Lab3 Papers

Group 3

New Directions in Cryptography Introduction

Paper written by Whitfield Diffie and Martin E. Hellman, pioneers in the field of cryptography (November 1976)

This paper introduces the idea of public key cryptography and the reasons for it’s creation

At a time when the digital world was rapidly expanding, traditional cryptographic methods were increasingly inadequate due to their reliance on secure key distribution and lack of digital signatures. Diffie and Hellman proposed a novel approach to solve these issues, thereby setting the stage for the secure digital communications we rely on today.

They needed some sort of “equivalent of a written signature”

What is the paper trying to convey or solve

Traditional cryptographic systems were limited by the need for secure key distribution and inability to provide digital signatures.

Goal of the Paper: To propose a new cryptographic framework that:

- Minimizes the need for secure key distribution.
- Supplies digital equivalents of written signatures.
- Transforms cryptography from an art to a science using public key systems.

"The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel." (pg. 1)

Real World Examples

1. Secure Internet Protocols (HTTPS, SSL/TLS): Diffie-Hellman is crucial in establishing secure sessions between web browsers and servers, allowing for safe data transfer over the internet. Before its implementation, securing these connections was more cumbersome, relying on direct, secure key exchanges which were not scalable for the internet's growth.
2. VPN Security: Virtual Private Networks (VPNs) use Diffie-Hellman to securely establish a shared secret key over a public network without prior communication. This method enhances the security of remote access to organizational networks, drastically improving the flexibility and security of remote work and data accessibility.

Attacks involving Diffie-Hellman

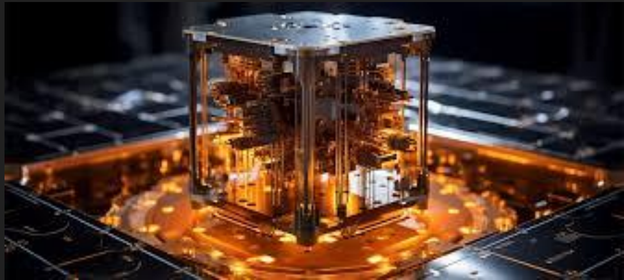
1. Technical Attack (Logjam Attack): Discovered in 2015, the Logjam attack exploits weaknesses in the way some websites implement the Diffie-Hellman key exchange. Attackers can downgrade vulnerable TLS connections to 512-bit export-grade cryptography, which can then be decrypted in real-time. https://weakdh.org/

2. Non-technical Attack (Social Engineering): A notable non-technical attack does not target the algorithm itself but rather the implementation or the users. For instance, attackers might use phishing to trick users into installing compromised software that undermines the integrity of otherwise secure Diffie-Hellman key exchanges, such as installing keyloggers that capture session keys as they are generated or exchanged.

Future/Threats

Continued Relevance: Despite the emerging threats, protocols like Diffie-Hellman are anticipated to remain foundational in digital security, particularly with advances in cryptographic techniques that address new vulnerabilities.

Quantum Computing Threats: Quantum computers pose a significant risk to traditional cryptography, including Diffie-Hellman, as they can potentially solve discrete logarithm problems very quickly—a fundamental challenge the security of Diffie-Hellman relies on. Current research in post-quantum cryptography seeks to develop new algorithms that can resist attacks from quantum computers, ensuring that the cryptographic foundations laid by techniques like those proposed by Diffie and Hellman evolve rather than become obsolete.



Bitcoin: A Peer-to-Peer Electronic Cash System Introduction

Paper written by Satoshi Nakamoto (October 2008)

This paper introduces the motivation and the implementation of Bitcoins

Introduces Bitcoin as a solution to online payments without a financial institution as an intermediary. The traditional trust-based model with financial institutions is fraught with mediating disputes and fraud risks.

"What is needed is an electronic payment system on cryptographic proof instead of trust..."
(pg. 1)

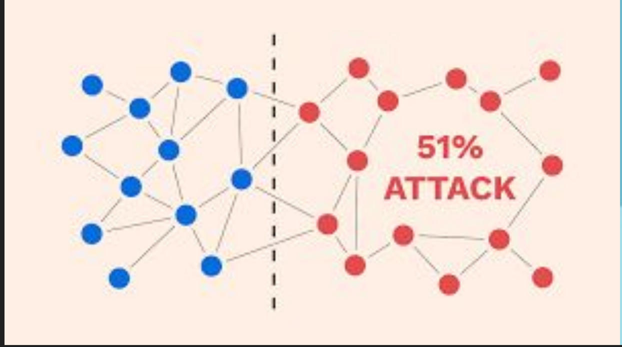
What is the paper trying to convey or solve

- The paper addresses the key challenge in digital currency: preventing double-spending without the need for a trusted authority.
- It proposes a decentralized network using cryptographic proofs to record transactions.
- It also goes through the specifics of how Bitcoin works talking about the steps to run the network and verification details with much more

Real World Examples

1. Overstock.com became one of the first major online retailers to accept Bitcoin in 2014. This adoption signaled a significant step towards mainstream acceptance of Bitcoin as a legitimate form of payment for goods and services. It showcased Bitcoin’s potential to act as a functioning currency, not just an investment vehicle or speculative asset.
2. MicroStrategy, a business intelligence company, adopted Bitcoin as a primary treasury reserve asset in 2020. By converting a substantial portion of its cash reserves into Bitcoin, MicroStrategy bet on the cryptocurrency as a more dependable store of value than traditional fiat currency, particularly in the face of dollar inflation.

Cybersecurity attacks



1. Technical Attack (51% Attack): Theoretical attack where if an entity gains the majority of the network's hash rate, they could conduct a double-spending attack or prevent new transactions from gaining confirmations, undermining the blockchain’s integrity.
2. Non-Technical Attack (Phishing Scams): Despite the robustness of the blockchain itself, the ecosystem is not immune to human error. Phishing attacks are common, where attackers fool Bitcoin holders into revealing their private keys, leading to the theft of their funds.

Future applications

- Longevity: Bitcoin's underlying principles are sound, and it is likely to remain a staple in the digital currency space. However, it will need to evolve, especially in terms of scalability and energy consumption.
- Current Threats: While the network is secure, it is not invulnerable. The most significant risks come from potential regulatory crackdowns, the environmental impact of mining, and technical issues like scaling and transaction time.
- Emerging Alternatives: New cryptocurrencies and blockchain innovations are continuously emerging. Some aim to improve on Bitcoin's limitations, offering faster transactions, more privacy, or more complex smart contract capabilities. However, Bitcoin's first-mover advantage and widespread recognition provide it with a significant edge.