## Why write about the Diffie-Hellman Key Exchange Protocol?

Diffie-Hellman Key Exchange originated from a simple question: how can two parties exchange keys, when eavesdroppers can listen in on every message exchanged during the process?

When the internet first started, universities and research institutes would lay cables from one end to the other. No communication would pass by another eavesdropper. However, when the modern internet involved, packets are sent everywhere. To visit a website hosted in America (e.g. Netflix), the packet would pass through many routers based in many countries. How then, can any communication be secure if no secure channel can be established?

Insecure channels form the foundation of the modern internet, so being able to establish a secure channel in an insecure channel is important. Key exchanges lay the foundation for any symmetric key encryption that is developed – first, a key needs to be exchanged.

The mathematical solution of the Diffie-Hellman Key Exchange is elegant. Two parties exchange messages with each other in public, much like two people talking to each other in public. At the end of the protocol, they can decide on a shared key that no one else knows. The important factor is that **information is not exactly shared during the exchange – information is created**. Furthermore, the protocol is one of the simplest security protocols which exist.

More interestingly, analysing the Diffie-Hellman protocol can reveal a lot of concepts on modern security. In the protocol, assumptions are precisely stated (e.g. that Discrete Logarithm is difficult). The protocol is based so strongly on the proof of hardness that if one day, a new algorithm would break the DL problem easily, then Diffie-Hellman would be insecure. Being able to reduce an entire protocol to a mathematical problem makes for an easy way to quantify the security of the protocol.