Privacy in the Age of Computers

Encryption, Steganography, Cryptography, and more.

Josh Natis

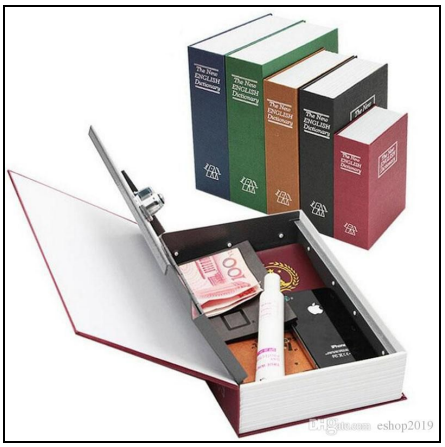
The Introduction

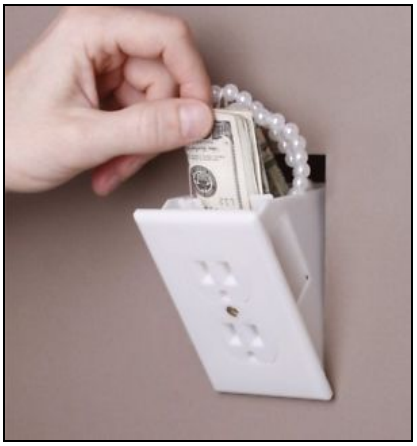
Imagine this:

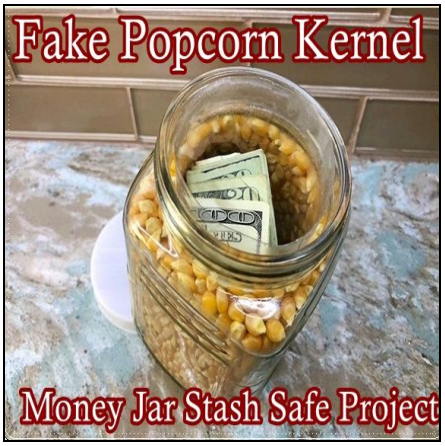
You're Jeff, just a regular guy living a regular life. One day, you get a letter in the mail informing you that your rich uncle living in Siberia has recently passed away and left you a whopping $75,000 in inheritance! The money is enclosed in the envelope. You don't have time to grieve, as you must quickly figure out how to secure your money before your no-good-dirty-rotten neighbor Jim attempts to steal your loot! What do you do?

Your first instinct is to hide the money -- perhaps you could shove it under your mattress like the gangster you are, or maybe you could bury it in the backyard along with the skeletons and dog bones. Those are feasible options, but only if your hiding place is not found. Given an infinite amount of time, no hiding place is truly secure. Security through obscurity is no security at all.

If you really want to outsmart Jim, you'll have to think outside the box. Maybe you could disguise the money in plain sight…







Some great examples brought to you by Google Images

Then again, there's always a chance that Jim also read this Ars Technica article on Steganography, so he'll be on to you and your tricks. This plan shares the same downsides as

your first -- if Jim ever catches on to the fact that you are attempting to hide something from him, your money will no longer be secure.

Suddenly you remember -- KISS (keep it simple, stupid). The obvious answer is to go buy a safe and lock your money up in there. As long as Jim doesn't have a key, he'll never be able to crack your safe and steal your cash.

The Connection

Of course, you probably don't have a rich uncle living in Siberia nor $75,000 in cash to hide. You probably don't even have a neighbor named Jim, because who in the world names their son Jim? Regardless, the above scenario is a rough analogue to the state of encryption and securing data in the age of computers. I'll attempt to draw the connection:

Data is power. The $75,000 in our example is equivalent to your online belongings -- your passwords, files, conversations, and etcetera. If you've been keeping up with the news, you may remember the shenanigans involving Facebook, Cambridge Analytica, and the Trump Administration where private user data was used in an attempt to skew the results of the 2016 presidential election. Although other factors besides encryption (or lack thereof) were at play, the main thing to note is the sheer power encapsulated in your data -- you're worth more than Jeff's $75,000.

Hiding the money was meant to serve as an example of "security through obscurity", which is a pretty instinctual way for humans to think about protecting their belongings. In the context of data and computers, the concept means something slightly different: "Security Through Obscurity (STO) is the belief that a system of any sort can be secure so long as nobody outside of its implementation group is allowed to find out anything about its internal mechanisms." In other words, the strategy is to hide your source code and not give anybody information about how your product works. This technique was frequently employed by the NSA, though it is heavily critiqued (as you could probably tell by the maxim included above, "Security through obscurity is no security at all"). However, this approach is essentially anti-thethical to the Open-Source and Free software movements, which have become commonplace today. There is a reason for the growing popularity of these movements -- for the most part, it is due to the validity of their claims. To quote ESR from his book, The Cathedral and the Bazaar, "given enough eyeballs, all bugs are shallow". This line of thinking claims that making code public, so that anybody could observe and contribute to it, is much more effective than keeping it secret and locked up. Ultimately, this means that security through obscurity is counterproductive, on top of not being considered a valid way of protecting data.

Jim's idea of disguising the money in plain sight is an analogue to Steganography. Although the sentiment of "hiding" is similar to STO (security through obscurity), this technique is a bit more complex than simply hiding something under your mattress. "The advantage of

steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest." The advantage this provides is not to be understated. For most forms of encryption, if an attacker had an unlimited amount of time and willpower, she would be able to use brute-force to break them. Yet, most attackers would likely not be interested in a jar of popcorn kernels (see the image on the previous page), so your $75,000 would remain safe. Historic uses of Steganography have been traced back to 440 B.C -- perhaps you've heard of the Trojan Horse? If for no other reason, Steganography is worth looking into simply because it's cool.

Lastly, we had the idea of storing the money in a safe. It's likely that you thought it strange for me to include that as the last example, when in reality it would have probably been Jim's initial thought. My justification is that safes don't exist in nature. It wasn't until somebody commoditized the idea of a safe that they became omnipresent objects in our society. This was necessary to point out, as "encryption" of data isn't necessarily the most intuitive idea to the average person. If you want to hide something, your initial idea likely isn't to obfuscate it -- it's just to hide it somewhere. The same applies to safes (not many would think to protect things by shoving them into a unopenable box that can only be accessed with a magic stick), except that at this point in our society they are common objects, so their concept has been normalized. Anyways, that was just a long-winded way of saying that cryptography is the norm in securing data today, though it is only one of the techniques in our arsenal. Modern cryptography is heavily based on mathematical theory. This indeed does mean that the "safe" is analogous to math… which is extremely cool. Many cryptographic algorithms are based on math that is easy to "do" if you have a "key" (similar to a regular key), but extremely difficult to "do" otherwise (of course nobody is doing this math by hand, but rather it is computed). This means that most algorithms aren't proved to be impossible to crack in general, but rather *in practice*. This concept of being "theoretically possible to break, but infeasible by any known practical means", is called being "Computationally Secure". This is opposed to being "Unconditionally Secure". As you will see later, there are a multitude of subfields of cryptography, each adding to the layer of complexity of which the field is notorious for.

The Meat -- A Preface.

Now that I've introduced cryptography and steganography, hopefully in enough of an intuitive fashion, I'll delve into the specifics of each. It is important to keep in mind that a lot of this consists of math -- specifically math that involves big numbers, isn't meant to be done by hand, and whose purpose it is to keep assailants at bay. What this means for you is that you should think of the math a bit differently as you would your typical educational math, since this domain does not employ it as a tool to model reality. For example, there is no analogue to prime numbers in our daily lives -- they are just a mathematical concept.

The Meat -- Cryptography

We've already established that data is extremely powerful, and thus must be secure. But is that the only reason? I'd like to point out the role that the human intrinsic need for privacy plays in making encryption as prevalent a field as it is. If we're to believe holy scriptures, then privacy has been an issue since the time of Adam and Eve (starting from the moment Eve took a bite of that apple). Being able to control what other people see and know about you is an integral part of human existence. This is why we wear clothes, have social filters, and et cetera. One of the original wonders of the internet was anonymity. Preserving that was a major part of bringing the internet into the forefront of society. Not being able to have a private conversation online would be a deal breaker for most.

(NOTES)
Analogy - Castle, defence in depth

TYPES OF CRYPTOGRAPHY

- *Substitution ciphers (ex caesar cipher)*
    - *letter frequency is preserved (e is most common letter)*
- *DES (data encryption standard, IBM NSA)*
    - *64 bit key*
- *AES*
    - *256 bit key*
    - *compromise between power and speed (too slow to load or encrypt means people wont use it)*
    - *server needs to send secret key to user's computer so it can unencrypt the message*
    - *key can be intercepted by an attacker*
    - *solution: key exchange*
        - *computers agree on a key without actually sending one*
        - *do this via one way functions (easy to do one way, but hard to reverse)*
        - *for example, easy to mix paint colors, but impossible to separate and hard to tell which exact colors we used to make the color*
        - *diffie helman modular exponentiation --*
        - *SYMMETRIC - key is the same on both sides*

- *ASYMMETRIC*
    - *public and private key*
    - *public lets you encrypt but not decrypt*
    - *for example, if i give you an open safe, you can put your money in there and close it, but without the key you cannot open it back up.*

The Meat -- Steganography

- Embedding data in images