



Haym @SalomonCrypto

Sep 25 · 21 tweets · [SalomonCrypto/status/1574107693580550144](https://twitter.com/SalomonCrypto/status/1574107693580550144)

(1/20) What is a Computer? What are their origins and why do we care so much about them?

A brief discussion of the history, function and purpose of computers.

(2/20) There is only one truth in this world.

Computers only know how to "think" in numbers and math, while humans think in words and ideas. But taking a step back, both math and human thought are methods of discovering and communicating the one global truth.

(3/20) This is a huge idea, much too big for the scope of this thread. For now, we will take this as fact:

Anything that can be expressed in and manipulated by thought can also be expressed in and manipulated by math.

Is computer science without computers just maths?



Barry Rountree

Computer Scientist, LLNL · Upvoted by

Daniel R. Page, [Theoretical Computer](#)

[Scientist](#) Author has **7.3K** answers and **38.9M...**

As chemistry without chemicals is just math, as physics without matter is just math, as biology without life is just math.

(4/20) Expressing a statement mathematically gives you the ability to show the statement is logically guaranteed to have a specific conclusion.

"Give me half" is an idea with an ambiguous result. "Give me 50% of your 10" is a mathematical statement with a specific result.

(5/20) The problem with math is that humans are very, very bad at it. Even the simple stuff is super tedious, the abstract stuff is near inaccessible.

And so, we started building machines to help us.

(6/20) Throughout history thousands of different machines have been built to help humans with difficult computation, but it wasn't until the middle of the 20th century when things start to get really interesting.

(7/20) Just like many of our modern foundational technologies, the development of computers was accelerated by war.

The wars of the 1900s were largest and most complicated wars ever fought: WWI and WWII.

(8/20) In wartime, communication is a critical process.

Good communication is required to field an effective military and to seize opportunity (and avoid disaster).

Poor communication leads to ruin.

(9/20) But there is another issue with communication: it can be overheard.

Especially considering the technology. Especially considering the size and scale of the people involved. Especially in the chaos of war.

(10/20) Overheard communication can be worse than no communication at all; this kind of eavesdropping allows your enemy to stay one step ahead of you.

Everything you plan will be expected, prepared for and will immediately provoke retaliation (if not preemption).

(11/20) During WWII especially, as logistics grew more complex and more broad, militaries and governments were required to relay more and more information to more and more people.

Unfortunately, the technology didn't (and largely still doesn't) allow selective broadcasting.

(12/20) The way digital communication works (wirelessly or not) allows anyone with access to the channel to read all of the communication. Given the scope and chaos of WWII, both sides had pretty regular access to the other's channel.

And so, a new solution was needed.

(13/20) The problem: Alice wants to send a private message to Bob over a public channel.

The solution: what if we spoke in a secret language?

(14/20) The problem with the naïve approach is that anyone that can speak the secret language can still listen in. If we continue to communicate in that language, eventually people are going to figure it out.

What if we used a new language every single day?

(15/20) For humans, who live in the world words, this is an incredibly difficult concept.

For computers, who live in the world of numbers, this is easy. We won't go into details here, but suffice to say that you can use math to both change a message and to recover the original.

(16/20) All participants of WWII understood this and attempted to build systems that leveraged this fact to create secure communications.

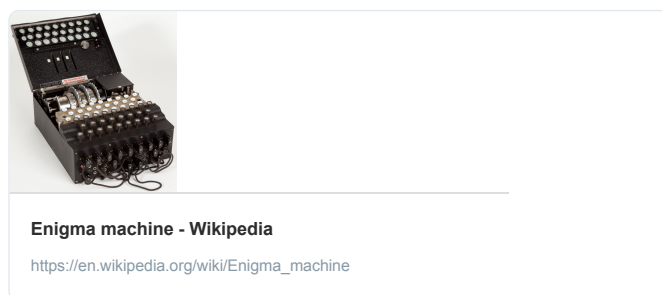
In particular, Nazi Germany developed a particularly strong system to encrypt their messages... they thought.

(17/20) Turns out, they had made a few costly errors that completely compromised their system and gave the allies a HUGE advantage early in the war.

Eventually they understood their mistake, but by that point a computational arms race was well underway.

(18/20) The history is actually very cool and I suggest you continue reading, but we will drop off here.

For us, the point is simple: war created the need for humans to process and transmit information MUCH faster than we can on our own.



(19/20) Modern computing continues on from WWII all the way to the smartphone you are (probably) reading this tweet from... every year getting both more powerful and much smaller.

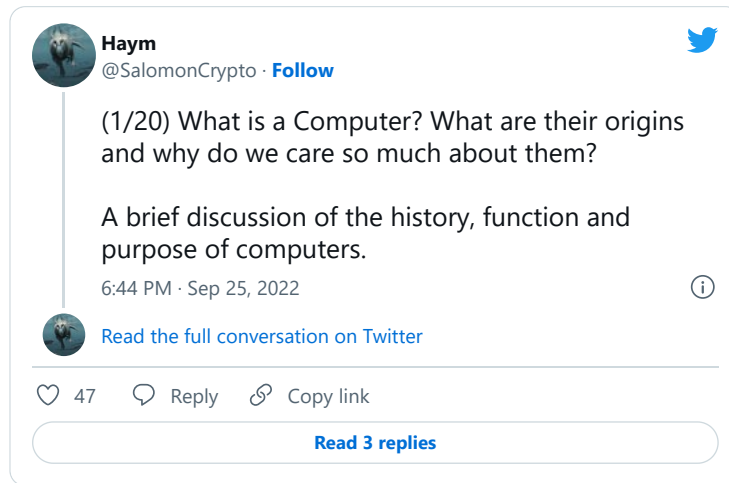
Always pushing towards the same goal:

(20/20) Computers create a context for the world's truth to be expressed and evaluated in their explicit mathematical form, allowing us to form definite proofs and make credible future projections.

And, of course, computers are the tools by which humans can access that space.

Like what you read? Help me spread the word by retweeting the thread (linked below).

Follow me for more explainers and as much alpha as I can possibly serve.



...