The **Diffie-Hellman key exchange** was created by Whitfield Diffie and Martin Hellman to address the issue of securely identifying a shared key between two people communicating via an unsafe network.
It would be easy for someone to eavesdrop on our conversations and alter the data we send over the network if they had access to the hardware through which our data flows. To stop listening in on our communications network and protect its confidentiality, cryptographic techniques were created. However, the employed cryptographic techniques will need to reveal some information in order for the parties involved in the communication to be able to interpret the encrypted messages they are sending to each other.

The talking parties should decide on this shared data, or cryptographic key, which will be referred to as the key. The proper ciphertext or plaintext can only be recovered after the message has been encrypted and decoded using the key.As was previously said, the sender and recipient must both have access to the same key for the cryptographic method to work effectively. While decryption is the recipient's obligation, encryption is the sender's responsibility. Without the common language, they are unable to converse.

Diffie-Hellman, to safely exchange keys over an unprotected network, key distribution and exchange can be combined. The proper operation of this system requires an understanding of prime numbers and modulo operations.

Binary values, or "bits," used by contemporary computers can have the values 0 or 1. A "qubit," on the other hand, is used in quantum computing and is based on the idea that subatomic particles may maintain (or "superpose") several states at once. This indicates that a qubit can simultaneously store a 0 and a 1. Quantum computers can calculate several values concurrently while classical computers can only calculate one value at a time. As a result, encryption may not be able to protect our online communications or stop illegal access to critical information like our financial records.

Similar to using the same key to lock and unlock a safe, symmetric encryption protects data. One method for breaking symmetric encryption is a "complete assault." In a brute-force attack, each potential decryption key is repeatedly tried by the attacker until they are successful.

In the first step, reliable symmetric encryption algorithms are created so that the data can be decoded most successfully through a thorough attack in the absence of the key. Furthermore, the way they are built makes it difficult for a typical computer to fully attack the system because there are so many different possible keys. The amount of work (or "work factor") necessary to launch a comprehensive attack can be calculated using the key length and other resources such as computer power, memory, energy, and money. Multiply the key length by one million to get the required security level. If the keys are too long, there will be so many incorrect answers that the required effort will be greater than what is physically possible in terms of time or space. Either there isn't enough electricity to power enough computers to do the job, or there isn't enough silicon to make enough computer chips to build enough computers. Each of these possibilities is equally likely.

When used in conjunction with cutting-edge methods of sorting through the results, quantum computing would allow for the simultaneous testing of many potential keys, greatly reducing the time needed to find the right one. The square root of the difficulty of the problem is made easier to solve thanks to the reduction, which is so significant that it is equivalent to shortening the key by a factor of two. If the key length yields 10,000 potential keys, halving the key length would result in a 100-fold reduction in the number of keys to test. In comparison to the existing approach, which necessitates the testing of 10,000 keys, it would be a major improvement.

Lecture Notes: 11/15/2022 – 11/27/2022