Privacy Café

What Is Encryption?

Encryption is the mathematical science of codes, ciphers, and secret messages. Throughout history, people have used encryption to send messages to each other in the hope that those couldn't be read by anyone besides the intended recipient.

Today, we have computers that are capable of performing encryption for us. Digital encryption technology has expanded beyond simple secret messages; today, encryption can be used for more elaborate purposes, for example to verify the author of messages or to browse the Web anonymously with Tor.

Under some circumstances, encryption can be fairly automatic and simple. But there are ways encryption can go wrong, and the more you understand it, the safer you will be against such situations.

THREE CONCEPTS TO UNDERSTAND IN ENCRYPTION

1. Private and public keys

One of the most important concepts to understand in encryption is a key. An encryption key is usually a simple file containing random data which is then mathematically applied to the information to be encrypted. Common types of encryption include, on the one hand, a **private key**, which is kept secret on your computer and lets you read messages that are intended only for you. A private key also lets you place unforgeable digital signatures on messages you send to other people. A **public key**, on the other hand, is a file that you can give to others or publish that allows people to communicate with you in secret, and check signatures from you. Private and public keys come in matched pairs, like the halves of a rock that has been split into two perfectly matching pieces, but they are not the same.

2. Security certificates

Another extremely valuable concept to understand is a security certificate. The Web browser on your computer can make encrypted connections to sites using **HTTPS, where the "s" means "secure"**. When they do that, they examine certificates to check the public keys of domain names—(like www.google.com, www.amazon.com, or ssd.eff.org). Certificates are one way of trying to determine if you know the right public key for a person or website, so that you can communicate securely with them.

From time to time, you will see certificate-related error messages on the Web. Most commonly, this is because a hotel or cafe network is trying to break your secret communications with the website. It is also common to see an error because of a bureaucratic mistake in the system of certificates. But occasionally, it is because a hacker, thief, police agency, or spy agency is breaking the encrypted connection.

Unfortunately, it is extremely difficult to tell the difference between these cases. This means you should never click past a certificate warning if it relates to a site where you have an account, or are reading any sensitive information.

3. Key Fingerprints

The word "fingerprint" means lots of different things in the field of computer security. One use of the term is a "key fingerprint," a string of characters like "342e 2309 bd20 0912 ff10 6c63 2192 1928" that should allow you to uniquely and securely check that someone on the Internet is using the right private key. If you check that someone's key fingerprint is correct, that gives you a higher degree of certainty that it's really them. But it's not perfect, because if the keys are copied or stolen someone else would be able to use the same fingerprint.

access

EDRi

LIGA VOOR
MENSENRECHTEN