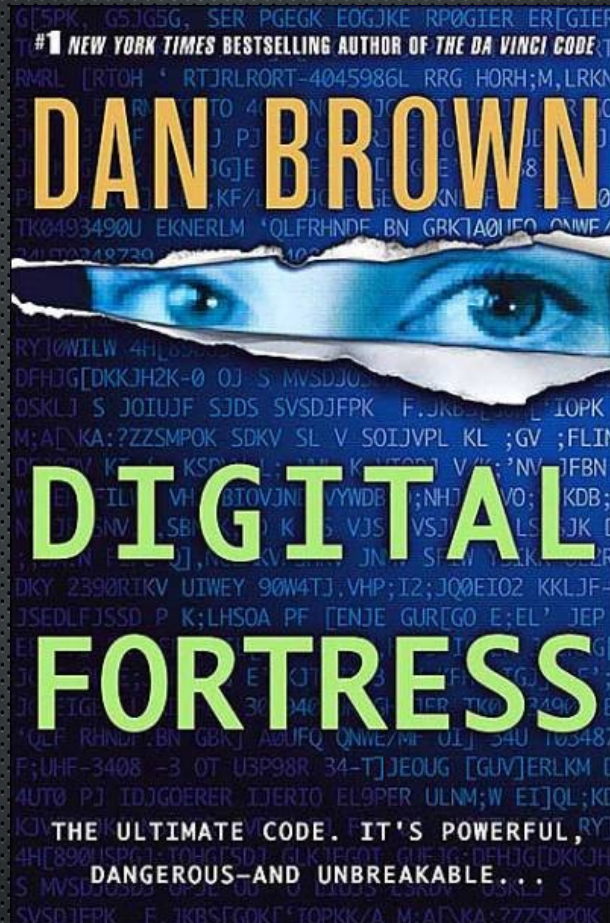


LIS-3353

One way milkshake stuff



Dan Brown is fun..but I threw this
book across the room..



We (probably, if not certainly) still
have unbreakable encryption.

yep. Even given all this NSA stuff.

But you have to be SUPER careful.

Encryption

Alice needs to send a verifiable message to Bob, but Carol is trying to listen in.

“This is a conversation between A and B so you can C your way out!”

Old school

Caesar Cipher. (yes, this really used to fool people)

DWWDFN WKH HDVW ZLQJ RI WKH IRUW
DW WKUHH RQ WKXUVGDB..

attack the east wing of the fort at three on
thursday

Also, hiding the message itself?

- Shave a guy's head, write the message on it.

....and wait.

Steganography

- Hiding the fact that the message (or payload) exists at all

Examples:

- fake personal ad to say something else
- - having a safe but hiding valuables in a shoebox
- - weird bits in a jpg

Steganography as (online) strategy?

Bad, because: Robots and radio



Better to be like “Yeah, you can have a copy.
Too bad you STILL can't read it. HA!”

Other old school strategies

- Navajo Code Talkers
- Harriet Tubman “Wade in the water”

Languages, dialects, patois'...

CULTURAL ENCRYPTION.

CULTURAL AUTONOMY.

Another note on strategy

- Secret method vs.

Public method (but secret key)

(score one more for open-source)



Newer strategies (if you can meet)

The bookstore strategy

OR

The One-Time Pad

but what if you CAN'T meet each other...

From this...



...to this. (and back?)



We need something
“milkshake-y”

What, even for a computer, is VERY FAST in
one direction..

..and IMPOSSIBLY SLOW in the other?

Hey, remember this?

24

/ \

4 6

/ \ / \

2 2 2 3

What about 17?

PRIME!

Shortcuts to factoring?

(Let's hope not.....)

But, we need MATH, since online = numbers.

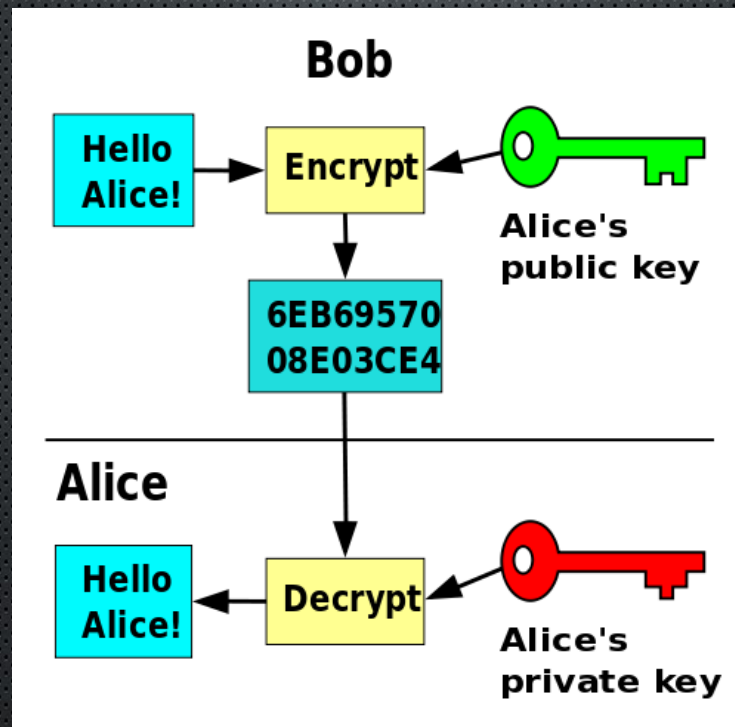
Hey, remember that prime number stuff? (warning, fake numbers below)

92348203942.....(random prime)
x 28059273729.....(random prime)

189808591765.....(big ol' composite)

Public Key Encryption

- Usually, with a physical key, you just have one key, right? The key that locks your door also unlocks it....but what if you separate those two? One does the locking, the other unlocking?



Recap

- To encrypt:

big composite number + clear message = coded text
(public key)

To decrypt

two primes + coded text = clear message
(private key)

Phil Zimmerman invents this and says “hey, this is pretty good privacy. I'll open source it...”



Eben Moglen calls him up a few hours later:
“Cool idea, bro.”

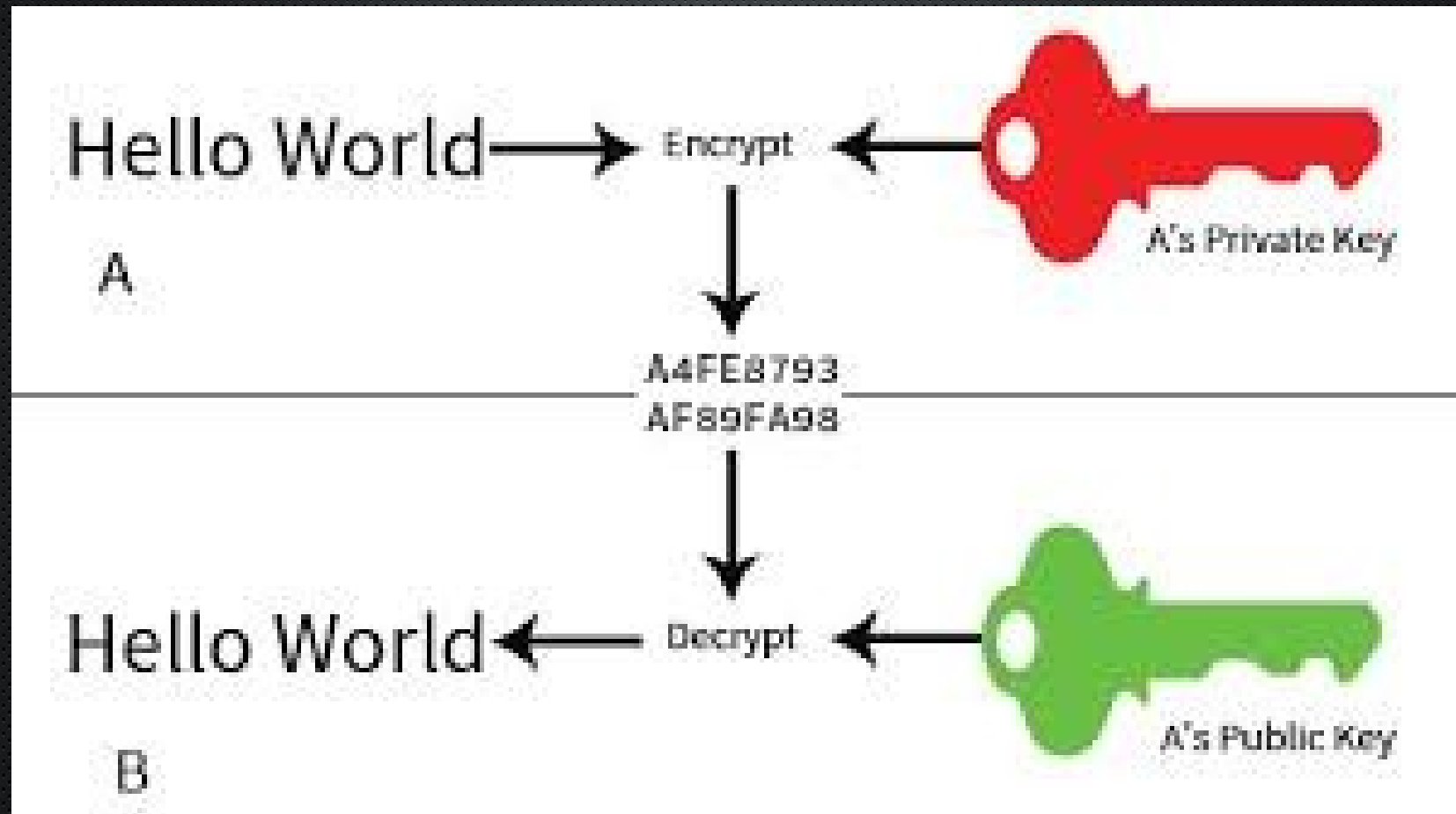
“also, in 5 hours when the FBI kicks down your door and throws you in jail, holler at me.”



Phil's a free man today. Why?

- ...he did something else at the same time, with the same technology.

Let's do something weird.
Let's do the opposite.



Who's more powerful than the government?

Even a government that is trying to stop terrorism?

The logo for amazon.com, featuring the text "amazon.com" in a bold, black, sans-serif font. Below the text is a curved orange arrow pointing from the letter 'a' to the letter 'z'.

Gotta sign those checks and credit cards...

- Encryption and digital signatures are two sides of the same coin.

You need digital signatures to send money, so we also have encryption. (mostly)

Other Milkshakekey Topics

- File/Message Verification
- Smart Password Storage
- Cryptocurrencies (e.g. Bitcoin)

But...the NSA?

...will discuss further :)