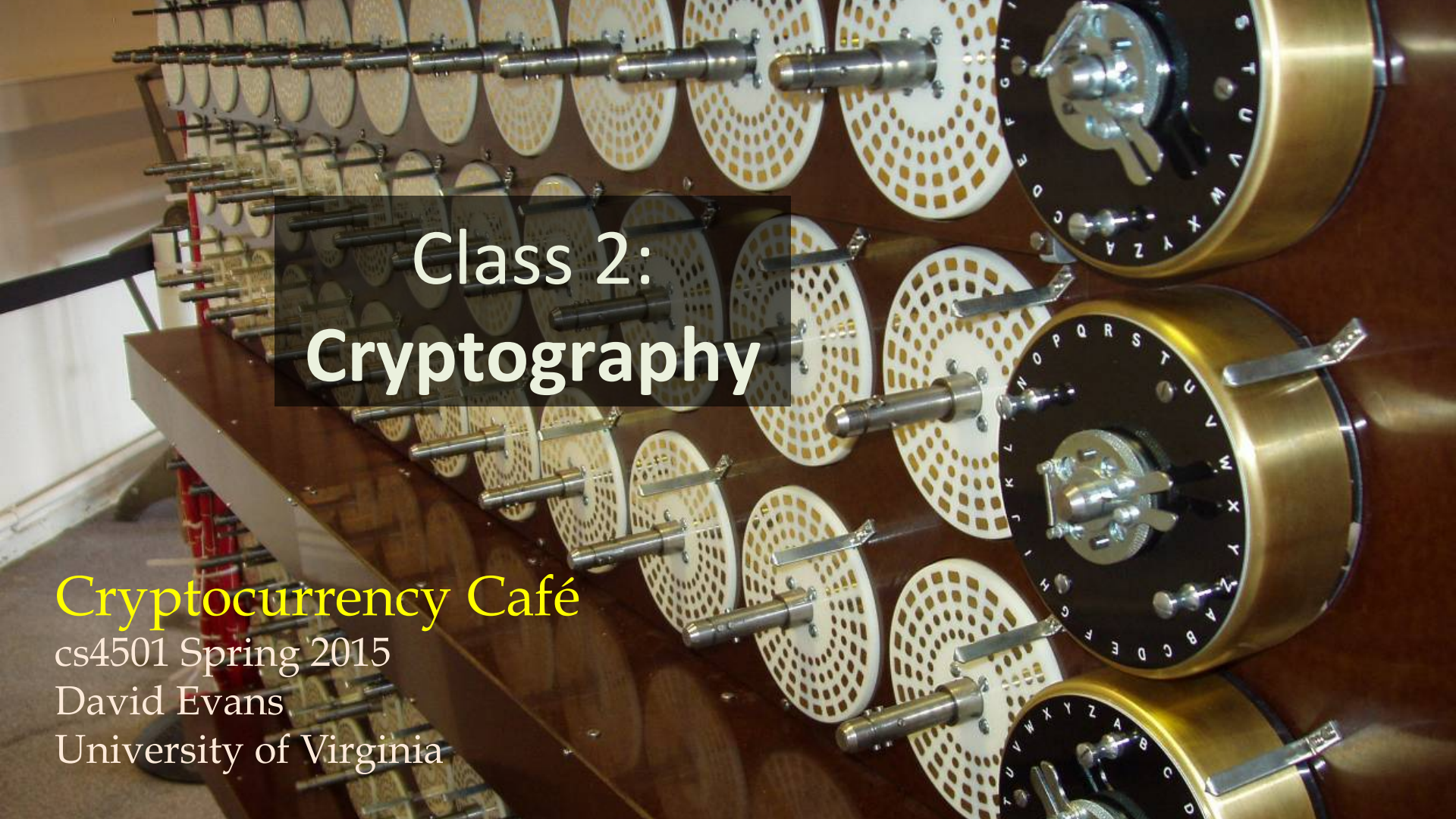


Class 2: **Cryptography**

Cryptocurrency Café

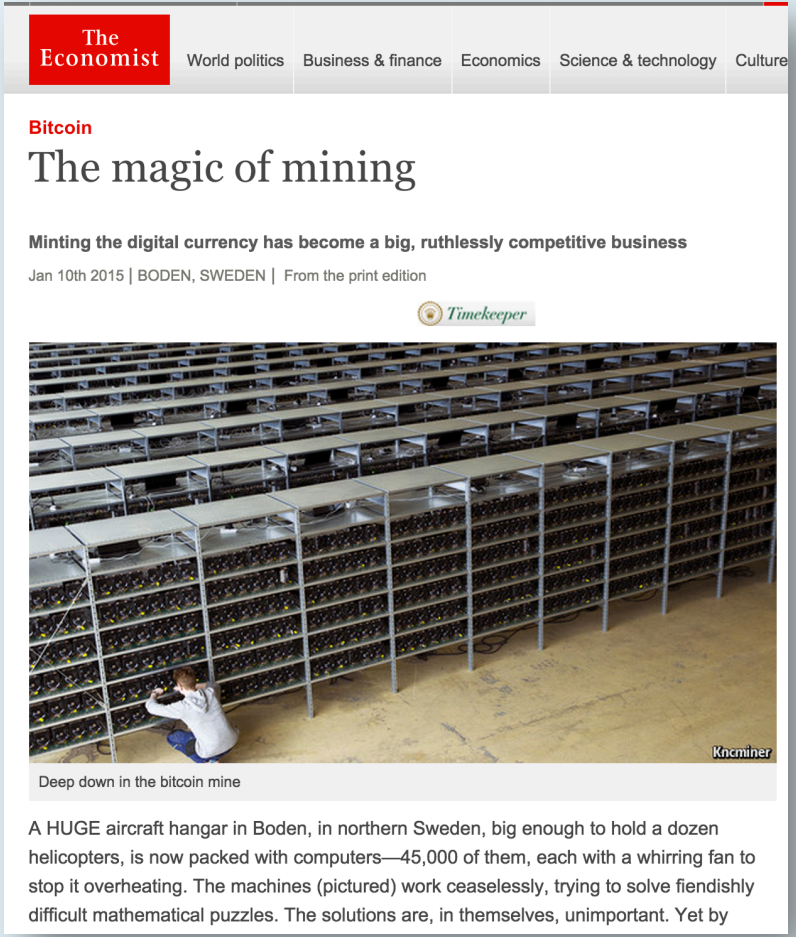
cs4501 Spring 2015

David Evans
University of Virginia

Goal for Today

- Notion of **ownership** of non-physical good
- Conceptual understanding of **key terms** and **principles** in cryptography
  - Cryptosystem
  - Attacks
  - Asymmetry
- Underlying foundation of bitcoin

Comments about “Magic of Mining”



The Economist | World politics | Business & finance | Economics | Science & technology | Culture

Bitcoin

The magic of mining

Minting the digital currency has become a big, ruthlessly competitive business

Jan 10th 2015 | BODEN, SWEDEN | From the print edition

Timekeeper

Deep down in the bitcoin mine

A HUGE aircraft hangar in Boden, in northern Sweden, big enough to hold a dozen helicopters, is now packed with computers—45,000 of them, each with a whirring fan to stop it overheating. The machines (pictured) work ceaselessly, trying to solve fiendishly difficult mathematical puzzles. The solutions are, in themselves, unimportant. Yet by

150

Bitcoin: The magic of mining (economist.com)

submitted 5 days ago by _chmod755_

48 comments share save hide give gold report

all 48 comments - sorted by: best

save

reddiquette formatting help

[–] **mshadel** 26 points 5 days ago

"The machines work ceaselessly, trying to solve fiendishly difficult mathematical puzzles."

Pet peeve of mine. Hashing is more like playing the lottery. It's not a puzzle at all, it's just extremely unlikely that an individual ticket will be a winner. Mining operations are just buying LOTS of tickets.

permalink save report give gold reply

[–] **thieflar** 5 points 5 days ago

It's a pet peeve of mine, as well, since it sort of implies that some math whiz could come through and figure out a new approach that makes the problem a lot easier and makes them some sort of superminer.

It's guess-and-check, not advanced calculus or anything. The problem itself (computing SHA-256 hashes) is not particularly difficult, just time consuming and highly automatable.

But alas, such nuances are too complicated for general audiences

r/bitcoin

150

Bitcoin: The magic of mining (economist.com)

submitted 5 days ago by _chmod755_

48 comments share save hide give gold report

search

all 48 comments - sorted by: best

save

reddiquette formatting help

[–] **mshadel** 26 points 5 days ago

"The machines work ceaselessly, trying to solve fiendishly difficul

Pet peeve of mine. Hashing is more like playing the lottery. It's n
that an individual ticket will be a winner. Mining operations are ju

permalink save report give gold reply

[–] **thieflar** 5 points 5 days ago

It's a pet peeve of mine, as well, since it sort of implies that s
out a new approach that makes the problem a lot easier and

It's guess-and-check, not advanced calculus or anything. The problem itself (computing SHA-256 hashes) is not particularly difficult, just time consuming and highly automatable.

But alas, such nuances are too complicated for general audiences

startrek

subscribe 85,965 readers

~93 users here now

subscribe 229,755 Bothans

326 dying to bring us information

Bitcoin

unsubscribe 148,350 readers

1,398 users here now

Bitcoin is *the currency of the Internet*: a distributed, worldwide, decentralized digital money. Unlike traditional currencies such as dollars, bitcoins are issued and managed without any central authority whatsoever: there is no government, company, or bank charge of Bitcoin. As such, it is more resista to wild inflation and corrupt banks. With Bitcoin, you can *be your own bank*.

If you are new to Bitcoin, check out We Use

150

Bitcoin: The magic of mining (economist.com)

submitted 5 days ago by _chmod755_

48 comments share save hide give gold report

all 48 comments - sorted by: **best**

save

reddiquette formatting help

[–] **mshadel** 27 points 5 days ago

"The machines work ceaselessly, trying to solve fiendishly difficult mathematical puzzles."

Pet peeve of mine. Hashing is more like playing the lottery. It's not a puzzle at all, it's just extremely unlikely that an individual ticket will be a winner. Mining operations are just buying LOTS of tickets.

permalink save report give gold reply

> [–] **thieflar** 6 points 5 days ago
>
> It's a pet peeve of mine, as well, since it sort of implies that some math whiz could come through and figure out a new approach that makes the problem a lot easier and makes them some sort of superminer.
>
> It's guess-and-check, not advanced calculus or anything. The problem itself (computing SHA-256 hashes) is not particularly difficult, just time consuming and highly automatable.
>
> But alas, such nuances are too complicated for general audiences.

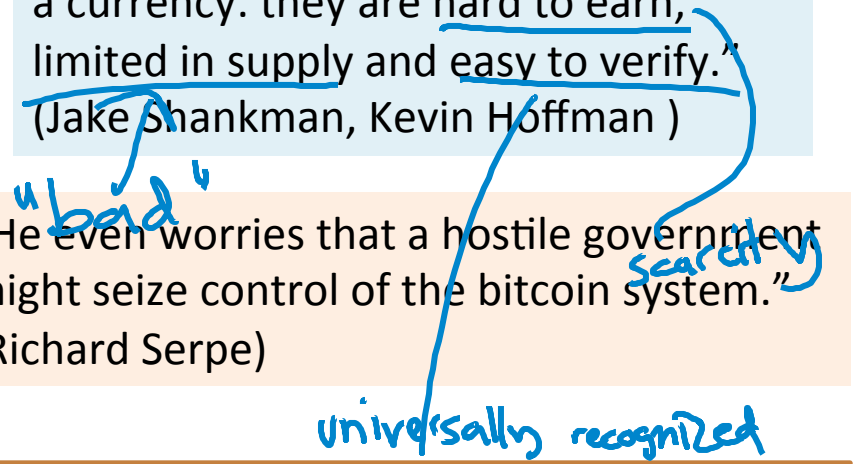
Selected Contributed Comments

"The enigmatic Mr Nakamoto designed the system to keep everybody honest."
(Tara Raj, Jake Rosenberg)

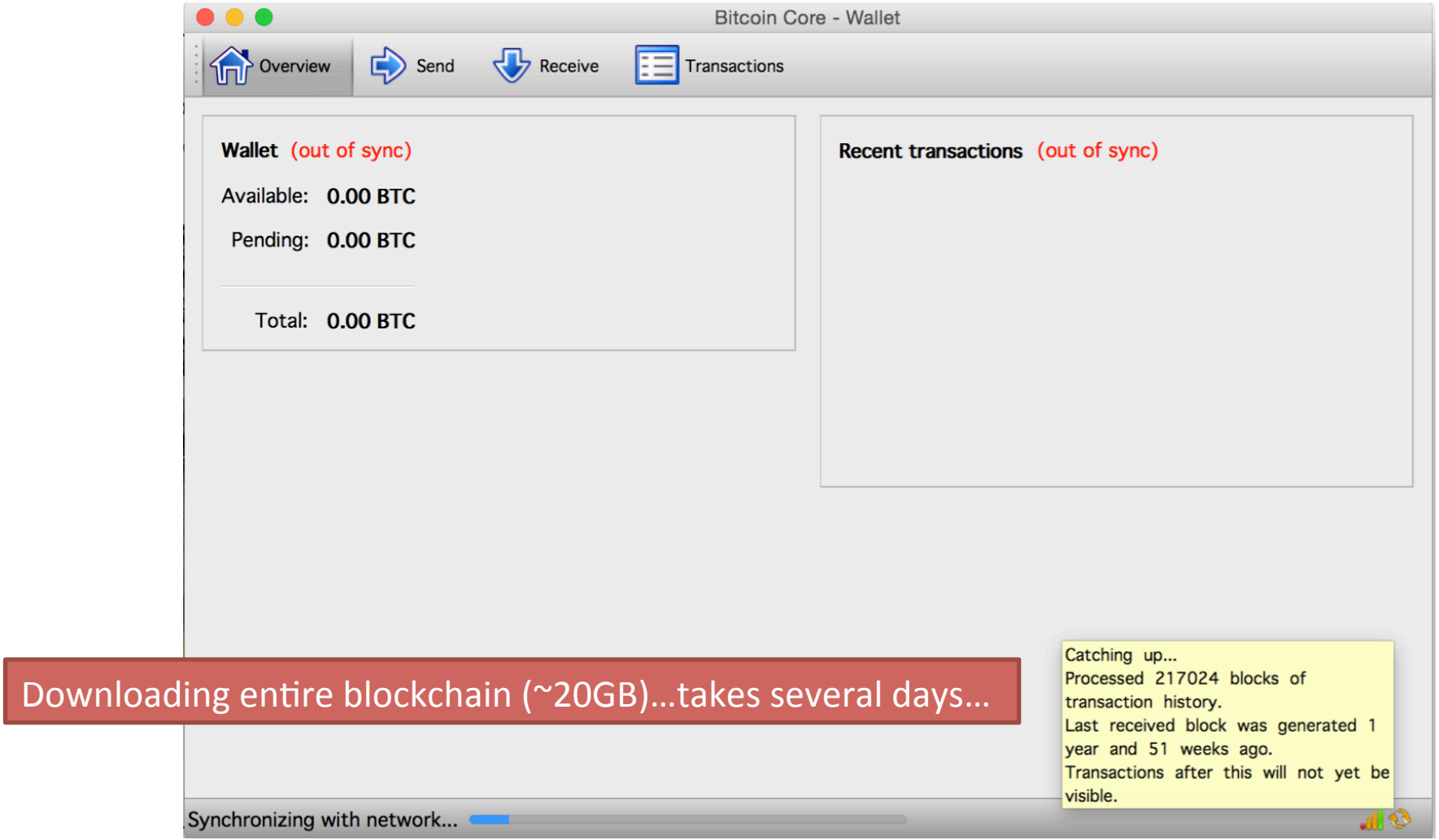
"A more fundamental worry is that digital-currency mining, like other sorts of mining, has environmental costs: all that number-crunching uses a lot of electricity, and not all of it comes from renewable sources…"
(Samuel Abbate, Elizabeth Kukla)

"Bitcoins have three useful qualities in a currency: they are hard to earn, limited in supply and easy to verify."
(Jake Shankman, Kevin Hoffman)

"He even worries that a hostile government might seize control of the bitcoin system."
(Richard Serpe)



Submitting google forms is a silly way to have a discussion! We'll have a course discussion forum set up by next week…


Bitcoin Core - Wallet
Overview
Send
Receive
Transactions
Wallet (out of sync)
Available: 0.00 BTC
Pending: 0.00 BTC
Total: 0.00 BTC
Recent transactions (out of sync)
Downloading entire blockchain (~20GB)…takes several days…
Catching up...
Processed 217024 blocks of transaction history.
Last received block was generated 1 year and 51 weeks ago.
Transactions after this will not yet be visible.
Synchronizing with network...

Recap

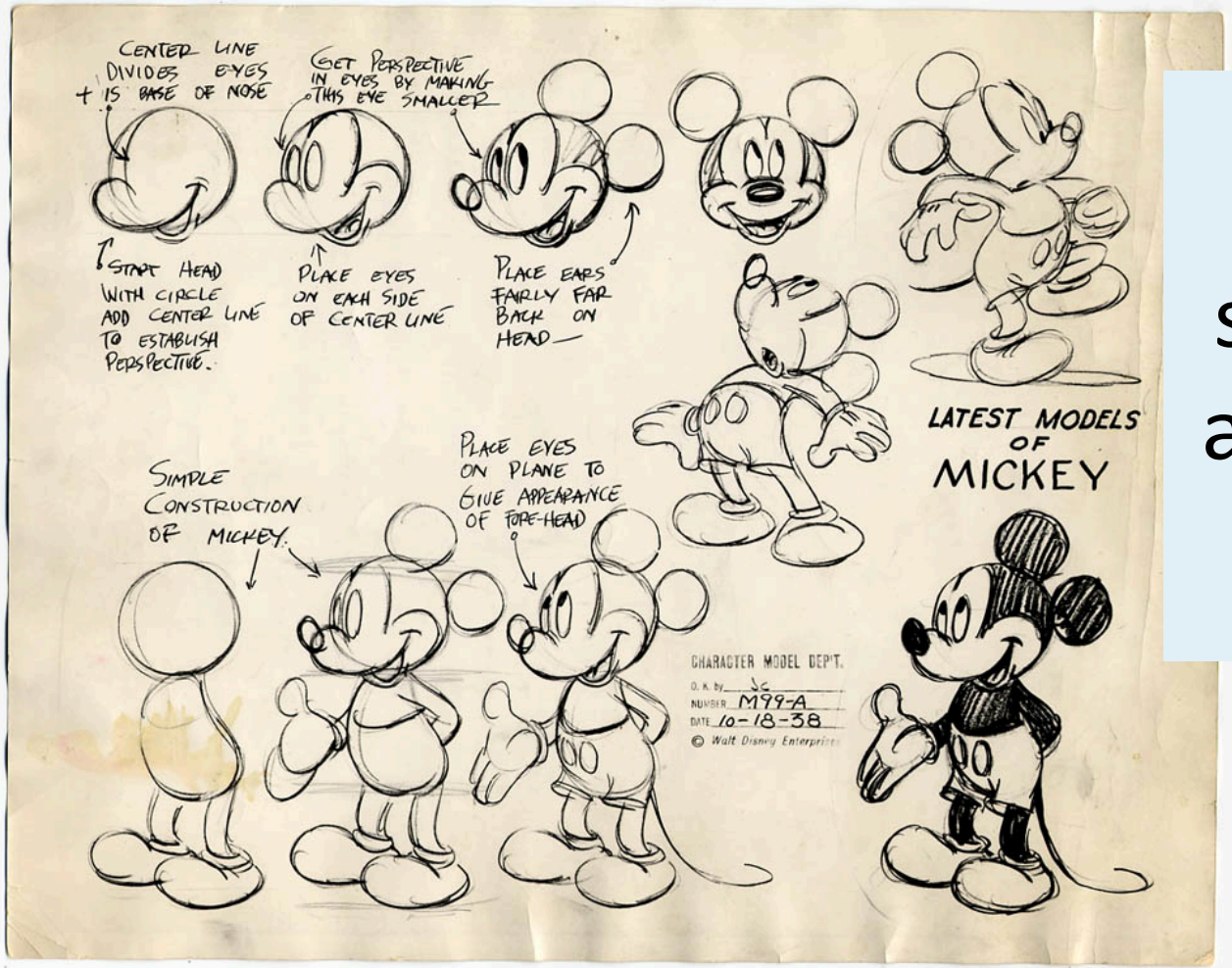
Currency is a ***medium of exchange***

At a minimum, must be:

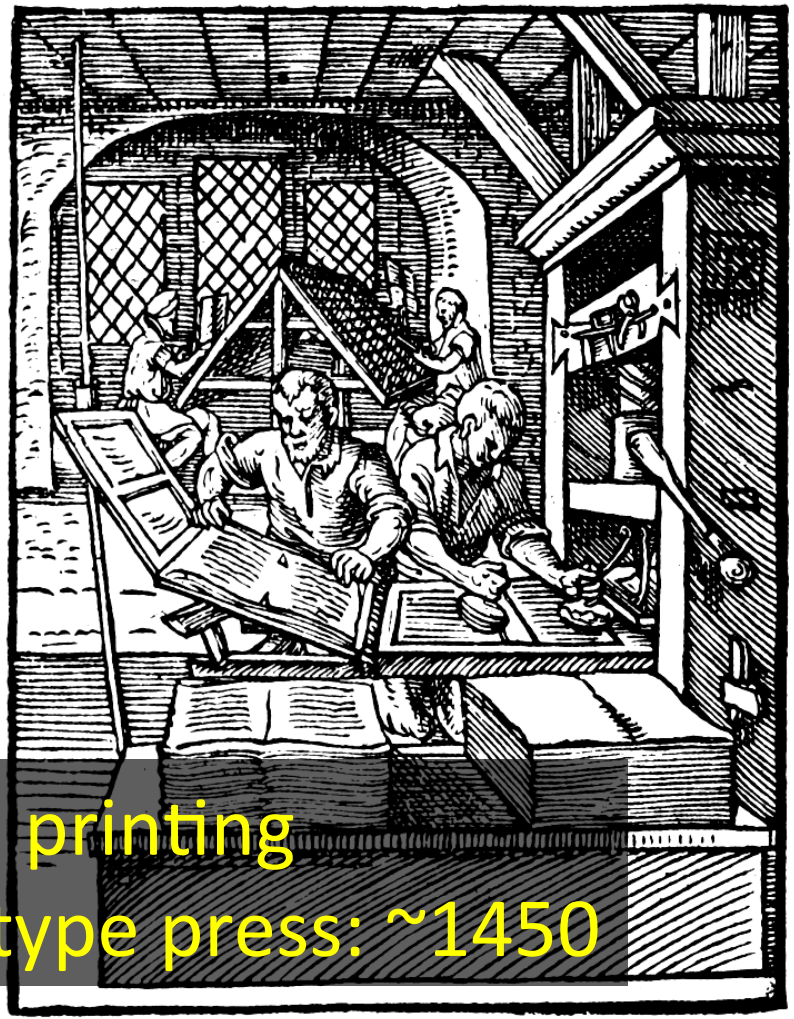
- ***transferable*** – can be exchanged
- ***scarce*** – limited supply

Can we make something scarce and transferable with just bits?


How can someone *own* something made of bits?



How can someone ***own*** anything easily reproduced?



Mechanized printing

Gutenberg movable type press: ~1450

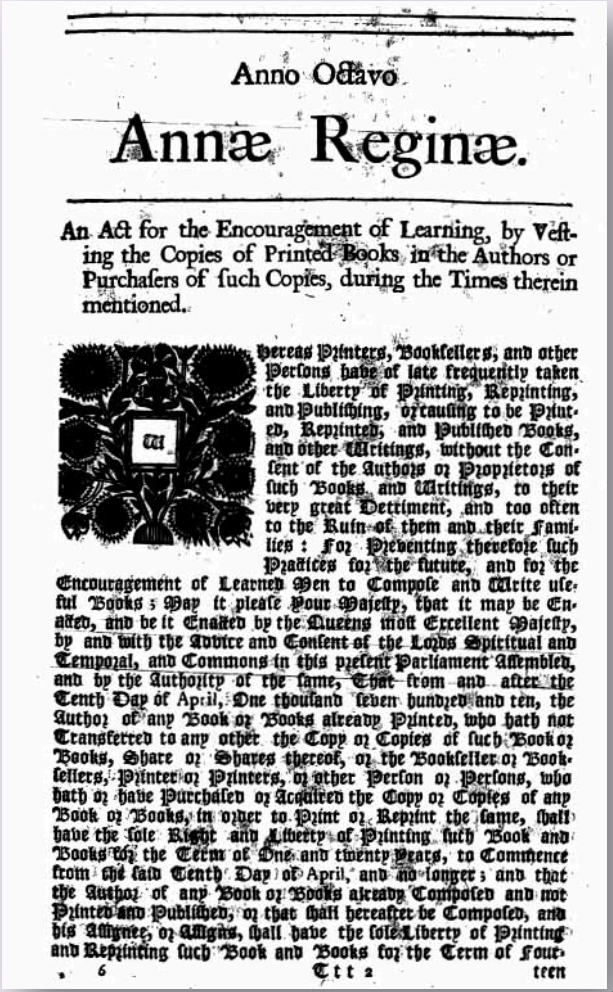
Worshipful Company of Stationers and Newspaper Makers (“**Stationer’s Company**”)

London 1403
Royal Charter 1557
Monopoly on printing
Responsibility to censor

Statute of Anne, 1710

"An Act for the Encouragement of Learning, by Vesting the Copies of Printed Books in the Authors or Purchasers of Copies, during the Times therein mentioned…"

Author has exclusive **14-year** right to copy work (living author can extend for another 14 years)



Anno Octavo

Annæ Reginæ.

An Act for the Encouragement of Learning, by Vesting the Copies of Printed Books in the Authors or Purchasers of such Copies, during the Times therein mentioned.

Whereas Printers, Booksellers, and other Persons have of late frequently taken the Liberty of Printing, Reprinting, and Publishing, or causing to be Printed, Reprinted, and Published Books, and other Writings, without the Consent of the Authors or Proprietors of such Books and Writings, to their very great Detriment, and too often to the Ruin of them and their Families: For Preventing therefore such Practices for the future, and for the Encouragement of Learned Men to Compose and Write useful Books; May it please Your Majesty, that it may be Enacted, and be it Enacted by the Queens most Excellent Majesty, by and with the Advice and Consent of the Lords Spiritual and Temporal, and Commons in this present Parliament Assembled, and by the Authority of the same, That from and after the Tenth Day of April, One thousand seven hundred and ten, the Author of any Book or Books already Printed, who hath not Transferred to any other the Copy or Copies of such Book or Books, Share or Shares thereof, or the Bookseller or Booksellers, Printer or Printers, or other Person or Persons, who hath or have Purchased or Acquired the Copy or Copies of any Book or Books, in order to Print or Reprint the same, shall have the sole Right and Liberty of Printing such Book and Books for the Term of One and twenty Years, to Commence from the said Tenth Day of April, and no longer; and that the Author of any Book or Books already Composed and not Printed and Published, or that shall hereafter be Composed, and his Assignee, or Assigns, shall have the sole Liberty of Printing and Reprinting such Book and Books for the Term of Four-

6 Ttt 2 teen

US Copyright Law

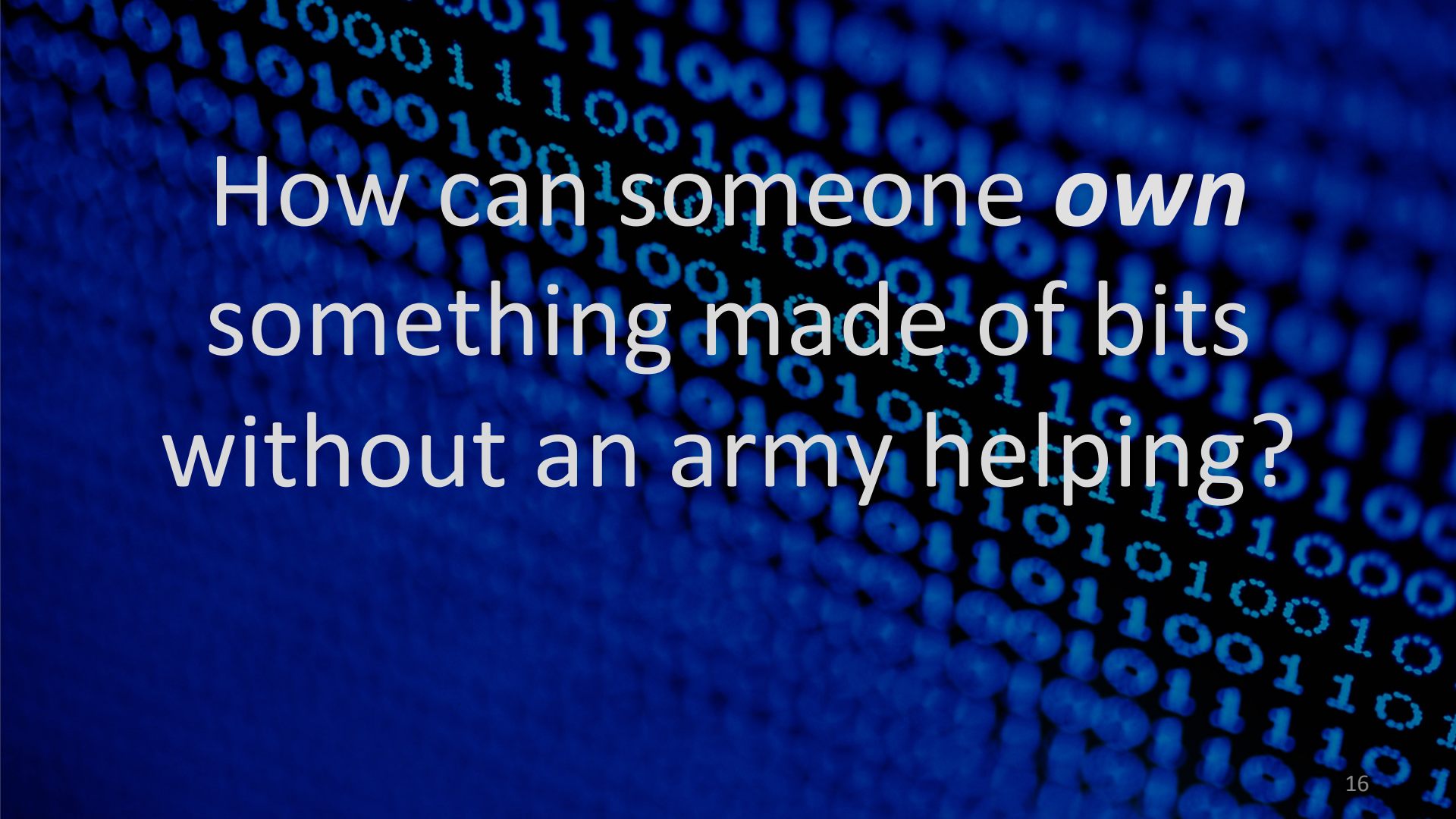
1790: 14 years (+ 14)

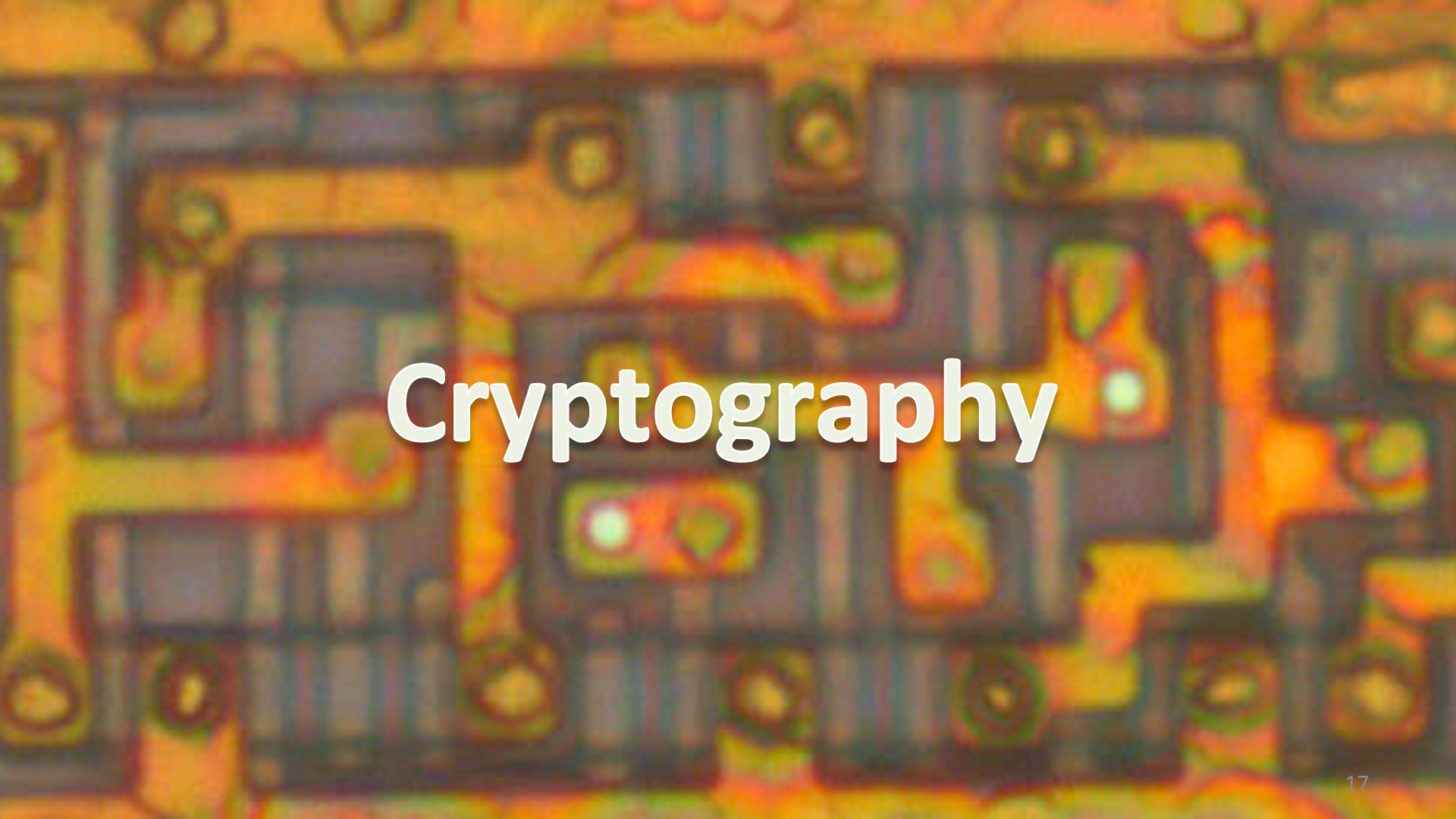
1831: 28 years (+ 14)

1976: life of author + 50 (75 for “corporate”)

1998: life of author + 70 (120 for “corporate”)

Created 1928


How can someone *own* something made of bits without an army helping?


Cryptography

What is cryptology?

Greek: *κρυπτός* = "***kryptos***" = hidden (secret)

Cryptography – secret writing

Cryptanalysis – analyzing (breaking) secrets

- *Cryptanalysis* is what an attacker does
- *Decryption* is what the intended receiver does

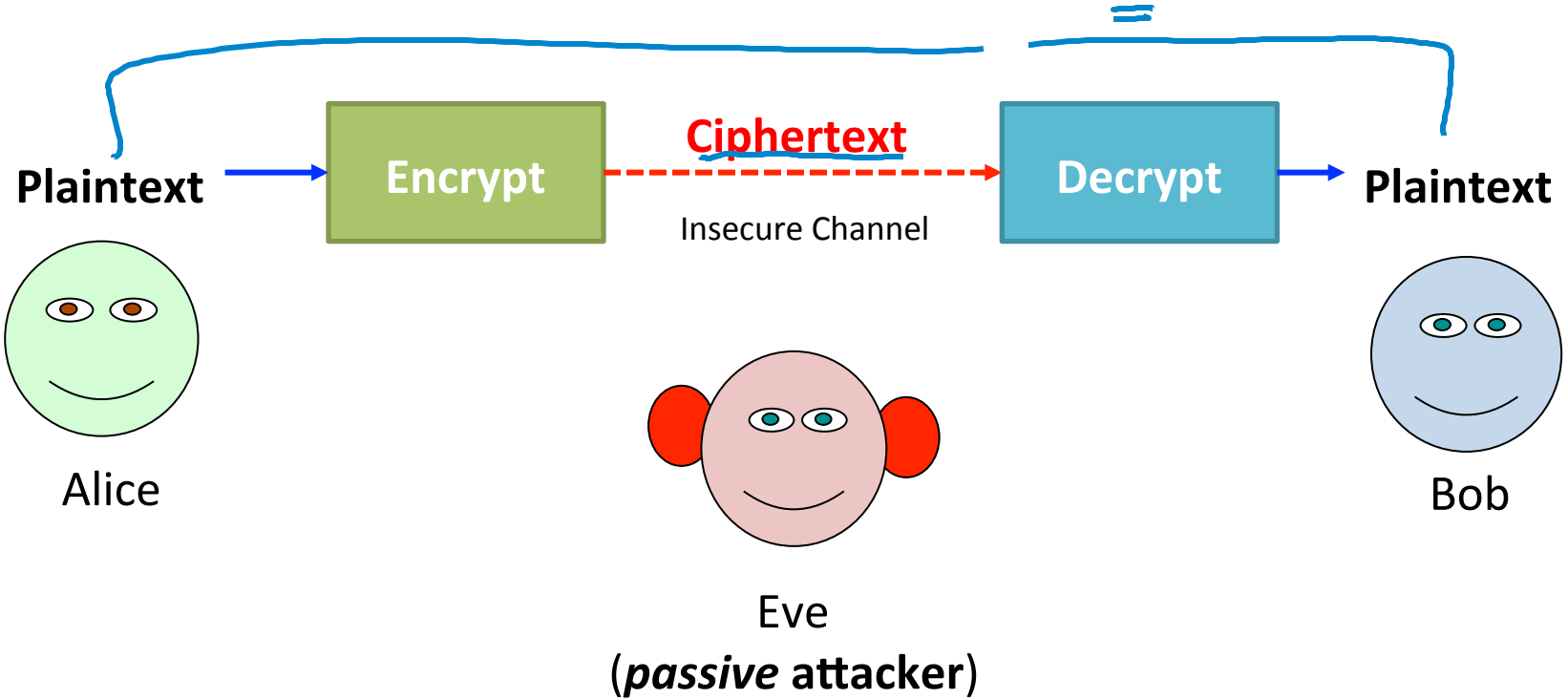
Cryptosystems – systems that use secrets

Cryptology – science of secrets

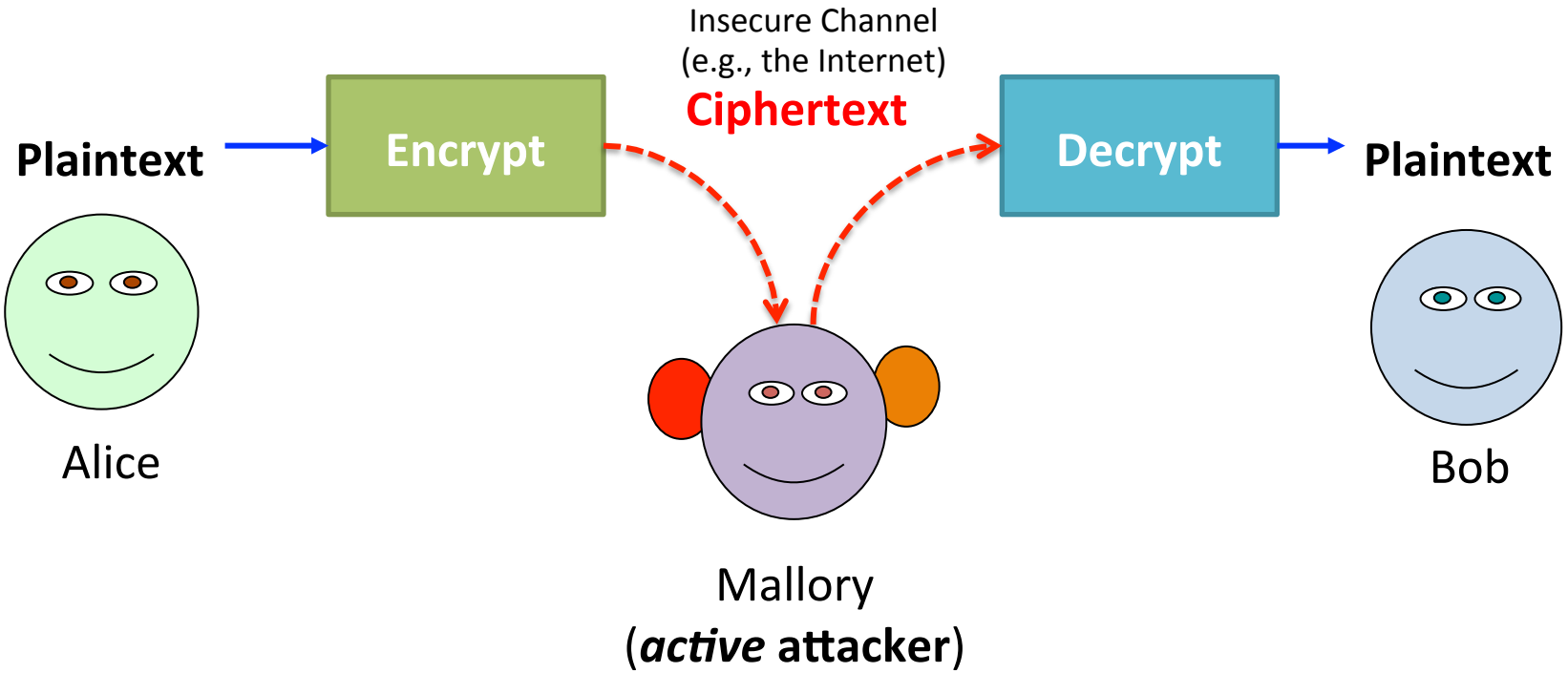
Cryptology is a branch of *mathematics*:
about abstract numbers and functions.

Security is an engineering goal: it involves *mathematics*,
but is mostly about *real implementations* and ***people***.

Introductions



Active Attacker



Message Cryptosystem

Two functions: $E(m\text{: byte}[]) \rightarrow \text{byte}[]$
and $D(c\text{: byte}[]) \rightarrow \text{byte}[]$

Correctness property: for all possible messages m, $D(E(m)) = m$

Security property: given $c \leftarrow E(m)$, it is "hard" to learn *anything interesting* about m.

Shafi Goldwasser and **Silvio Micali**
2013 Turing Award Winners
(for doing this in the 1980s)

It **is possible** to state the security property precisely (and prove a cryptosystem satisfies it given hardness assumptions).

Message Cryptosystem

Two functions: $E(m:$ byte[]) ➔ byte[]
and $D(c:$ byte[]) ➔ byte[]

Correctness property: for all possible messages m, $D(E(m)) = m$

Security property: given $c \leftarrow E(m)$, it is "hard" to learn *anything interesting* about m.

Kerckhoff's Principle

JOURNAL

DES

SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

mechanism not secret

2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

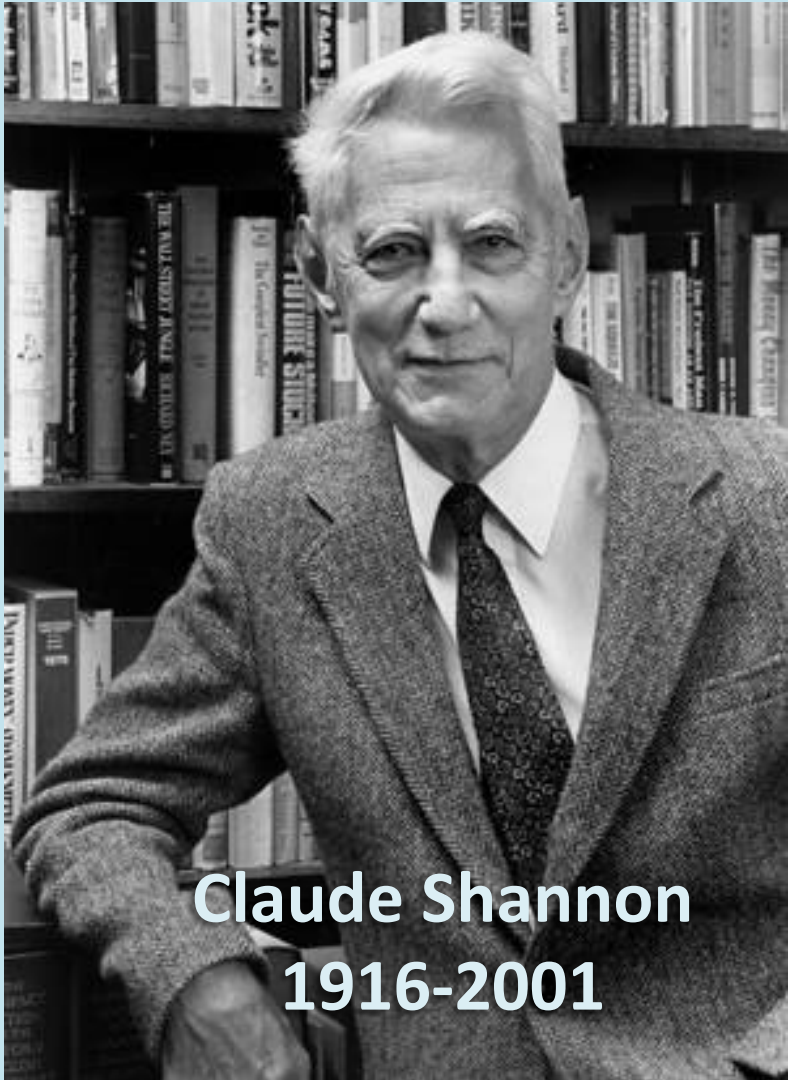
enemy

A. Notions historiques.

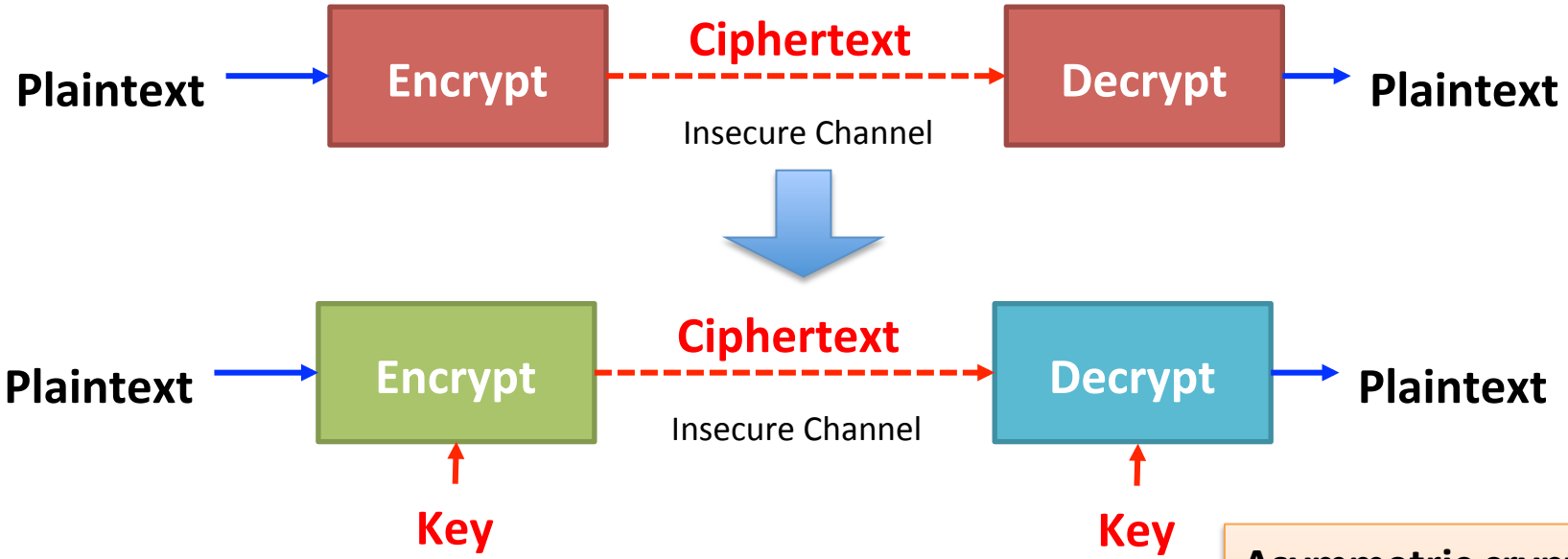
La *Cryptographie* ou l'*Art de chiffrer* est une science vieille comme le monde ; confondue à son origine avec la télégraphie

Auguste Kerckhoffs

"The enemy knows the system being used."
Claude Shannon, *Communication Theory of Secrecy Systems* (1949)



(Keyed) Symmetric Cryptosystem



Only secret is the key, not the E and D functions that now take key as input

Asymmetric crypto: different keys for E and D, so you can reveal E without revealing D.

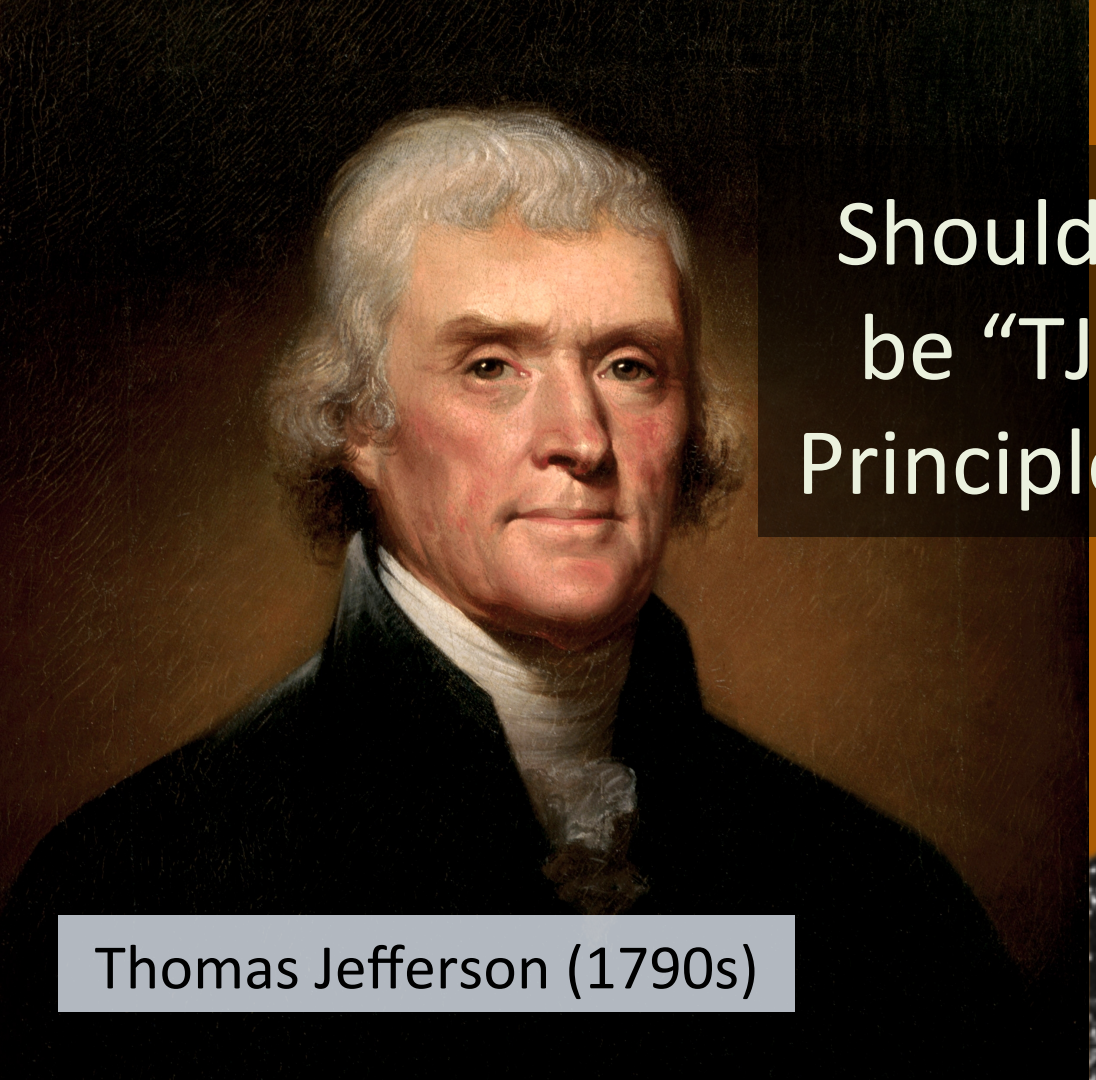
Jefferson's Wheel Cipher

Jefferson's Wheel Cipher

26 wheels arranged in a **secret order** on a spindle, each wheel has **randomly-permutated alphabet** around rim

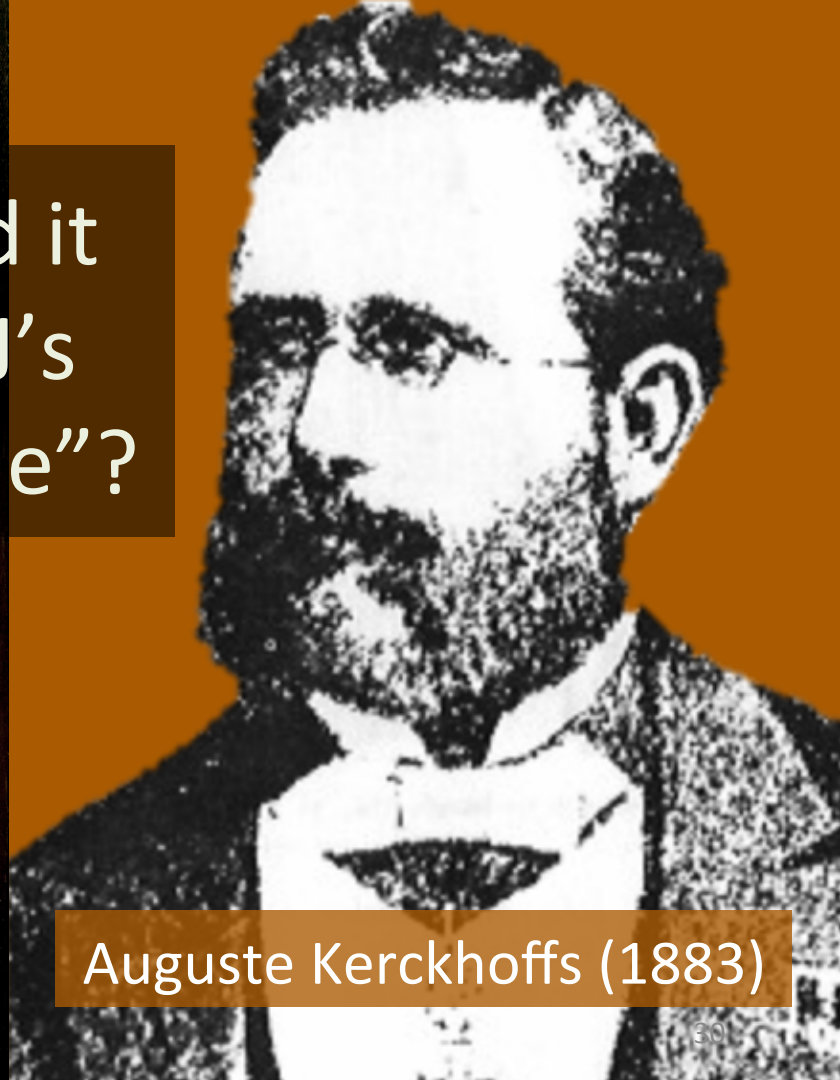
Encrypt: turn wheels to display plaintext, then pick a **"random"** row as ciphertext

Decrypt: arrange wheels in same (secret) order, line up ciphertext, look for plaintext



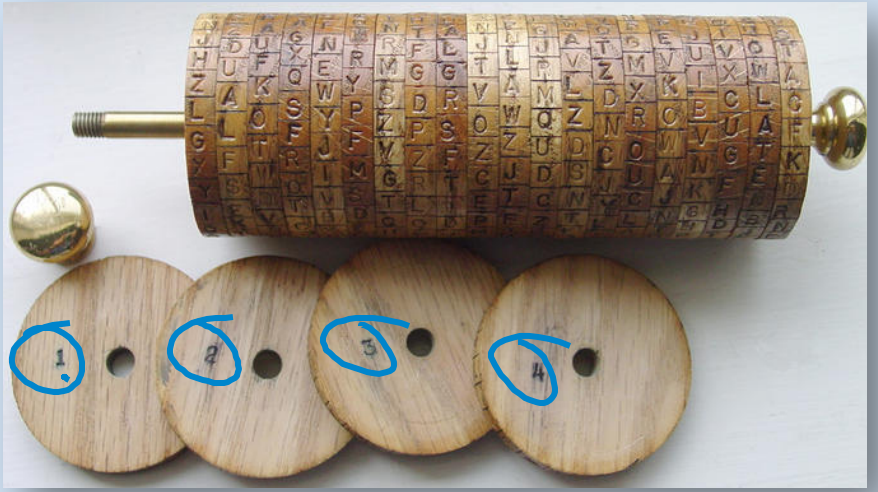
Thomas Jefferson (1790s)

Should it be “TJ’s Principle”?



Auguste Kerckhoffs (1883)

on the periphery of each, and between the black lines, put all the letters of the alphabet, not in their established order, but jumbled, & without order, so that no two shall be alike. ***now string them in their numerical order*** *on an iron axis, one end of which has a head, and the other a nut and screw; the use of which is to hold them firm in any given position when you choose it.*



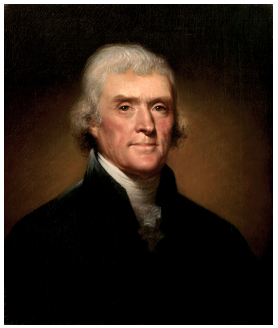
Jefferson's description of wheel cipher (1802)

Key Space

Key space: K = set of possible keys

Key is **order of wheels** on spindle:

$$|K| = 26 \times 25 \times \ldots \times 1 > 10^{26}$$



Key is **jumbling of letters on wheels**:

$$|K| = (26 \times 25 \times \ldots \times 1)^{26} > 10^{691}$$

Brute Force Attack

Try all possible keys in some order,
until you find one that works.

```
def brute_force(ciphertext):
    for guess in all_possible_keys(N):
        plaintext = decrypt(key, ciphertext)
        if plausible_message(plaintext):
            return plaintext
```

What is necessary for brute force attack to succeed?

(Im)Practicality of Brute Force Attacks

Minimum energy needed to flip one bit

(*Landauer limit*) ≈ $kT \ln 2 \approx 2.8$ zepto-Joules

$k \approx 1.4 \times 10^{-23}$ J/K (Boltzmann's constant)
T = temperature (Kelvin) (300K)

Bit Flips	Energy	WolframAlpha Description
2^{56} (DES)	2×10^{-3} J	"acoustic energy in a whisper"
2^{80} ("low security")	3×10^{3} J	"metabolic energy of one gram of sugar"
26! (Jefferson+Kerkchoffs)	1×10^{6} J	"energy of one gram of gasoline"
2^{128} (AES minimum)	9×10^{17} J	"twice energy consumption of Norway in 1998"
2^{256} (AES maximum)	3×10^{56} J	"1/120th mass energy equivalent of galaxy's visible mass"

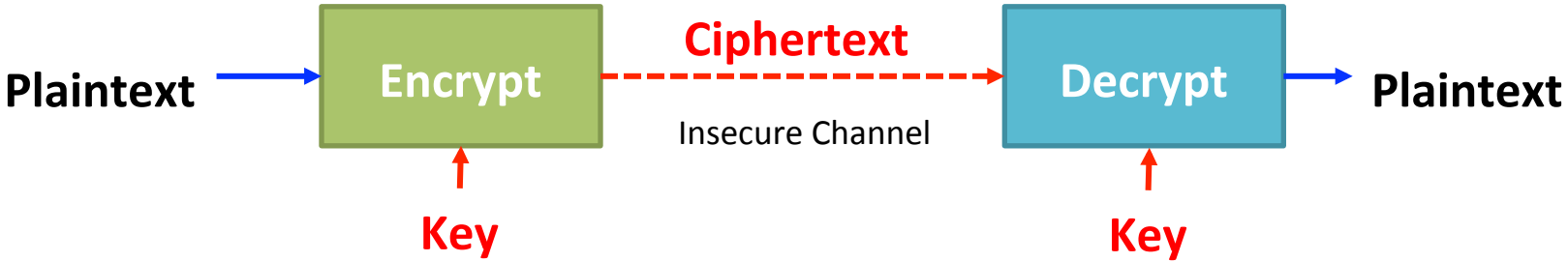
Bit Flips	Energy	WolframAlpha Description
2^{56} (DES)	2×10^{-3} J	"acoustic energy in a whisper"
2^{80} ("low security")	3×10^{3} J	"metabolic energy of one gram
(Jef		oline"
2^{128}		on of
2^{256} (AES maximum)	3×10^{56} J	"1/120th mass energy equivalent of galaxy's visible mass"

This is the best (unrealistic) possible case for a **brute force attack**: don't need to do anything other than represent key and physically most efficient bit flips.

Bit Flips	Energy	WolframAlpha Description
2^{56} (DES)	2×10^{-3} J	"acoustic energy in a whisper"
2^{80} ("		ram
(Jeffe		line"
2^{128} (A		n of
2^{256} (AES maximum)	3×10^{56} J	"1/120th mass energy equivalent of galaxy's visible mass"

But, assumes better than brute force attacks are not possible. **All of these ciphers have weaknesses**, and are much less secure than maximum security possible for that size key.

Can we use symmetric cryptosystems to ***own*** bits?

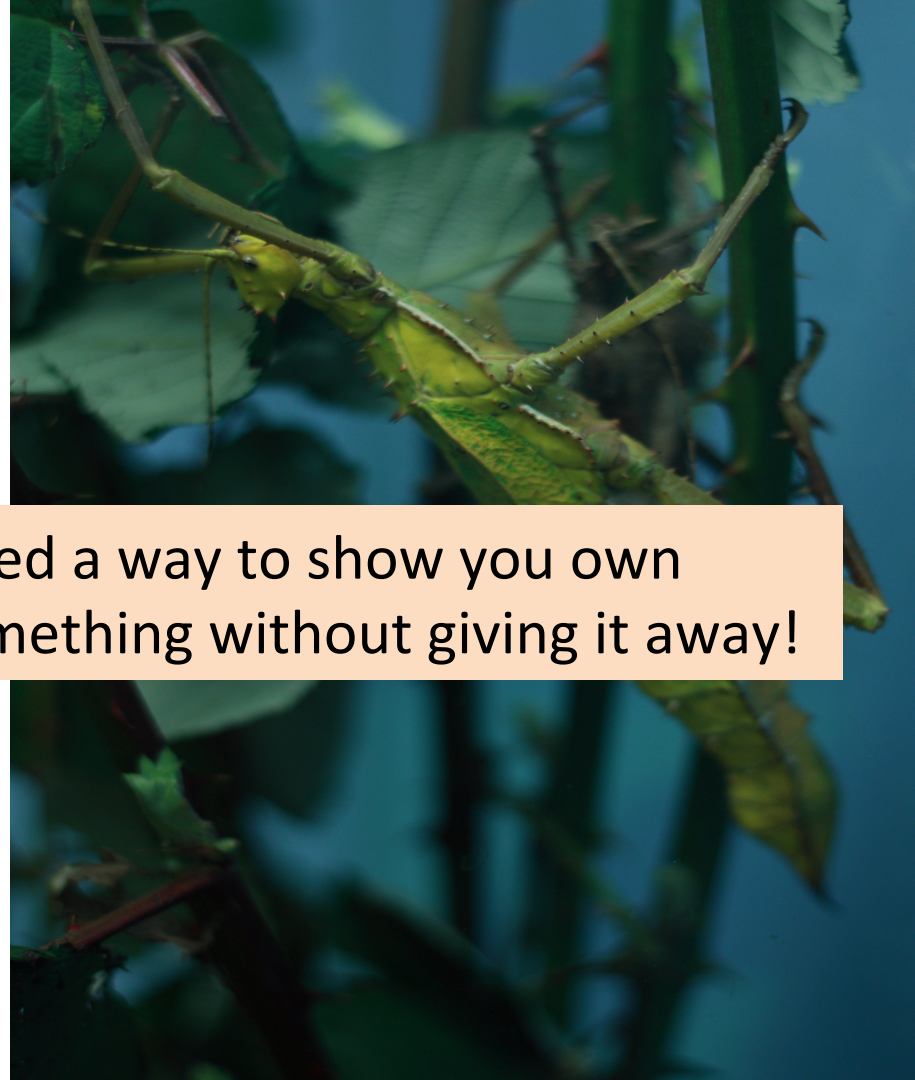



Asymmetric Cryptography
小 心 碰 头
MIND YOUR HEAD

Asymmetry Required

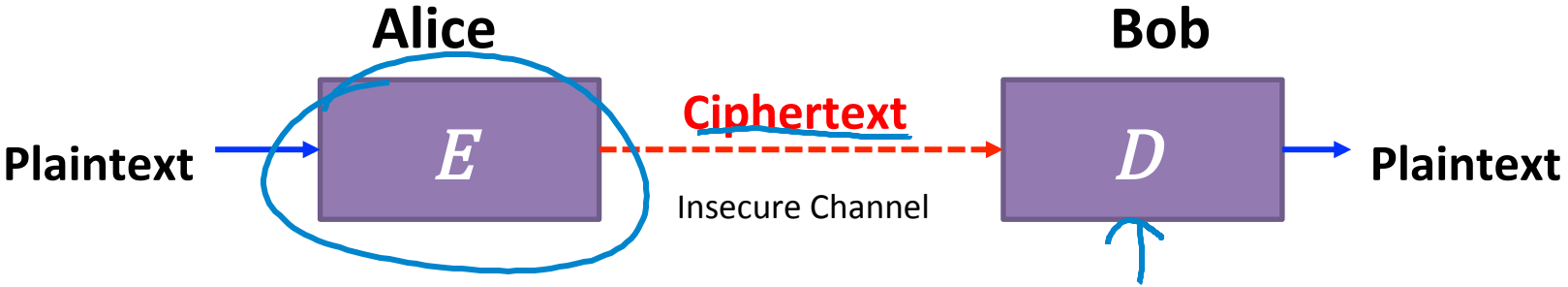
Messages: send Alice a message that only Alice can read

Signatures: verify Alice signed a message, but not impersonate Alice



Need a way to show you own something without giving it away!

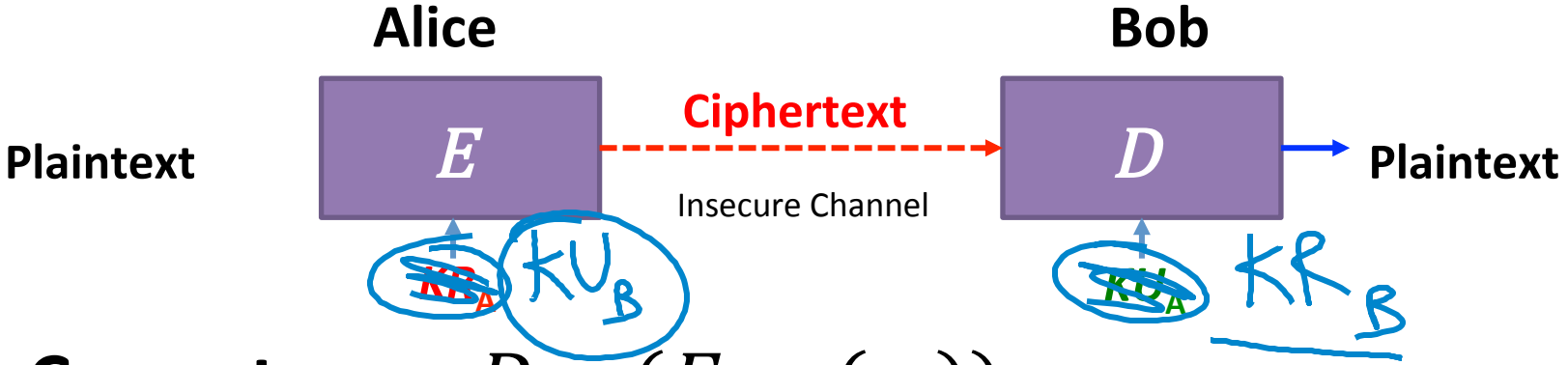
Asymmetric Cryptosystem



Correctness: $D(E(m)) = m$

Security: given $E(m)$ and E, cannot learn anything interesting about m or D

Asymmetric Cryptosystem (with **Kerckhoffs' Principle**)



Correctness: $D_{KU_A}(E_{KR_A}(m)) = m$

Security: given $E_{KR_A}(m)$, E, KU_A, and D, cannot learn anything interesting about m or KR_A.

Providing **Asymmetry**

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

No function (publicly) known with these properties until 1977…


Len Adleman
Adi Shamir
Ron Rivest

RSA Cryptosystem

$$E_e(M) = M^e \bmod n$$

$$D_d(C) = C^d \bmod n$$

public

Bitcoin uses elliptic curves instead of RSA (next week).

$n = pq$ p, q are prime

d is *relatively prime* to $(p-1)(q-1)$

$ed \equiv 1 \bmod (p-1)(q-1)$

Correctness of RSA

$$E_e(M) = M^e \bmod n$$
$$D_d(C) = C^d \bmod n$$

Correctness of RSA

$$E_e(M) = M^e \bmod n$$
$$D_d(C) = C^d \bmod n$$

$$D_d(E_e(M)) = (M^e \bmod n)^d \bmod n$$
$$= M^{ed} \bmod n$$
$$= M$$

This step depends on choosing e and d to have this property: uses Fermat's little theorem and Euler's Totient theorem

Bonus: Works in Both Orders

$$E_e(M) = M^e \bmod n$$
$$D_d(C) = C^d \bmod n$$

$$E_e(D_d(M)) = (M^d \bmod n)^e \bmod n$$
$$= M^{de} \bmod n$$
$$= M$$

Providing **Asymmetry**

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

Does RSA satisfy these?

Using Asymmetric Crypto: **Confidentiality**

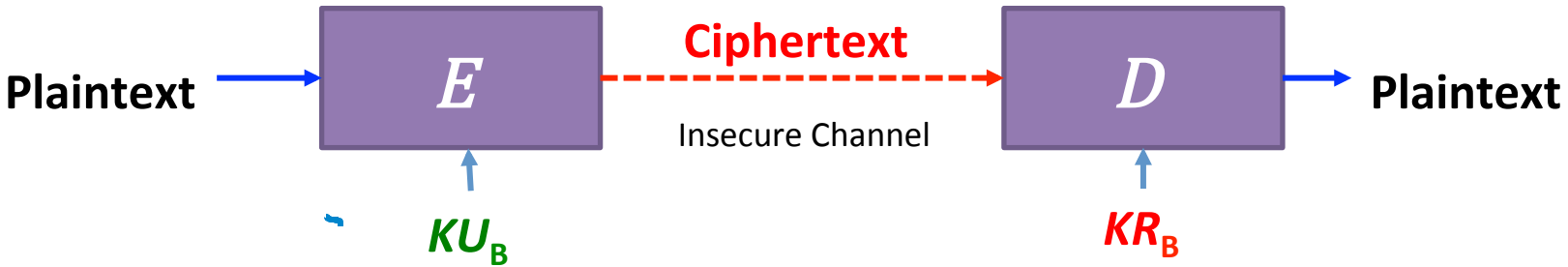
Alice

Sends confidential messages to Bob using his public key

Bob

Generates key pair: KU_B, KR_B

Publishes KU_B



~10000*x* slower than AES! Only use when asymmetry is needed.

Using Asymmetric Crypto: **Signatures?**

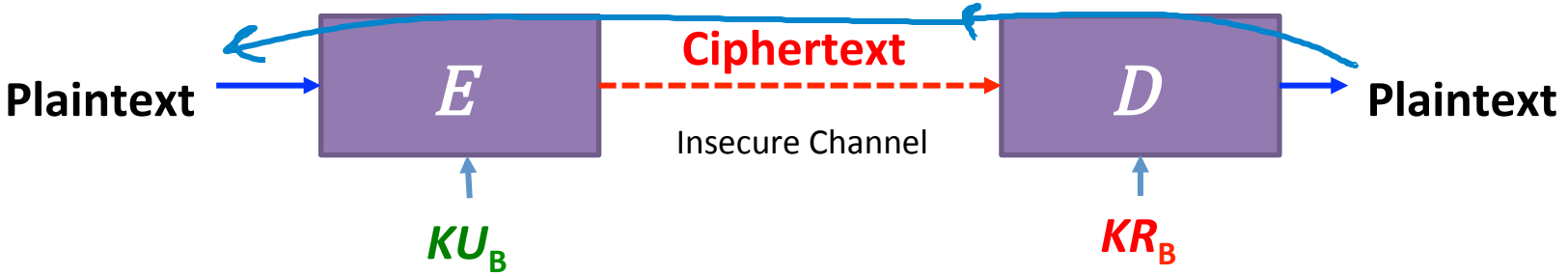
Alice

Sends confidential messages to Bob using his public key

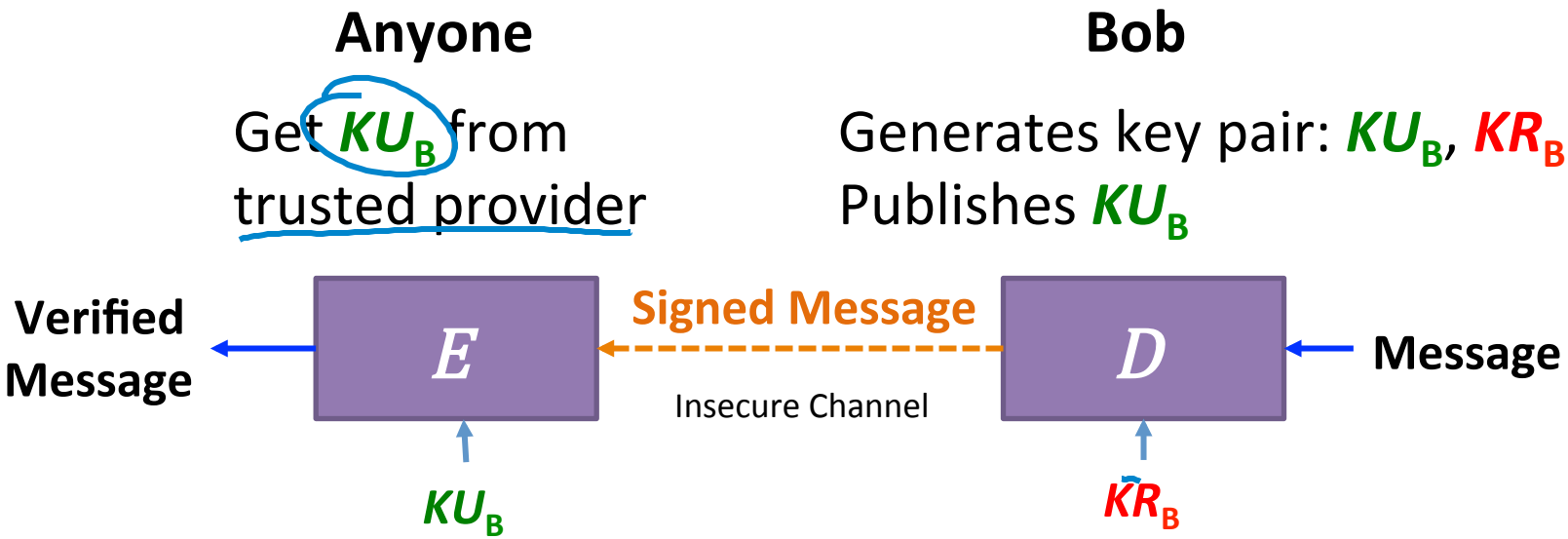
Bob

Generates key pair: KU_B, KR_B

Publishes KU_B

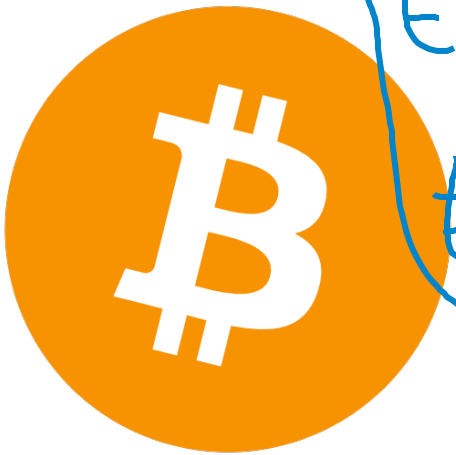


Using Asymmetric Crypto: **Signatures**




Can we make money yet?

Owning a Coin



$E(PR_y$ "I'm giving A to q. - PU_y "

$E(PR_x$, "I'm giving coin x to y.

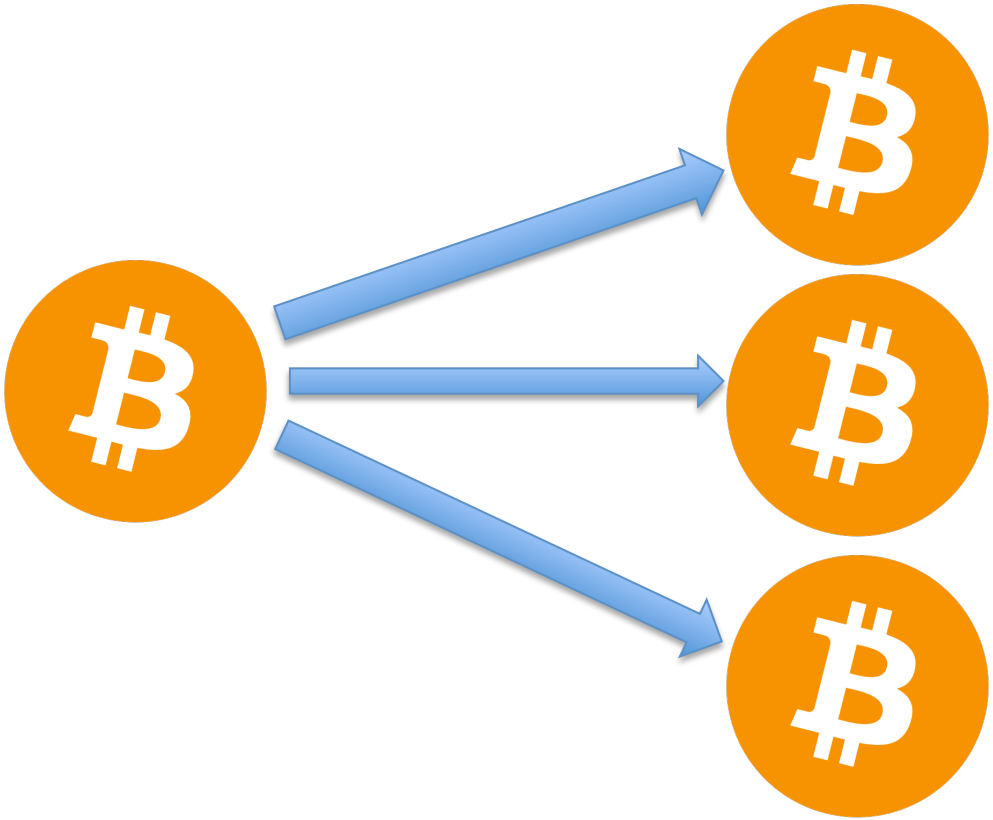
Coin ≈ public key

$E($"I own Coin x." and no else does.", $PR_x)$

Private key = "Owner"

(PU_x, PR_x)

Getting Rich!



Charge

- Achieving **scarcity** is a hard problem!

- No class Monday (Martin Luther King Day)
- See notes for readings
- Project 1 will be posted in a few days