Supplemental Resources on Digital Signatures

Below you'll find many supplemental resources on digital signatures!

Be sure to read/watch these resources as they will help deepen your understanding of these algorithms.

ECDSA

Cloudflare provides a great article on how ECDSA is used on the web. If you've ever thought about how HTTPS works, this is your chance to dig in further!

Of course, wikipedia has a write-up on ECDSA. Naturally, it's very heavy math, however there are some interesting tidbits in here to pick up even if your math isn't super strong!

This resource is similar to the wikipedia article above, except it does a much better job of explaining ECDSA mathematics in simpler language.

Bitcoin

Bitcoin uses secp256k1. The parameters for this curve are thought to be the least *random*, they are predictably selected, so there is supposedly less likelihood of a backdoor hidden in this algorithm.

In our Exchange project, we'll need a way to go from a public key to an address, so it is useful to understand how Bitcoin derives addresses. The diagram at the bottom of this article shows the derivation of the address starting all the way from the private key.

This is further technical detail of the address derivation. It also explains the **Checksum** written into Bitcoin.

> Bitcoin chose Base 58 for it's addresses because this format removes commonly mistaken characters like zero "0" and upper-case o "O".

Diffie-Hellman Key Exchange

We talked about Whit Diffie and Martin Hellman discovering the Public Key quite a bit. However, we didn't talk much about the Diffie-Hellman exchange which is critical to the TLS handshake for HTTPS.

> The Diffie-Hellman key exchange is utilized in a **hybrid** cryptosystem since it uses asymmetric cryptography for the handshake and then symmetric cryptography for the message passing.

To understand more about this key exchange, check out this colorful explanation as well as this more mathematical one. And another good follow up is this video on Elliptic Curves.

RSA

Just like with ECDSA, wikipedia gives a good overview and the cryptobook gives a good explanation in plain English.

There are two great videos on RSA mathematics given by Eddie Woo on YouTube (his **WooTube** channel !). Here is part 1 and part 2.

> There is supposedly evidence of a RSA Backdoor planted at some point in time.

Mark Complete