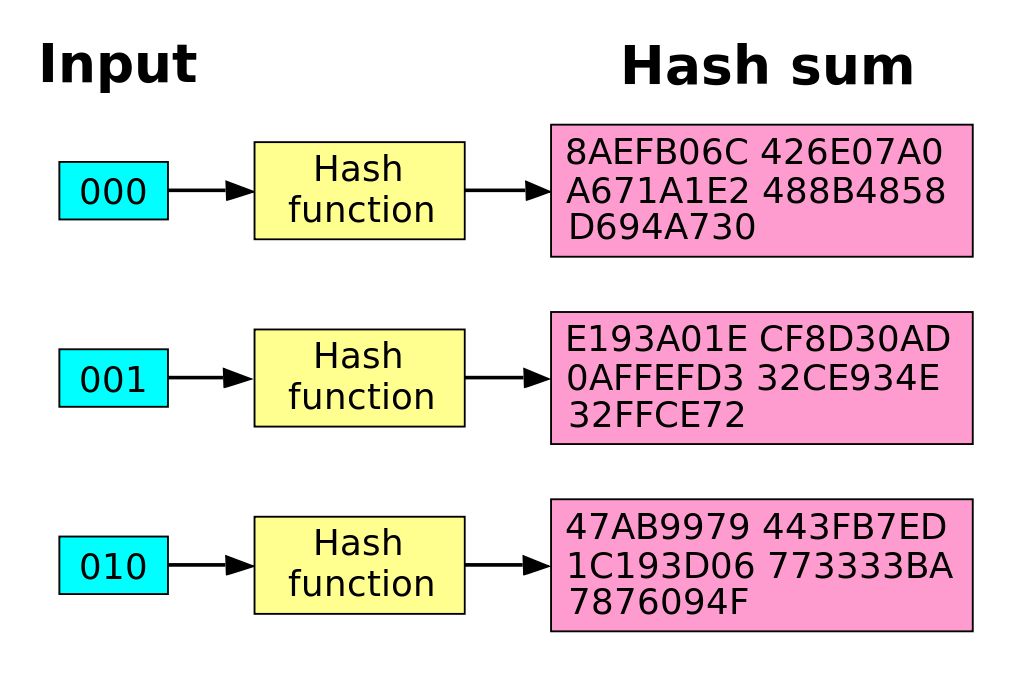
Rhetorical Situation

The word “Encryption” has appeared frequently in mainstream media recently. Between the UK government trying to make encryption illegal to the FBI trying to force Apple to create a backdoor for the iPhone, encryption is the new hot topic in technology the media is now focusing on. However, many people don’t realize why encryption is so important, and a lot of that is because they don’t understand what it means. I am writing a blog post intended for the general public to provide an introduction to encryption. This should give people who are confused about a basic understanding of why Apple’s fight with the FBI and the UK’s actions are significant. This extended definition will be in the form of an article on a blog or online newspaper intended for all to see. In order to enhance he reader’s understanding of the term encryption there will be several diagrams and visuals included in the article.

Extended Definition:

With the announcement of Apple refusing to comply with the FBI’s demand for a backdoor into the iPhone, everyone seems to be talking about encryption. But what does “encryption” really mean? And why would Apple refuse to comply with the FBI over it? It all has to do with how electronic devices interpret data. A computer’s memory can be thought of as millions of rows of “switches” called “bits” that can either be on (0) or off (1). When 8 of these bits are put together, it is called a byte and represents a number between 0 and 255. Each of these numbers can represent a character: letters, digits, punctuation, emoji, etc. This is how files are stored, by declaring that some arbitrary chunk of memory is now going to be taken up by the data for this file and then writing the relevant information to that memory.

 However, since this data is stored in this way, any program can read that memory and understand what it is. Encryption is the process of taking data and making it unreadable without some sort of “key.” When someone encrypts a file, at a very basic level, what they are doing is walking through each byte in that file and running it through some sort of mathematical computation. These computations are called “hashing functions” and are often operations that are quick for a computer to execute but take forever for a computer to do the inverse, that is undo. For example, squaring a number is easy for a computer to do since all it has to do is multiply the number by itself. However, doing the square root of a number takes a lot more computational time (it is more computationally complex) since the computer might have to guess and check until it is correct. So if you don’t know how a file is hashed, guessing and checking until you are correct could take thousands or even millions of years to decrypt. However, whenever you encrypt a file, you need to have a way to read it. This is where “keys” come in. Keys are generated with a hash to provide the user with a way to decrypt the data. This way, whoever encrypts the file can share the key with whomever they want to have access to the encrypted file and not have to worry about the data being intercepted by someone else. There are many different strategies for encryption that take different approaches to hashing the data and generating the keys, but the basic premise is that once a file is encrypted, it is unreadable by anyone who doesn’t have the key to decrypt the file.

In the case of the FBI versus Apple, the FBI wants there to be a Sway for the FBI to have access to the key that encrypts iPhone data. For security purposes, programs that encrypt data frequently hand the generation of keys off to some random factor on the device and keep that key hidden from the programmer and the user. This results in secure software that even the programmer cannot break into. However, if a programmer wants to be able to access this key later, they can build in what is called a backdoor, which gives them access to encrypted data without the knowledge of the user. This is the equivalent of a locksmith replacing the locks on your door and making a copy of the key that he keeps for himself in some drawer in his shop. Even if he promises to never enter your house without your permission, he still has the access to do so without it. This is why Apple creating a backdoor to the iPhone is so controversial as it would put millions of devices at risk of invasion of privacy.