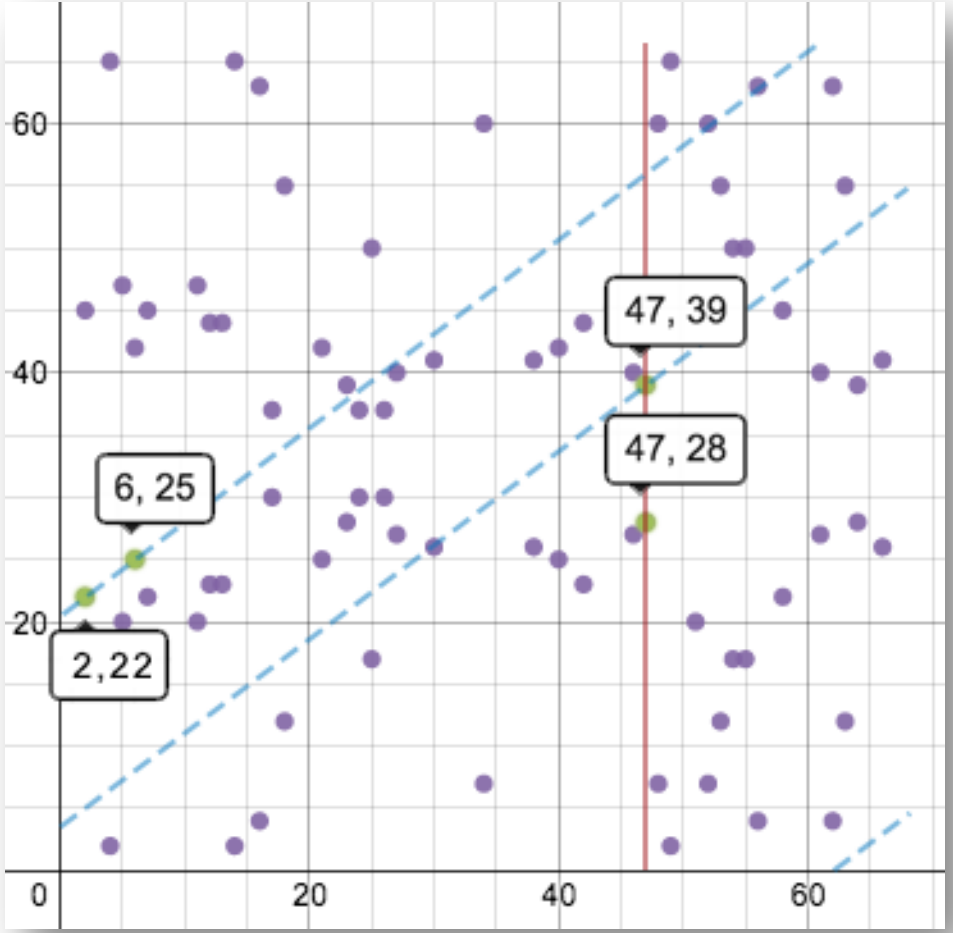


Addition

$P + Q = R$

What should we do if P = Q?

Image from: http://www.coindesk.com/math-behind-bitcoin/



Addition

Same idea for finite fields (just more complex)

Picture is for F_{67}.

How would this look for F_{huge}?

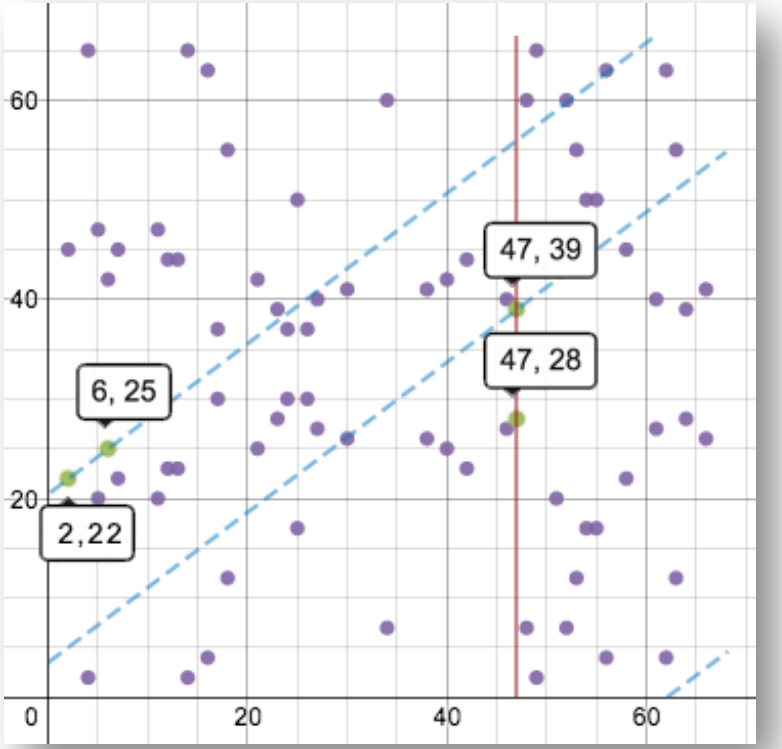
Image from: http://www.coindesk.com/math-behind-bitcoin/

Density of Elliptic Curve

$y^2 = x^3 + 7$ in $GF(2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1)$

(Believed to be) Hard Problem

Elliptic curve discrete logarithm problem: given points P and Q on an elliptic curve, it is **hard** to find an integer k such that $Q = kP$.



Charge

- **Investigate** the bitcoin you received
- **Project 1** will be posted before midnight tonight and due on Jan 30
- **Readings:** Satoshi's original bitcoin paper, Chapter 5

Next class: how to use Elliptic Curve Crypto for **signatures**;
how (**not**) to use Elliptic Curves for pseudorandom number generation
Next week: preventing double spending