When is a Tree Really a Truck? Exploring Mental Models of Encryption
Justin Wu and Daniel Zappala, Brigham Young University

This paper is included in the Proceedings of the Fourteenth Symposium on Usable Privacy and Security.
August 12–14, 2018 • Baltimore, MD, USA
ISBN 978-1-939133-10-6

Open access to the Proceedings of the Fourteenth Symposium on Usable Privacy and Security is sponsored by USENIX.
When is a Tree Really a Truck?
Exploring Mental Models of Encryption

Justin Wu
Brigham Young University
justinwu@byu.edu

Daniel Zappala
Brigham Young University
zappala@cs.byu.edu

ABSTRACT
Mental models are a driving force in the way users interact with systems, and thus have important implications for design. This is especially true for encryption because the cost of mistakes can be disastrous. Nevertheless, until now, mental models of encryption have only been tangentially explored as part of more broadly focused studies. In this work, we present the first directed effort at exploring user perceptions of encryption: both mental models of what encryption is and how it works as well as views on its role in everyday life. We performed 19 semi-structured phone interviews with participants across the United States, using both standard interview techniques and a diagramming exercise where participants visually demonstrated their perception of the encryption process. We identified four mental models of encryption which, though varying in detail and complexity, ultimately reduce to a functional abstraction of restrictive access control and naturally coincide with a model of symmetric encryption. Additionally, we find the impersonal use of encryption to be an important part of participants’ models of security, with a widespread belief that encryption is frequently employed by service providers to encrypt data at rest. In contrast, the personal use of encryption is viewed as reserved for illicit or immoral activity, or for the paranoid.

1. INTRODUCTION
Many security and privacy experts advocate for the widespread adoption of encryption, both as a security measure for protecting against third-party attackers and as a privacy preserving tool. Indeed, recent years have seen encryption incorporated by default into popular software, such as instant messaging apps like WhatsApp and in mobile devices operating systems like Google’s Android and Apple’s iOS. However, previous studies have shown that when users are actively involved in the process of encryption, they can struggle to accomplish this task [5, 10, 11, 15, 17, 23]. This is important because the misuse or misapplication of encryption technologies can be devastating. Those who incorrectly use encryption tools may falsely believe themselves protected by technology whose guarantees no longer hold due to their mistakes. Perhaps more dangerous still, users who do not understand the risks of the technology could well find themselves in a situation of self-imposed denial of service, permanently locked out of accounts and data which they have lost the keys for, and—unlike with passwords—no one who can help them recover them.

In the context of encryption, where the cost of users’ mistakes can be grievous, circumventing the possibility of user error by transparently incorporating encryption into software, thus bypassing the user entirely, is a desirable and effective option. Indeed, in scenarios where encryption has already achieved widespread deployment—smartphone encryption, TLS / HTTPS, and secure messaging apps—it has succeeded by doing precisely this. Unfortunately, while this approach is indeed effective, its applicability is not without limits [6, 12]. Automation is not always a perfect solution; even the best software at times encounters errors that require user interaction to proceed [22]. With high levels of automation, users likely lack the context necessary to make the correct response. In two cases where encryption has been transparently applied, for example, studies of the efficacy of TLS browser warnings [2] and of the authentication ceremony in secure

Figure 1: One participant’s diagram. The top half reveals how they visualize the encryption of textual data to occur, while the bottom half shows their impression of how pictures are encrypted.
The functional nature of mental models has serious implications for design: accurate or inaccurate, someone’s mental model is what they rely on when they interact with and troubleshoot systems [19]. Subsequently, a proper understanding of mental models can be beneficial in user-centered design, affecting both the intuitiveness of tools as well as the efficacy of our communication with users [21]. Extending beyond use, mental models also have implications for adoption, as users’ perceptions of the utility of a security or privacy tool is a critical element in their decision of whether or not to adopt.

There is some evidence from previous research that suggests that users’ mental models of encryption are flawed or incomplete [1], although there has heretofore never been a systematic effort to profile and understand what these mental models may be. To help us better understand how users perceive encryption, we have executed a qualitative study consisting of 19 semi-structured interviews focused on profiling users’ models of encryption. We thus present the first directed effort to explore users’ mental models of encryption.

We explored three facets of participants’ perceptions of encryption: what it is, how it works, and its role in their lives. Interviews with participants were divided into two halves. The first half of the interview was designed to elicit their mental models of encryption and pertaining to the mechanics of encryption. In addition to questions probing these concepts, participants were tasked with “encrypting” both text and non-textual data (a picture) in a brief, but illustrative diagramming exercise, an example of which can be seen in Figure 1. The second half of the interview focused on how encryption might be used, and presented participants with three distinct encryption use cases for discussion.

By analyzing the results from our interviews, we have categorized participant responses into a set of four mental models. These models vary in complexity and detail, but ultimately reduce to a functional abstraction of access control. Based on our observations about these models and other remarks made by our participants, we outline a number of important implications regarding the future of encryption software design and risk communication.

The contributions made by this work are as follows:

1. **Presents first directed effort at exploring mental models of encryption.** Previous research that has investigated perceptions of encryption have only done so as parts of larger efforts, such as to understand secure communication or general security behaviors. This work is the first to focus exclusively on this issue.

2. **Identifies four mental models of encryption.** Based on interviews consisting of both verbal questioning and a diagramming exercise, we identify four properties—one functional, one structural—that comprise a mental model of encryption. By correlating individual participant responses with these properties in a data matrix, we compiled a set of four mental models of encryption that highlight the differences in the way people perceive the structure and function of encryption.

3. **Outlines implications for design and risk communication that arise from participants’ perceptions of encryption:**

   - **Encryption is restrictive access control.** Despite the varying levels of detail and complexity in participants’ mental models of encryption, they nevertheless produce the same functional abstraction: restrictive access control. Designers should contemplate whether encryption contexts align with this model and, if not, consider presenting users with a functional model for interaction that more closely aligns with that of access control.

   - **Models of encryption are of symmetric encryption.** Participants’ functional models for the role of keys and sharing keys coincide closely with symmetric encryption. Their structural view of what keys are, furthermore, does not align well with asymmetric encryption, and could be a major usability obstacle in the use of software employing public key cryptography unless an alternative model is presented to users.

   - **Confusion about encryption strength.** Even participants with similar mental models described a wide array of timescales in which they believed encryption could be broken. A number of factors appear to play a role in this discrepancy, such as varying perceptions about the capabilities of attackers.

   - **Grassroots adoption is also a public relations battle.** Participants largely viewed encryption as already being deployed by the service providers they deal with regularly, such as banks and online merchants. However, when it turned to personal use of encryption, they felt strongly that the use of encryption was the domain of those engaging in illegal or immoral activity, or the paranoid.

2. **METHODOLOGY**

The data presented in this work is sourced from 19 semi-structured interviews conducted with participants from the United States. Each interview lasted between 30–60 minutes, and participants were each compensated the equivalent of $15 USD for their time. Our study was approved by our institutional review board.

2.1 **Recruitment**

Participants were recruited using the Prolific research platform, and interviews were conducted until data saturation was reached. Prolific allows for prescreening of potential participants by filtering for a number of demographic variables. To maximize ease of communication, we limited the pool of potential candidates to only those Prolific participants who both reside in the United States and speak English as a first language.

Our study was listed as a task on Prolific, advertised as “phone interview on an Internet-related topic.” Interested participants self-selected into the study and registered via an online scheduling form that was linked in the Prolific task. In accordance with Prolific’s requirements, we did not collect
any personal information beyond first name and Prolific email address (Prolific provides an associated email to each account for communication purposes). Participants who scheduled were contacted via their Prolific email, and three things were communicated: (1) the study coordinator’s phone number, (2) an instruction to have pen and paper ready during the scheduled time in preparation for the diagramming exercise, and (3) a request for consent to transcribe and share study data after anonymization.

2.2 Demographics
19 participants in total participated in our study. Our sample skewed heavily male (n=13, 68.4%). Participant age ranges were fairly diverse: 7 between 20-29, 5 between 30-39, 5 between 40-49, 1 between 50-59, and 1 between 60-69. We had some students (n=6, 31.6%), but most of our participants were not in school. While we did not seek explicit socioeconomic demographics, we know that 7 of our participants had full-time employment (36.8%), while the remainder worked either part-time or not at all.

2.3 Study design
Interviews were conducted remotely, by phone. They were semi-structured, with a set of questions that were asked of each participant, and others that were asked only of specific individuals as their responses warranted. The interview guide can be found in the Appendix, and interview transcripts have been made available for download at https://mentalmodels.internet.byu.edu.

2.3.1 Introductory information
As each interview began, the coordinator informed the participant that the topic for discussion would be technical in nature, and that it was expected that there would be questions for which they had no answer; in such an event, they were to instead offer their best guess. While such answers might be speculative in nature, and thus seem undesirable, our goal was to understand how participants would perceive software if all they knew was that it used encryption in general, which mirrors this situation.

They were then reminded of the need for pen and paper for the drawing exercise, and asked to prepare them if they had not already done so (no participants actually needed the reminder). Finally, participants were asked to give a brief description of their line of employment and/or area of study, to get a sense for technical background. They were also asked to describe what types of devices they own and use, and what types of tasks they perform on them.

2.3.2 Encryption mechanics
At this point, the main portion of the interview began. Participants were first asked to describe what came to mind when they hear the word “encryption.” Follow-up questions were asked as necessary to have participants clarify their responses. They were typically asked to explain where they might have seen or heard the term used, to seek insight into the contexts in which they believe encryption appears. They were then asked to describe what types of imagery they associate with the term, with the goal being to help us understand what types of visual metaphors might work well when communicating about encryption. As discussion on these questions drew to a close, the coordinator initiated the diagramming exercise.

2.3.3 Diagramming exercise
The diagramming exercise consisted of two tasks where we asked participants to illustrate the encryption of textual and non-textual data respectively. The latter was particularly important because we supposed that imagery of textual encryption would be prevalent in popular media, and were curious how participants might react to the idea of encrypting something else.

When this segment of the interview began, participants were first informed that the point of the exercise was to help the coordinator visualize what the participant had in mind, and not a test of artistic ability. They were asked to write down the following sentence on their paper, “This is a message to be encrypted.” It was then explained that they were to imagine encrypting this message: their task would be to draw what they imagined would happen. No explicit instructions were given as to form to avoid influencing participants, which unfortunately led a couple participants to generate diagrams that were too lacking in detail to have interpretative value. Participants were given as much time as needed to finish the task, being told to alert the coordinator when they were done. Once they had finished this first task, they were then told to draw “a simple picture, such as a tree, cloud, or stick figure,” and repeat the same task, diagramming what they imagined would happen if this picture were to be encrypted. Upon completion of this second task, they were asked to text or email a picture of their work to the coordinator.

After the picture of their drawing was received by the coordinator, discussion about its contents began. Participants were asked to walk the coordinator through their drawings and explain the various elements of their illustration, with the coordinator prompting for clarification as needed. Participants were also asked to explain how they imagined the process of decryption would work: the coordinator described a scenario in which an encrypted message was sent to a friend or family member, and asked what the receiving party would need to do to read the original message. Finally, participants were asked to characterize how difficult they expected it would be for two groups—hackers (representing individual attackers) and the NSA (representing institutional resources)—to break encryption.

2.3.4 The role of encryption in life
After the diagramming phase, participants were informed that the discussion was about to transition away from what encryption is and how it works to how it might be used. They were then asked if they thought encryption played any role in their life. If participants’ responses were restricted to institutional use—such as by banks, the government, online vendors—we also asked them if they thought there might be individuals who used encryption for personal reasons.

Finally, the last segment of the interview involved introducing each participant to three encryption use cases that are available to normal users. These are mobile device encryption, HTTPS, and secure messengers. Some participants had already mentioned one or more of these prior to this part of the interview; if they did so, the topic was discussed at that earlier point. Otherwise, the three use cases were presented and discussed in this order.

With the partial exception of HTTPS, our aim with this part of the interview was not to assess participants’ famil-
We explained to our participants that both Android and Android devices that are encrypted is much lower, although Apple to enable encryption by default on devices running iOS would protect them from. We then asked them to describe what information they serve as a useful first look at the perceived utility of encryption in daily life.

Mobile device encryption
Nearly all iOS devices are encrypted, due to a decision by Apple to enable encryption by default on devices running iOS 8 or higher. As a result of fragmentation issues, the number of Android devices that are encrypted is much lower, although it is expected to improve with time as new Android devices now also ship with encryption enabled by default. Because of the relative ubiquity of smart devices, their importance in daily life, and the likelihood of their being encrypted, they serve as a useful first look at the perceived utility of encryption in daily life.

We explained to our participants that both Android and iOS devices had functionality that allowed for encryption. Each of our participants had, and regularly used, at least one mobile device, and thus had the necessary context needed to share their impressions. We asked what they thought it meant to encrypt their smartphone or tablet, drawing a juxtaposition to the encryption of data as had been discussed previously. Participants were then asked why they imagined someone might want to encrypt their device, that is, what would be protected by doing so? Finally, we asked them to explain who they considered enabling device encryption would protect them from.

HTTPS
User interactions with HTTPS are well-studied, and the technology is extremely widely deployed, with efforts in play to make it ubiquitous; it thus provides another useful example for examination. With this use case only, we began by asking participants if they had ever noticed an “HTTPS” or lock icon in their browser, located near the address bar. Since all had, we then asked them to describe what they believed these indicators to mean. After they had responded, we informed them that it represented an encrypted connection between their browser and the web server of the site they were visiting. We then asked them to describe what information they believed it was meant to protect and whom it would protect them from.

Secure messaging apps
Our final examined use case, secure messaging apps, are a class of instant messaging apps that use end-to-end encryption. A handful have seen fast-growing adoption, albeit not for their security properties [1], and are a growing area of interest for security research. We began by asking participants if they used any popular instant messaging apps, such as WhatsApp or Facebook Messenger, to establish a frame of reference. We then explained that secure messaging apps are a subset of these types of apps, the difference being that they encrypt all communication made via the app. Participants were asked why they imagined someone might wish to encrypt daily communications, and not just what is more commonly considered sensitive data, such as financial information. They were also asked who they thought encryption was meant to protect their communications from.

2.4 Data analysis
The audio of each interview was recorded and transcribed. These transcriptions were then jointly coded by the study researchers via open collaborative coding per the conventional content analysis approach. Coding was only performed in meetings where both authors were physically present and jointly reviewing the transcripts. Any disagreement was resolved via on-the-spot discussion, and thus we did not calculate inter-rater agreement.

We separated participant responses into two types: those to be explored as individual themes, and those that we identified as serving functional or structural roles in users’ mental models. From our codes, we chose four structural and functional properties that comprise the mental model of encryption.

We then went through each participants’ transcripts anew, and filled in a matrix, matching each participant’s responses to the corresponding mental model components. Finally, we grouped these individual models into sets based on what we identified as critical dividing boundaries derived from fundamental structural or functional differences. Each of these sets became one of our final mental models, and represents a unique abstraction of encryption.

3. RESULTS
In executing this study, our goal has been to explore the space of user perceptions of encryption and not to quantify the extent to which users possess certain views. Accordingly, we do not provide quantitative measures of the frequency with which various opinions were expressed, and instead have attempted to characterize a representative set of the issues our participants described.

3.1 Impressions about encryption
At the start of each interview, we began by asking each participant to describe what came to mind when hearing the word “encryption.” This served to give us some sense of the context in which they imagine encryption exists—the environments in which it is used and the purposes it serves. Responses broadly fell into three categories: characterizations of encryption itself and then contexts and current events that they associate with encryption.

A number of participants described encryption itself, including terms such as “algorithm,” “encode,” or “secret code.” Participants also described imagery that they associated with encryption, such as Lloyd1, who related encryption with “that scene in the Matrix, where the letters are falling out of the sky and it’s like the code of the Matrix.” This imagery of long, indecipherable strings of symbols was commonly shared by our participants, and particularly evident during the diagramming phase of the interviews.

Encryption was also clearly associated with security and privacy in our participants’ minds. They mentioned both broad properties such as “security,” “safety,” “protect,” and “privacy” in addition to specific contexts where they imagined encryption was used such as “access control,” “email,” and “passwords.”

1 All names used are pseudonyms.
Current events involving encryption also stood out to participants when they became notable enough to be covered by mainstream news media, as with Edward, who explained that he noticed such events “when they’re big enough to show up in the normal news. I’m not putting much effort into looking for this.”

3.2 Mental models of encryption

Mental models have been described as having alternatively structural and functional properties. Structural properties describe how participants perceive the internals of how encryption works, while functional properties characterize how participants interact with encryption. Because, as we expected, our participants largely did not have any experience with encryption tools, our focus is primarily on the structural properties, although we did evaluate some functional aspects via presented scenarios. Based on our coding of participant responses, we compiled a set of four properties that comprise a mental model of encryption:

1. **Inputs to encryption/decryption**: This property is taken from the follow-up questioning segment of the diagramming exercise, and describes what inputs, if any, participants believe are necessary for the encryption process (aside from the object to be encrypted).

2. **Encryption output format**: This property is taken from each participant’s diagram, and refers to how they depicted the output of encrypting the text/picture.

3. **Encryption process**: This property is taken from each participant’s diagram and follow-up questioning, and characterizes what they imagine the process of encryption itself entails.

4. **Decryption process**: This property is taken from follow-up questioning about each participant’s diagram, and characterizes how they imagine the process of decryption occurs.

Before continuing further, there is something we wish to impress upon the reader: the “obvious” solution to the issues we explore—i.e., improving the accuracy of users’ mental models—may not be as simple as it seems. If we leave tool design static, attempting instead to correct inaccurate mental models, we run into the issue of the difficulty of effective communication regarding encryption, both in terms of message (what to convey) and medium (how to convey it). Moreover, this approach places the responsibility for change upon users.

Alternatively, we can alter software design to more closely align with users’ mental models. This places the onus for change upon developers, who we feel have both stronger incentives and the knowhow to do so. This is the approach we espouse in this work. We do note, however, that if the community as a whole can make headway on communication efforts, the most productive approach will be to tackle this problem from both ends.

The following mental models are listed in general order of complexity/detail, proceeding from the simplest to the most detailed, although some models may be “equally” complex, and differ instead on certain critical details. A diagram of these models and their relationship can be found in Figure 2.

3.2.1 Model #1: Access control

The first and most basic model of encryption provides only the most minimal abstraction of access control. Unlike the remainder of our participants who recognized that encryption transformed the source data somehow, the two participants who possessed this model instead viewed encryption as an extension of credential-based access. As can be seen in Figure 2, this model has multiple “N/A” entries, to signify that their model did not even allow for the existence of these properties.

When first presented with the diagramming task, Edward immediately felt at a loss to characterize what encryption might look like. He asked, “Does it actually have a look? Is it just something that ‘what comes in your mind’ or does it actually have a certain look? It’s all just... online. It’s all zeroes and ones.” When later discussing his illustration (Figure 3) with the coordinator, he added, “I didn’t really think of a physical change, really, aside from something coming up on a barrier,” which indicates that he had likely never previously considered that encryption might actually transform data somehow, instead associating encryption solely with a notion of access control.
Selena employed a similar metaphor, analogizing encryption to a “wall”: “I mean, I’ve like heard of protection but I don’t know exactly what it means. And I’ll be honest, I’m really a person who’s been—I don’t want to say sheltered, but— But I’m thinking a wall.”

3.2.2 Model #2: Black box

The next model advances the previous model slightly. It is functionally similar to the first model in that participants with this model similarly viewed it as an extension of existing credential-based access. However, participants who had this model did understand that encryption would transform the source data—that is, they understood that encryption was an active process, though they did not have a strong sense of how this process functions. As Diana explained, “You don’t really know what it means, but you know that it means something; you just don’t know what. I feel like that kind of works with encryption, because when they’re like, ‘oh, it’s encrypted, your stuff is protected,’ I kind of know what that means, but I don’t really know what they’re doing to make that happen.”

Wally explained how encryption is something that “sort of run[s] in the background.” The software would transparently handle both encryption and decryption as it “gets the information and gobbles it all up and translates it into something else and as it comes out the other side it’s sort of put back together.” This black box perception of encryption is well-captured in his diagram, shown in Figure 4.

In another example, Figure 5 depicts Eva’s diagram for encrypting the cloud that she had drawn. She, as with many of our participants, did not have a concept for the digital representation of image data, and so did not first transform her illustration into a digital representation before transforming it. Instead, she drew the “only thing [she] could think of”—a watermark—because she knew that “they put watermarks to keep people from stealing,” and she associated encryption with protection against theft.

This model is more functional than structural, with some conception of what encryption will do for you, but not how it works. Subsequently, participants had to analogize from other security mechanisms that were more familiar to them, such as a “watermark” in Eva’s case or “password dots” in Diana’s. Because this model correctly perceives encryption as a process, these participants did have some notion of necessary inputs, even if, due to a loose conception of how encryption worked, that input might simply be the encryption algorithm itself.

When asked how decryption might occur, Diana shared that a “key” would be needed—“I think they’d have to send a key with it, or else I wouldn’t know what to do with it.” What, then, was this key? Her response was one echoed by many of our participants: a key is a reversed list of the operations executed during the transformation (encryption) process. “Well, if the letters were sort of mixed-up randomized, then I think, from that, they could make a key based on how it’s been randomized, where the letters went or where they originally were, and they could hand me that, and from there, I could...”
unrandomize the letters.” (A handful of others possessed a similar, if slightly different view: a key was a like translator that guided the reversal.)

3.2.3 Model #3: Cipher
The cipher model differs from the black box model in that participants with this model had a clear sense of how the “transformation” process of encryption works: constituent portions of the source are deterministically substituted into another form, i.e., a cipher. As can be seen in Figure 6, this substitution cipher behavior extended even to the encryption of image data: Allen defined deterministic transformations of the various curves in his cloud to be enacted by the encryption process.

For example, Fred described “a simple algorithm for it,” where each letter would be replaced by the letter a specified distance from it alphabetically. “If the original letter is ‘T,’—that’s the first variable—it’ll add four letters, so it’ll go ‘U,’ ‘V,’ ‘W,’ and end on ‘X.’ And then every letter after that, continue to add 4 to each. The cipher is ‘+4′ basically.”

3.2.4 Model #4: Iterative encryption
Participants with this model were the most descriptive and detailed. When it comes to the properties we have discussed in other models, they share only some superficial similarities. They all believed that encryption would transform the source data. Their notion of what type of operations are performed by the encryption process varied. Their impressions of the difficulty of breaking encryption similarly varied, although they generally imagined it would be a non-trivial task. We chose to unify these participants under a single model, however, because their models jointly exhibit a shared property not found elsewhere: they explicitly described the encryption process as an iterative one involving multiple passes over the source data in order to produce the encrypted output.

For example, Figure 7 shows Franklin’s depiction of how textual encryption would work:

“Interviewer (I): Okay, great. Let’s start with the part at the top where you’re encrypting the message. Can you explain what that second line is to me? You have something on the left and an equals sign and then something on the right and it says one trillion or some very big number. Can you explain that to me?

Participant (P): Yeah, it’s converted to those various symbols to the power I’ve put it in.

I: And when you say ‘to the power,’ what do you mean, what are you describing?

P: The conversions are that many times or roughly that many times.”

Their model for what types of operations were to be performed at each iteration varied from person to person. Lloyd, for example, described a model where “scrambling” happens “a bunch of times.” Franklin believed encryption to be a mathematical process at heart, explaining that if math were responsible, then encryption would “be uniform, it would follow certain specific laws, it would be rational.” Nicole described a complex process where encryption “would be either swapping or rearranging and [...] adding an infinite amount of extra garbage to it or just infinitely changing all the different parts of it to be different things.”

3.2.5 Shared secrets
One vital aspect of interaction with encryption software is an understanding of the requirements for decryption. To help us understand how participants envisioned this process, we asked them to imagine a scenario where they had encrypted a message for a friend or family member, just as in the diagramming exercise. We then asked them to describe what they felt the receiving party would need in order to read the original message. As mentioned earlier, participants described needing something to reverse the operations that encryption had performed, which they frequently called a key.

When asked how their friend or family member would acquire access to such a key, most participants did not have an idea or answered that they would make arrangements in-person. Some thought about sending the key over another medium, but at least one participant, Lloyd, recognized the circular nature of this problem: if the goal was to establish a secure channel, then wouldn’t you need an existing secure channel to convey the key? “I have no idea. Arcane computer wizardry?”
'cuz you think you'd have to encrypt the key and encrypt the encryption on the key." Brent, on the other hand, imagined that perhaps keys might be tied to login credentials, such that "maybe you just receive them when you log on or view something that’s encrypted."

### 3.2.6 Encryption strength
We asked participants to contextualize their responses as timescales in which two parties would attempt to break an encrypted message: hackers and the NSA. Conceptions of what it would take to break encryption were all over the board, ranging from minutes to years to practically impossible. A deeper discussion of these responses is included in Section 4.4.

### 3.3 The role of encryption
Perceptions of encryption extend beyond what it is and how it works to more functional views, such as the role it plays in life. As part of our effort to better understand how people view encryption, we asked participants to describe the perceived role of encryption in daily life in general and also in three use cases that we presented for discussion.

#### 3.3.1 Encryption in daily life
When we first planned to include a question about the role of encryption in daily life, we were concerned that participants would not think that encryption was at all present in their lives, and that we would subsequently be unable to glean anything from their responses. To our pleasant surprise, however, all of our participants responded immediately with examples to this question. Indeed, their answers throughout our interviews make it apparent that encryption plays an important role in our participants’ models of computer security as a whole.

Nearly all participants felt confident that any service providers they engage with that deal in sensitive information proactively encrypt their data, with banks and major online vendors first coming to mind. Most participants seemed to associate encryption with online activity, although a couple participants did mention credit/debit cards, a likely reference to EMV chip technology. Despite this online-oriented view of the entities responsible for encrypting their data, however, it was clear that—excepting those few participants who were explicitly aware of TLS and its purpose—participants simply did not have a model allowing for encryption of data in transit, only at rest. For example, Diana informed us that "I think once you send the data or whatever, that it’s not really yours anymore because now they have it, so maybe once they get it, they can do whatever they want with it, so they can encrypt it that way. Once you send the data and they get it, they can fuzz it or jumble it or do whatever they do when they encrypt it, and then you’re good to go."

Because our participants unilaterally brought up institutional use of encryption in response to this question, we also asked whether they imagined there were individuals who used encryption in personal contexts as well. Participants all believed that there were, although their responses centered on sensitive contexts, whether that be business interests such as investment information or intellectual property or for more nefarious uses, such as illicit or immoral activity.

For example, when we asked Diana about the individual use of encryption, the following dialogue played out:

"I: What about individuals as opposed to institutions? So not talking about a company or the government, do you think there are people that use encryption on a regular basis?
P: Maybe if they’re doing something illegal?
I: And why do you think they would be using encryption in that case?
P: So they don’t get caught?
I: So you mean to hide what they’re doing from other people?
P: Yeah.
I: Any other examples that you might be able to think of?
P: Maybe if they’re an entrepreneur and they’re making something that they don’t want to be stolen, they’d use encryption.
I: So again, basically any time what you’re doing is sensitive?
P: Yeah."

Participants also recognized that there might be some who employed encryption out of generic privacy concerns, but typically classified such concerns as “paranoid.” Nicole, who sometimes needed to use encryption tools at the request of clients, characterized the situation in this manner: “For some people, I think it’s a level of paranoia, almost. To have everything need to be encrypted. But for some people, particularly that are in the tech industry, it’s almost like a biblical need. So when I’m dealing with someone who’s really into encryption, I have to think of it from their standpoint of a desire for privacy and security– Of course, the paranoia that someone’s gonna care.”

In general, the personal (non-business) use of encryption seemed to be viewed quite negatively: either you use encryption because you have something bad to hide or because you’re paranoid.

#### 3.3.2 Use case #1: Smartphone encryption
The first use case we presented for discussion was that of smartphone encryption. All of our participants used mobile devices—many had both smartphones and tablets—and thus all had the context necessary to understand this use case. When we asked participants to explain what they believed smartphone encryption meant, responses primarily viewed it as a form of access control, tied to the passcode lock they already had on their devices. In one example, Abe explains that, “I imagine that it means to take the data on it and do the same thing: put it in a code that’s only able to be broken by you, by something like your passcode or thumbprint.”

Some participants recognized that encryption would protect their storage medium itself, such that “if someone stole my phone and they didn’t have my passcode, they wouldn’t be able to access my phone’s hard drive or storage and read all my data” (Allen). Some, however, just saw it as an additional protection over the passcode lock of unknown nature, such as Brent: “It might just add another extra layer of it, ‘cuz I thought the password lock was up there in terms of protection because it’s a thing only you would know unless someone used social engineering to figure it out. I feel like it would just add another layer.”

Participants viewed their phones as important stores of personal data, with encryption potentially protecting items such...
as login info (via apps), photos, contacts, and texts. When describing who encryption was meant to protect their phones against, the ever-present catchall of “hacker” was present, but participants also described the need to defend against physical threats (when devices are either misplaced or stolen) and law enforcement. For example, Mary first described smartphone encryption as protecting things one “wouldn’t want other people to see.” When asked to clarify who she meant by “people,” she explained, “I was just gonna say somebody who just steals your phone, but yeah. Probably hackers too because there was the huge photo dump with the iCloud stuff.”

3.3.3 Use case #2: HTTPS
As mentioned earlier, with our second use case—HTTPS—we began by asking if participants were familiar with seeing either “https” in the address bar or the lock icon nearby. All participants were, and so we asked them to explain what they believed these indicators represent. While a small number were fully aware of TLS and its purposes, by and large, participants responded that they were indicators of site security. Edward, for example, believed that it meant sites had been reviewed by a third party and received a seal of approval: “maybe it’s just another entity, like a government entity, that would review certain sites and give a seal of approval. But other sites, that are newer or not as established, that don’t have that because they’re not under review.”

Interestingly, a couple had previously clicked on these indicators and read a little about them, and knew that HTTPS involved certificates, although they nevertheless still conflated these with site security. Brent explained, “it informs me of who it belongs to, like what company stands behind it and basically it’s like a certificate of who we are, we are authorized, and we are secure.”

Participants’ model for what types of information were being protected involved the sensitive data they conveyed when online, such as credit card information when shopping at online merchant sites. Interestingly, while there was some variance in their model of technique and/or target, i.e., the site or you directly, the attacker model was consistently that of hackers.

3.3.4 Use case #3: Secure messaging apps
Our final use case was that of secure messaging apps. While not all of our participants had previously used instant messengers, and thus lacked the direct comparison, all regularly texted and had at least this level of context. We explained to them that secure messaging apps were a class of instant messengers that encrypted communications via the app. We drew an explicit contrast to “sensitive information,” such as financial information, and participants were asked to describe why they thought someone might want to encrypt daily communications by comparison.

While many participants did first think of sensitive, potentially damaging conversations such as those pertaining to cheating on a partner, there were a number of responses that saw potential use for privacy in more mundane settings, though they didn’t personally envision such a use for themselves. This dialogue with Carol is an illustrative example of this sentiment:

“I: What I want to ask is: why do you think we might want to encrypt daily communication? For example, it’s easy to see why you might want to encrypt financial or medical information, but why do you think someone might want to encrypt their daily communication?

P: Probably for illegal reasons.

I: Can you explain a little?

P: Well, if you’re doing things that aren’t necessarily legal, you don’t want people knowing about it that shouldn’t know about it or the government looking into your things.

I: Are there other use cases that you might imagine?

P: Why a normal person wouldn’t want people looking into their stuff, basically? Because it’s none of their business, for one thing “laughs” You might have personal things going on too, like an affair or something like that, that you wouldn’t want other people knowing. But normal people can’t look into that, so it would be more like government or police.

I: Is this something that you would ever do personally? Use something that encrypts your daily communication?

P: Personally? I doubt it.

I: Can you explain why you might not?

P: I don’t have anything to hide or worry about.”

4. DISCUSSION
The models we observed, and other remarks our participants made, have implications for the way encryption is presented to users, both in design and communication. We now discuss the issues we observed and include our suggestions for a way forward.

4.1 Encryption is access control with a symmetric model
From the simplest mental model we observed to the most detailed and complex, they all reduced to the same functional abstraction: restrictive access control. Structurally, participants varied in how they imagined the encryption process acted on the data it was meant to protect, but all of our participants believed that encryption served one purpose: preventing undesired access.

Simultaneously, participants’ mental models of encryption coincide very nicely with symmetric encryption. They understood that a shared secret would be needed, and also struggled to imagine how key sharing could safely occur, which hints at the key distribution struggles of symmetric encryption. Moreover, while their structural models of what the shared secret actually was were inaccurate, this mistaken belief nevertheless carries similar functional properties. More specifically: (1) if you believe the shared secret to be the set of transformations itself, then compromise of the key is tantamount to compromise of the encrypted data, and (2) loss of the shared secret results in the loss of ability to decrypt encrypted data. Thus, while participants had a flawed model of what a symmetric key is, their ability to interact with one is likely unimpacted.

Relevantly, this strong correlation of existing mental models with a symmetric encryption model also implies that the asymmetric encryption model is non-intuitive. Because keys
in symmetric and asymmetric encryption fulfill such different roles, getting users to understand public and private keys—
even from a functional perspective—seems an uphill battle,
particularly because we have yet to find an appropriate real-
world analogy for the role of public and private keys [17].

Consider, for example, the task of verifying keys (e.g., in
an authentication ceremony) in secure messaging apps. In a
standard access control model, authentication is a unidirec-
tional process: the accessing party verifies to the mechanism;
only one agent is active in this scenario. Verification in an
asymmetric encryption model, such as the authentication cer-
emony; however, requires both sending and receiving parties
to validate one another. Given an access-control abstrac-
tion for encryption, what does the process of verifying the
sending party’s key even mean in the context of receiving
encrypted data? Lacking a model, when users are asked to
perform verification, they are likely to fall back on ad-hoc,
non-cryptographic methods done, as has been observed [18].

**Recommendation**

This common perception of encryption as access control
can be useful in the right contexts. Because it was shared
by all our participants, even those with the most simple
mental models, it can serve as a lowest common denominator
model off which to build, and is likely a useful and intuitive
abstraction in certain use cases. For example, encryption of
personal data at rest, such as that done by mobile devices,
is a good fit for this functional model. Digital wallets, such
as those commonly employed by cryptocurrency, are likely
another use case that fits well with the access control model.

Because asymmetric encryption necessitates a functional
abstraction so foreign to participants’ existing models, the
presentation of interaction mechanisms as “encryption” is
perhaps an unwise approach in these contexts. Instead,
perhaps the way forward is to present users with interaction
abstractions altogether separate from encryption, with a
focus on matching functional, rather than structural, models.

**4.2 Grassroots adoption is also a public rela-
tions battle**

Participants felt that encryption is meant to protect sensitive
information. While, on the surface, this view isn’t necessarily
incorrect, the nuances of this belief have grave implications
for the grassroots adoption of encryption because it suggests
that the perceived utility of encryption is low. More specifi-
cally, from a security perspective, participants believed that
companies already encrypt their sensitive customer data,
such as financial information. With respect to privacy con-
cerns, the personal use of encryption in contexts such as daily
communication, by contrast, is viewed negatively because
it is believed that such data would only be perceived as
sensitive if the user were engaging in either illicit or immoral
activity, or were “paranoid” about the value of their data.

Thus, in scenarios where encryption is seen as having value,
using it is seen as the responsibility of someone else, whereas
in scenarios where using encryption would fall upon them
personally, its use is perceived as improper. This has serious
implications for adoption: if users do not perceive encryption
as having utility—or worse, see its use as stigmatized—then
they are unlikely to make proactive effort to adopt encryption
software even if usability concerns could all be resolved.

**Recommendation**

If our participants’ responses generalize to larger populations,
then it suggests that improving the usability of encryption is
likely not enough: improved risk communication will also be
necessary. That is to say, improving the how of encryption is
unlikely to alone resolve adoption issues; we must also focus
on the why. Users can perhaps be helped to understand
that there are benefits deriving from their individual use
of encryption; even if not personally, but then perhaps to
society as a whole. One of our participants, for example,
described how the personal use of encryption might make
sense in a different cultural context:

Lloyd: “So keeping all that stuff that’s very personal to your-
self is probably good both from a ‘keeping personal stuff per-
sonal’ sort of way and—although this is a little paranoid
in itself, and although this isn’t a big deal right now—but
if in ten years, that person’s engaging in civil unrest, and
that information’s out there, that person can be threatened
indirectly. It sounds really paranoid but that sort of shit
happens in China all the time, you know? [...] that sort of
stuff happens when governments have the ability to straight
up read all the data and you have that kind of oppressive
government going on.”

**4.3 Confusion about encryption strength**

Participants’ perceptions about what it would take to undo
encryption varied greatly, even among participants with simi-
lar mental models, and even among participants’ individual
responses themselves.

One potential cause for this is that factors external to their
mental model seem to have influenced participants’ beliefs.
One participant was aware of the FBI’s inability to break the
encryption on the iPhone of a suspect, and so decided that
encryption was therefore very strong. Another participant
explained that he had seen encryption in popular media and
it had always been broken, leading her to conclude that “if/it
obviously can be done pretty easily.” Other participants noted
the existence of data breaches, which, in combination with
their belief that companies routinely encrypt data, signified
to them that encryption is regularly broken by criminals.

Participants’ responses also made it evident that beliefs about
the strength of encryption—and by extension, its ability to
protect their data—appeared to be focused more on the
capabilities of attackers than it was on the fundamentals
of the technology itself. In other words, even if it takes
incredible resources to break encryption, that doesn’t mean
anything if an attacker has those resources. For example,
Fred assumed that encryption would take “years” to undo
without a quantum computer, which would instead need just
“seconds.” However, because he believed that the NSA does
possess quantum computers, he believed encryption to be
rather fragile as far as they were concerned.

**Recommendation**

It seems that if we wish users to understand the protective
capabilities that encryption can offer them, we must convey
its strength specifically within the context of the capabilities
of likely attackers. We echo the sentiments made by Wash in
his mental modeling effort [20]: “without an understanding of
threats, home computer users intentionally choose to ignore
advice that they don’t believe will help them. Security edu-
cation efforts should focus not only on recommending what actions to take, but also emphasize why those actions are necessary."

4.4 Learning how encryption works doesn’t help
Given that the mental models we describe seem to be flawed or incomplete, one natural reaction might be to assume that the proper course of action is to simply teach users how encryption really works. Research has shown, however, that “correcting” existing mental models can be a difficult task: “one cannot merely present people who hold an incorrect understanding with the correct information” [19]. Indeed, “the ‘broadcast of facts’ approach has been discredited by experts in safety risk communications” [16].

In our study, two participants had been exposed to the detailed mechanics of encryption previously, and yet still evidenced confusion. Clark, having learned of the WannaCry ransomware attack when it made the news, had attempted to learn something about how encryption worked, including watching a video on “how AES-256 encrypts stuff.” This glance into the inner workings of encryption had nevertheless failed to fully impress itself on him, and he explained that all he knew was that “[i]t’s scrambling the, uh, the message. Uh – By doing a lot of math, I don’t know much beyond that.”

Brent described how his girlfriend was well versed in security matters, and had once taught him about encryption. For that reason, he remembered the terms “public” and “private” key, although he remembered neither their function nor their purpose.

Recommendation
Rather than relying on attempts to imbue users with an accurate model of how encryption works as the path to usable encryption, we should make efforts to align designs and communication efforts with the functional models users already possess.

4.5 Consider the context
The way security indicators are interpreted is dependent on users’ perception of what threats exist within the respective context. The HTTPS/TLS browser indicators (e.g., the lock icon) were very effective in the sense that our participants had all noticed their existence, and a couple of participants had even clicked them for more information. However, their interpretation of what these indicators meant is worryingly inaccurate.

Participants mostly lacked a model of the man-in-the-middle as a potential threat, and thus when presented with security indicators, believed them to be representative of site security and not connection security. Those who had clicked through and were aware of the existence of certificates similarly misinterpreted their meaning, believing they meant that a certain site had been “certified” by a third-party. As these browser indicators are not at all a direct measure of site security, but rather indicative of an encrypted TLS connection between the user’s browser and the web server, one could very well have a secure connection to an unsafe website, as Lloyd suddenly realized during his interview. “Oh, really; that’s what that means. I shouldn’t do that then! Because it could be an encrypted way to send my password to hackers!”

Recommendation
Security indicators must be carefully designed, with an aim of not just being noticed and trusted, but also with an eye to construct validity. That is, we must take caution to ensure not only that users understand indicators, but that they do not misunderstand them.

5. LIMITATIONS
Our study carries with it several limitations that are a direct consequence of our sample and sampling method. First, our sample consisted entirely of residents of the United States, and results may be subject to cultural effects. Similarly, our participant recruitment requirements necessitated English speakers; it is conceivable that this would have strengthened cultural effects, if any. Finally, our sample skewed heavily male, and it is possible that this had an effect on our findings, though we did not observe any notable differences between the models of male and female respondents.

The data collected was self-reported, qualitative in nature, and subjected to a coding process. Our findings, as presented, are thus subject to interpretation, and it is entirely possible that other researchers may come to different conclusions. For this reason, we have made our data publicly available.

Additionally, while we did continue our interviews until a perceived data saturation point, it must be acknowledged that our sample size falls on the low end. It is possible that with additional interviews, we would have observed additional behavior. However, because we were exploring a topic for which people’s perceptions are fairly shallow due to limited exposure, and because participants’ mental models were already very similar, we do not believe it likely that we would find any substantially different results with more interviews.

Finally, as explained to our participants before each interview began, encryption is a technical topic that our participants were largely unfamiliar with, and their mental models were unlikely to have been very developed beforehand. For example, when we asked Eva how decryption might occur, she proudly declared, “I never thought about that! You don’t.”

Indeed, it was often evident that participants’ models were evolving during the interview itself, as they considered issues that had not previously occurred to them; this is in contrast to investigating mental models of systems that users frequently interact with, which guide existing behavior. In one explicit example of this occurring, when Sam was asked to explain what a “key” was (a term he had used unprompted), he changed his mind mid-sentence: “The key is kind of like the schema of the code. [...] The algorithm so to speak— No, it’s not the algorithm. The algorithm is what actually does the encryption, but it has to function with a certain pattern, and the key is like the file that knows exactly what pattern that the encryption then does.”

Because participants had to think through issues such as this as part of the interview, and because such thought was typically prompted by questions from the interviewer, it is possible that mental models of encryption in practice are more shallow than as presented here.

6. RELATED WORK
Previous research in this space, as it relates to our study, can largely be divided into two categories: (1) studies concerned
with the usability of encryption and (2) mental modeling efforts in the computer security space.

6.1 Encryption usability

Beginning with the seminal work, “Why Johnny Can’t Encrypt” [23], now published almost 20 years ago, many studies have documented the long history of usability struggles in the encryption domain. As our study is directed at perceptions of encryption, however, we focus on those that reveal difficulties of understanding and not use.

Whitten and Tygar’s classic work [23] tested how standard usability design principles hold up in the domain of computer security by evaluating PGP 5.0, an example of encryption software that was (at the time) considered to meet principles of good design. In addition to a number of interface design flaws discovered via a cognitive walkthrough, a user test found that participants struggled to execute a simple encryption task, simultaneously evincing confusion about core concepts such as the public key model. Tong et al. [17] examined in detail one of the criticisms posed by Whitten and Tygar, evaluating the metaphors used to communicate public key cryptography concepts. They developed a new set of metaphors that focused on the actions involved in the encryption process instead of the cryptographic primitives at work. Testing revealed that these new metaphors improved the efficacy of communication and improved the user-experience. These studies reveal that the mismatch between developers’ and users’ models of how to use encryption tools is a major cause of usability problems, underlining the importance of first understanding how users think when designing security tools.

Two more recent studies have made some progress in understanding mental models of encryption, although only as part of an investigation of broader topics. Abu-salma et al. [1] studied mental models of secure communication as part of a larger effort to understand obstacles to the adoption of such tools. They found frequent misunderstandings, several of which reinforce our own. First, some of their participants conflated authentication and encryption, which is captured by our access control model. They also found that participants often equated encryption with some sort of data encoding or scrambling process, which we frequently observed in our interviews. Probing participants’ understanding of the differences between end-to-end encryption and client-server encryption, they found nearly no one who could distinguish between them. This coincides with our findings that participants’ perception of encryption was nearly unilaterally that of encrypting data at rest, with the exception of a few informed individuals who had some knowledge of HTTPS.

Ruoti et al. [13] examined the risk perceptions and security behaviors of a number of suburban adults. As part of their effort, they asked participants if they had heard of encryption before. They reported that most of their participants understood the basic principles of symmetric key cryptography, recognizing that “encryption relies on a shared key.” By contrast, our more focused exploration of this issue revealed that while participants indeed had some notion of a shared secret in its broadest sense, their conception of what a shared secret might be differs quite drastically from the traditional cryptographic sense. More specifically, instead of an input to an encryption algorithm, many of our participants believed that the set of operations performed during the encryption process were themselves the shared secret.

6.2 Mental modeling in computer security

While not directly relevant to our study, similar efforts have been to explore mental models in a computer security domain, their application in computer security having been previously encouraged [4, 9, 16].

Vollamer and Renaud [19] described the concept and its role in computer security. Importantly, they characterized the methods for exploring mental models, such as think-aloud and diagramming. Wash [20] presented findings of users’ mental models for home security, identifying eight “folk models” that users rely on to guide them in making security decisions. (This was later replicated with a German population, by Kauer et al. [8].) His approach for synthesizing interview data into discrete mental models served as a guide for the process we followed in this work. Bravo-Lillo et al. [3] demonstrated how mental modeling can be used to understand how novice users and advanced users interpret and react differently to security warnings. They presented participants with a series of warnings and asked questions about their perceptions and thought process. Kang et al. [7] explored mental models of the Internet and how that affects user perception of privacy and security and included a diagramming portion as a central element of their work. As mentioned previously, we employed both a question-and-answer process (similar to Wash and Bravo-Lillo et al.) as well as a diagramming exercise (like that used by Kang et al.).

7. CONCLUSION

In this paper, we present our findings drawn from 19 semi-structured interviews with U.S. participants about their perceptions of encryption. Our focused effort to explore these perceptions sheds additional light on, and adds nuance to, existing research that touched upon aspects of this problem. We identify four mental models of encryption, of varying levels of detail and complexity, that convey functional abstractions of access control and the mechanics of a symmetric encryption model. We highlight concerns about the current state of how encryption is presented to users and how they are expected to interact with encryption tools.

Perhaps because our study focuses on perceptions of encryption divorced from implementation, we find an urgent need for improved risk communication efforts regarding encryption. Notably, we must make greater attempts to contextualize why participants should use encryption in a manner that takes into consideration their threat models. Similarly, we should strive to frame the functional aspects of encryption in a form that matches the intuitive models users possess, regardless of their technical accuracy.

8. ACKNOWLEDGMENTS

We would like to express our appreciation for Rick Wash and Emilee Rader for their guidance in the early stages of this work. We also thank the anonymous reviewers for their helpful feedback. This research is sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD) via contract number HHSP23201600046C.
9. REFERENCES


Appendix

Interview introduction

1. Before we start, I just wanted to say that what we're going to talk about today is likely to be a subject you're not very familiar with—so please don't worry, this isn't a test. Instead, I'm interested in hearing what you think and feel, so don't be worried if you don't think you know the answer to a question. If that happens, just take your best guess. Also, if you're ever confused by a question I'm asking, please let me know, and I'll try to explain or rephrase.

2. If there are no other questions, let's get started.

3. To begin, I'd like to get a general sense for your background, and so I'd like to ask: what do you do for a living?

4. Now I'd like to get a sense for your computing environment. Can I ask what types of devices you own: laptop, desktop, smartphone, etc.? What types of things do you do with them on a regular basis?

Existing thoughts on encryption

1. Now I'd like to turn to the topic for today. My first question is: what comes to mind when I say the word “encryption”?
   • What sorts of imagery do you picture in your head when I say that word?
   • Where have you seen or heard that term before?

2. Now I'd like to begin the diagramming task I mentioned in the email. Before we start, I'd like to remind you that this isn't a test of your artistic ability; this is just to help me get a better sense for how you imagine things work.

3. I'd asked you to prepare a pen and paper for this: do you have them ready?

4. Great. Now, on your piece of paper, please write the sentence, “This is a message to be encrypted.” Now, what I want you to do is imagine you're going to encrypt this sentence, and draw whatever you think that looks like. Take as much time as you need and let me know when you're done.

5. Next, could you just draw a simple little picture for me? It can be anything, like a cloud, tree, stick figure—anything. Now, I want you to do the same thing you just did, but with the picture. Imagine you're going to encrypt this picture, and draw whatever you think that looks like. Again, take as much time as you need and let me know when you're done.

6. Could you take a picture of the drawing with your phone and text or email that to me? Thanks.

7. [Once the email with their picture arrives...] Great, I got it. Could you walk me through what you drew?

8. Okay, so my next question is: imagine you're going to send an encrypted message to a friend or family member and what they get is just the encrypted part. What would they have to do to read the original message?

Examples of encryption

1. Okay, we're going to change gears a bit now from what encryption is and how it works to how it gets used.

2. First, what role do you think encryption plays in your life?
3. **What about individuals?** Do you think there are people that use encryption on a personal basis?

4. Now, I'm going to introduce a few examples of places where encryption does exist. Again, it's entirely fine if you've never heard of any of these before: I'm interested in hearing your impressions anyway, so please make your best guess.

5. **[Smartphone encryption]**: The first example is smartphone encryption. Both iOS—if you have an Apple device—and Android allow you to encrypt your smartphone. Now, my first question is: what do you think it even means to "encrypt" your smartphone?
   - Why do you think this function exists? What do you think encryption is supposed to protect?
   - Who do you think encryption would be protecting your phone from?

6. **[Web encryption/HTTPS]**: The next example we’re going to discuss is encryption of data that goes out over the Internet. Have you ever noticed an “HTTPS” or little lock icon near your address bar when using a browser? What do you think it means?

7. So what it means is that the data going between your browser and the web server is encrypted.
   - What do you think encryption is protecting in this case?
   - Who do you think it’s protecting you from?

8. **[Secure messengers]**: Now I want to talk about secure messaging apps. Have you ever used an instant messenger like WhatsApp, Facebook Messenger, Signal, or Telegram?
   - So it makes sense why you’d want to encrypt sensitive information like financial information. But why do you think someone might want to encrypt their daily communications?
   - Who do you think you’d be protecting your communications from by encrypting them?