Week 3

**From our look at the history of cryptography (including this chapter) identify one key moment in the evolution of cryptography. Explain why you think it was important and what impact it had. Don't choose the same topic as one of your classmates.**

1997 was a banner year for the burgeoning internet. The base version of the 802.11 wifi standard gets introduced to the IEEE. Deep Blue proved that it wasn't a fluke by beating Garry Kasparov a second time. Google.com was registered as a domain name as was Facebook.com, Netflix.com, and Craigslist.com. 22 years ago and still products and items defining the collaborative, distributed, and powerful nature of ubiquitous computing and network connectivity today. Computing power was taking a leap in quantity of resources as well as the interconnectivity of users and those user's resources.

Amidst all this was Distributed.net. It was one of the first volunteer based, distributed computing projects. It's genesis came out of RSA set of challenges to demonstrate the need for stronger and stronger encryption. RSA published blocks of ciphertext to the public using more and more complex encryption mechanisms. To win the prize money a team had to provide the plaintext and key that would yield the ciphertext. The context of RSA offering these challenges is intrinsically tied to the EFF/Bernstein/NSA fight that was working its way through the courts during the 90's. For any challenges like this the main contenders had been lone cryptographers that happened to have the awareness of the challenge, the know how to attack the cipher, and most importantly access to spare CPU time. A rarified subset of the world and consequently RSA felt that they had to offer up these challenges to draw more focus to the weakness of the shorter key lengths.

Along comes Distributed.net. A collective of interested parties that had the flash of insight and determination to make the leap to attacking this problem using a relatively new approach. Create a simple client that would allow people to "donate" spare cpu processing power by running the client. The client would periodically connect back to the orchestration server to deliver the work it had already computed as well as pull down the next item to process. Looking back through the lens of 22 years it seems a trivial leap to make clients that anyone could install that would divide and conquer the keyspace for a brute force attack. Hindsight is 20/20. This project demonstrated the feasibility of many small contributions coming together to rival the gated community of super computing. It stumbled into and developed solutions to distributed workload problems. How to handle disparate rates of workloads completed by different nodes. How to build infrastructure to handle the incoming data. How to encourage participants by making the statistics into a game. How to then deal with participants willing to corrupt the results. On and on. It inspired SETI@Home, Folding@Home and various other projects of communal good came later and are directly attributed to the path this highlighted.

<https://en.wikipedia.org/wiki/Distributed.net>