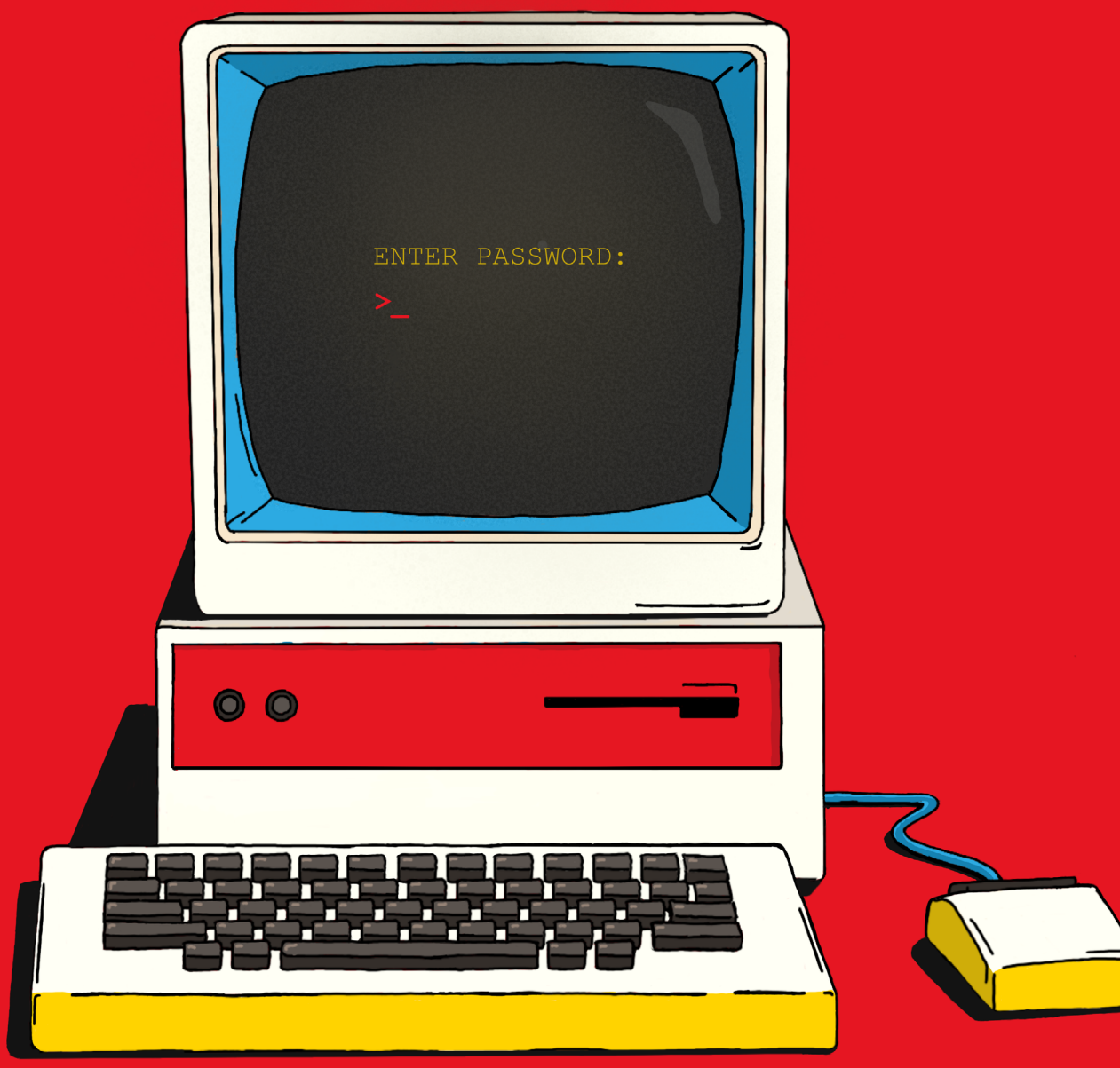
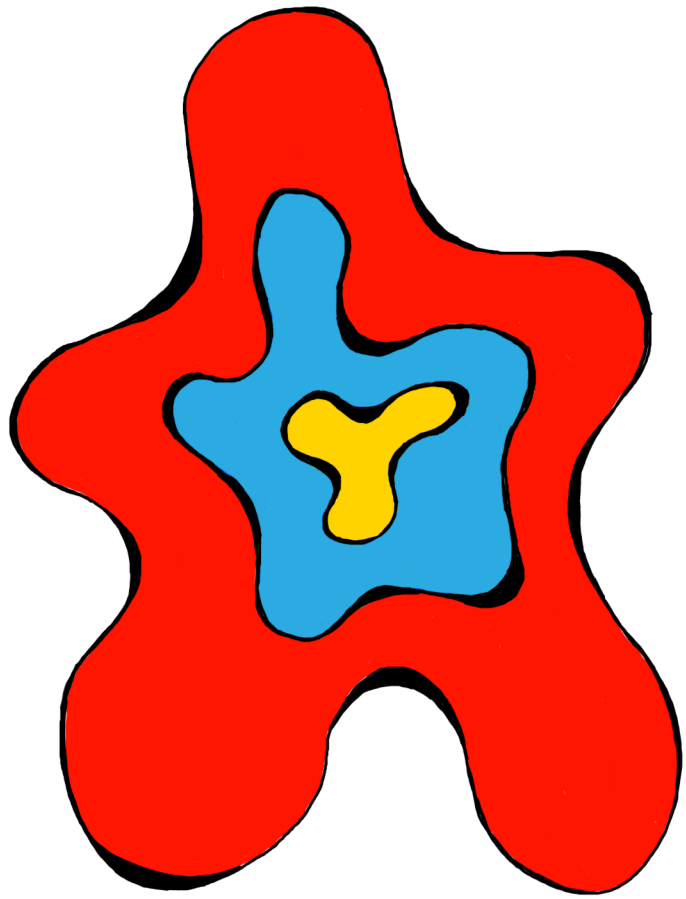
FRONTIER



Cryptography



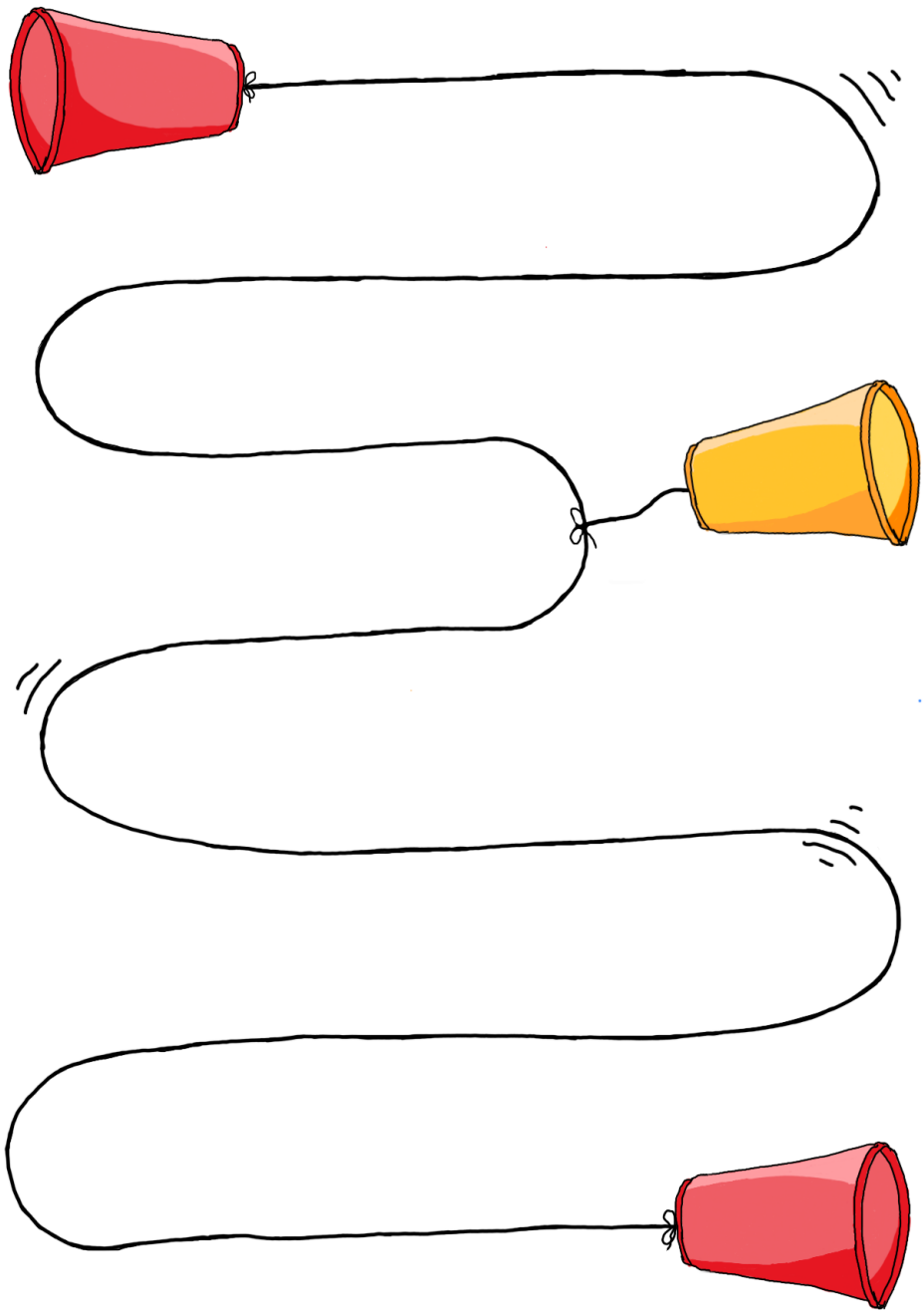
“I have no special talents.
I am only passionately curious.”

What brought you here? To decide to pick up this book and open it? Perhaps what you and I share is a similar passionate curiosity for all things — that part of our human nature that drives us to explore.

When I was younger, people would ask me what I wanted to be when I grew up. I always struggled to give them a good answer because it wasn’t some occupation I was looking for. I was chasing a feeling I couldn’t yet put into words. I wanted to be on the ground at Bell Labs in the 40’s, CERN in the 50’s, NASA in the 60’s and Silicon Valley in the 70’s. I wanted to feel the buzz and excitement at standing on the edge of the known staring into the endless unknown. That unknown where the brave would venture out into, hoping to push it back, bit by bit. A final horizon which beyond lay opportunity, wonder and hope.

The frontier.

The frontier is a metaphysical boundary between all that we know and all what we don’t. I imagine it as this ever-morphing blob across the multidimensional space that represents our knowledge. The Frontier, is a collection of books that aims to take you, wherever you may currently reside and together make our way to a new pocket of the frontier. This first issue is a ticket out to the nascent galaxy of **cryptography**.



Introduction

Cryptography is a field that seems to stand just beyond the reach of our observable world yet it's there all around us, quietly playing an immensely important role in our everyday lives. Our phones, our laptops, our entire digital presence is made possible by the magic of cryptography.

And yet cryptography is no recent endeavour either. It has been there with us as far back as the advent of writing itself. While we all benefit from it, only a small number of us know its importance and even fewer feel the curiosity to delve any further. The world of cryptographers is worryingly small. You, however, by picking up this book, are one of those select few. And I hope to reward your curiosity by taking you on a journey as we slowly uncover the magic that lies at the frontier of cryptography.

This book is divided into two parts, loosely following what I believe are the two big eras of cryptography in recent years: the era of ***data*** and the era of ***compute***. This all kicks off in the 1970s where the rise of computers thrusts cryptography to the fore. It is during this time that DARPA begins connecting computers into what will eventually become the World Wide Web yet also the time where we experience the first computer viruses and hacks. Information is gushing around at an unprecedented velocity. Uncontrollable, it's both terrific and terrifying.

Warning: Here Be Dragons

You may already hold some prior notion of cryptography as something frighteningly complex and esoteric. I would, however, like to show you that this is not actually the case; that cryptography is both more accessible than you may have thought and plays an even more significant role than you may have conceived. This book attempts to make very few assumptions of what you currently know, starting at the very beginning and gradually ramping up to the interesting and exciting concepts at the edge of our collective knowledge. To get you there, I will utilise diagrams, figures, analogies and metaphors. I've also turned to math. Many of you might wince at the word and flash back to your dreaded high school math classes. But, math is the most powerful tool we have at explaining logic.

It is its own language used to succinctly explain complex ideas, and, once you're able to sit there and face those foreign squiggles undeterred, you may see how beautiful it really is. Mathematics is the backbone of cryptography, and while you should be able to get by without comprehending the equations, to not include them at all would be like watching a film without sound.

Why Do We Need Cryptography?

Cryptography, at its core, arises from our desire to control the way information is communicated. The explanation for this desire may be based on a very important event in history: the advent of writing. Prior to this, all information was communicated only through spoken words. In the spoken world, all communication is ephemeral — ending the moment the sound waves dissipate — and local, travelling only as far as your voice carries. This is not without its benefits. For one, you almost always know the identity of the person that shared the information. Was it an order from the chief or did it come from a fellow forager? We will refer to this as **authentication**[1]: knowing who said what and **integrity**: knowing that what was said wasn't tampered with. Secondly, you can often tell who was within earshot. If **privacy** was required, you could make sure that it was just you and that other person that could hear what you're saying. Of course, you couldn't stop that person from spreading the secret further but that's something that's out of cryptography's control, even today.

This is all to say that the need for cryptography wasn't in high demand back then.

When written language came along, we were able to spread ideas far quicker than before and this allowed us to expand beyond the small tribes we once were. But with writing, authentication, integrity, and privacy became far more difficult. You could no longer verify the identity behind that information nor could you be sure who else might read it. You had to trust and that trust caused the abrupt end of many kings and queens[2].

Since then, the art of cryptography has been around us, chiefly to serve those purposes: authentication, integrity and privacy. Whether spies, lovers or prisoners, so began the race of continually improving the way we hide information and the techniques we have to uncover it. Fast forward to modern times, cryptography has become ubiquitous in the digital age.

> **Every time you open a web page, check your emails, send a meme in a group chat or book flights, there are a series of cryptographic protocols working beneath the surface to ensure that no one can imitate you or imitate the people or services you interact with.**

Making the digital world a safe sphere to operate in is a thankless but necessary task. The challenge of preventing malicious actors into this safe sphere gets harder as we make progress in other fields such as artificial intelligence and quantum computing. Take a second to imagine a world where all those daily acts I listed above could not be trusted; where the only way was to revert to interacting with everyone in the physical realm. Cryptography ensures that we don't lose the digital realm that has been quintessential to the development of modern society.

Have You Got Something To Hide?

While authentication and integrity are quite clearly positive things to build in our world, many of us sit on the fence as to privacy. It's a rather nuanced topic and something that I thought ought to be tackled early on in a book dedicated to cryptography. "I've got nothing to hide" is a stance I've heard when someone wants to question why have privacy at all. This is, however, a bit like saying "I trust whoever is watching". It's not just about your goodness, it assumes the observer also has your interests at heart. Our democracies benefit from secret ballots not because voters are guilty, but because they are free. Our economies benefit from startups who can protect an informational edge over incumbents with far more power. Our societies are fairer when those in power can't abuse information asymmetries. Privacy is definitely needed, and thus cryptography, but it's no doubt a double-edged sword. Even our language is shaped by the morality behind privacy. We use words like confidential, transparent and accountable when it benefits us and conceal, expose and surveil when it doesn't.

After the mass shooting in San Bernardino in 2015, the FBI came to Apple asking for custom iOS software to help them break into the phone of one of the shooters. Apple claimed that if they were to build a tool to weaken the device, it could be used again and again and were thus dubious that it would stay "just for the good guys." Apple then went on to become the subject of their own criticism when they proposed adding child abuse detection software for all iCloud photos. Fighting terrorism and child abuse are causes most of us would agree with, however the overarching concern was that once Pandora's box was opened it couldn't be closed and we'd be none the wiser if it continued to be used for good or not. Cryptography exists in this context to improve on the tools society needs when it wants to decide what information should be visible or not.

Introducing the Characters in Our Journey

The way I will go about explaining the concepts in cryptography will follow a predictable pattern so it's helpful to make that pattern clear to you from the start. Cryptography consists of primitives and protocols. **Primitives** are the fundamental building blocks. They are the tools like blenders, whisks, pots, and ovens, with specific purposes, that cryptographers use to build

protocols. The **protocols** here are recipes. They tell you how to take some ingredients (some input information), and using these tools at your disposal, bake a cake. However, rather than a cake, a cryptographic protocol may take information you wanted to send to a friend and allow it to reach the friend in an authenticated and private way. Often cryptographers are thinking up ways to improve an existing primitive by coming up with a better algorithm — a version of that primitive that is perhaps faster or cheaper than its predecessor just like induction stoves improved on the electric stoves that were commonplace prior. While improvements are an important part of the frontier, I won't tend to cover them in as much detail as the entirely novel primitives.

Cryptography inherently involves communication between people. There will always be at least two parties that want to use cryptography to reach some shared goal. Thus to explain how cryptography works, I will constantly come back to a cast of characters that have been invented by cryptographers over the years to the point that this has become a quirky convention embedded in the very fabric and would be remiss of me to not follow[3]. At the centre of it all we have the two protagonists: **Alice** and **Bob** (A & B). The story also needs an antagonist, someone who will do anything to prevent their goal. It's important to consider the antagonist to analyse the protocol. For example, how secure is it? This malicious agent is referred to as **Mallory**. The last character is trustworthy **Trent**. Trent has the fortunate or unfortunate condition of being infallible and is often brought in to show either a) what the protocol is trying to achieve or b) what trust assumptions the protocol might have.

Lastly, I'd like to remind you that although frontiers are ever expanding, this book is unfortunately not. You should think of this book as more a journey out to cryptography's frontier rather than cruising around its edges. Much of the book focuses on providing the background and context that will allow you to understand the latest research rather than delving into specific papers themselves.

Our first few chapters begin with the most fundamental primitives of cryptography: symmetric and asymmetric cryptography.