Diffie-Hellman Key Exchange

Names: Tyrek Kelly, Lassine Guindo, Marcus Jackson, Bangalie Koroma, Ulises Servellon, Antonette Simms, Lucky Uchendu

Introduction

- Diffie-Hellman is a secure way for two people to create a shared secret key over a public channel using math.
- Alice and Bob each pick a private secret, mix it with public numbers, and exchange results so they both compute the same secret key without revealing their private numbers.

Why is it important?

- **Diffie-Hellman enables secure communication over the internet by allowing two people to create a shared secret key without meeting in person.**
- **This secret key is then used to encrypt messages, making sure only the intended recipient can read them.**

Advantages of Diffie-Hellman

SECURE KEY EXCHANGE: ALLOWS SECURE KEY EXCHANGE OVER AN INSECURE CHANNEL.

NO PRIOR KEY SHARING NEEDED: PARTIES DO NOT NEED TO SHARE KEYS BEFOREHAND.

FOUNDATION FOR OTHER PROTOCOLS: USED IN MANY SECURE COMMUNICATION PROTOCOLS LIKE TLS, IPSEC, AND SSH

Real World Scenarios

- Virtual Private Networks (VPNs)
- Scenario: VPNs are used to create secure connections between remote users and private networks over the internet.
- Contribution to Secure Encryption: Diffie-Hellman is used during the initial setup of the VPN connection to securely exchange cryptographic keys between the user's device and the VPN server. This ensures that all data transmitted over the VPN is encrypted and protected from eavesdroppers

- Online Banking
- Scenario: Online banking platforms require secure communication channels to protect sensitive financial transactions and personal information.
- Contribution to Secure Encryption: Diffie-Hellman is used to establish a secure connection between the user's browser and the bank's server. By securely exchanging keys, it ensures that all data, such as login credentials and transaction details, are encrypted and cannot be intercepted by attackers

Potential Threats

Man-in-the-Middle Attacks: A hacker can secretly jump in between two people during the key exchange and trick them into thinking they're talking to each other, when really, the hacker is in control.

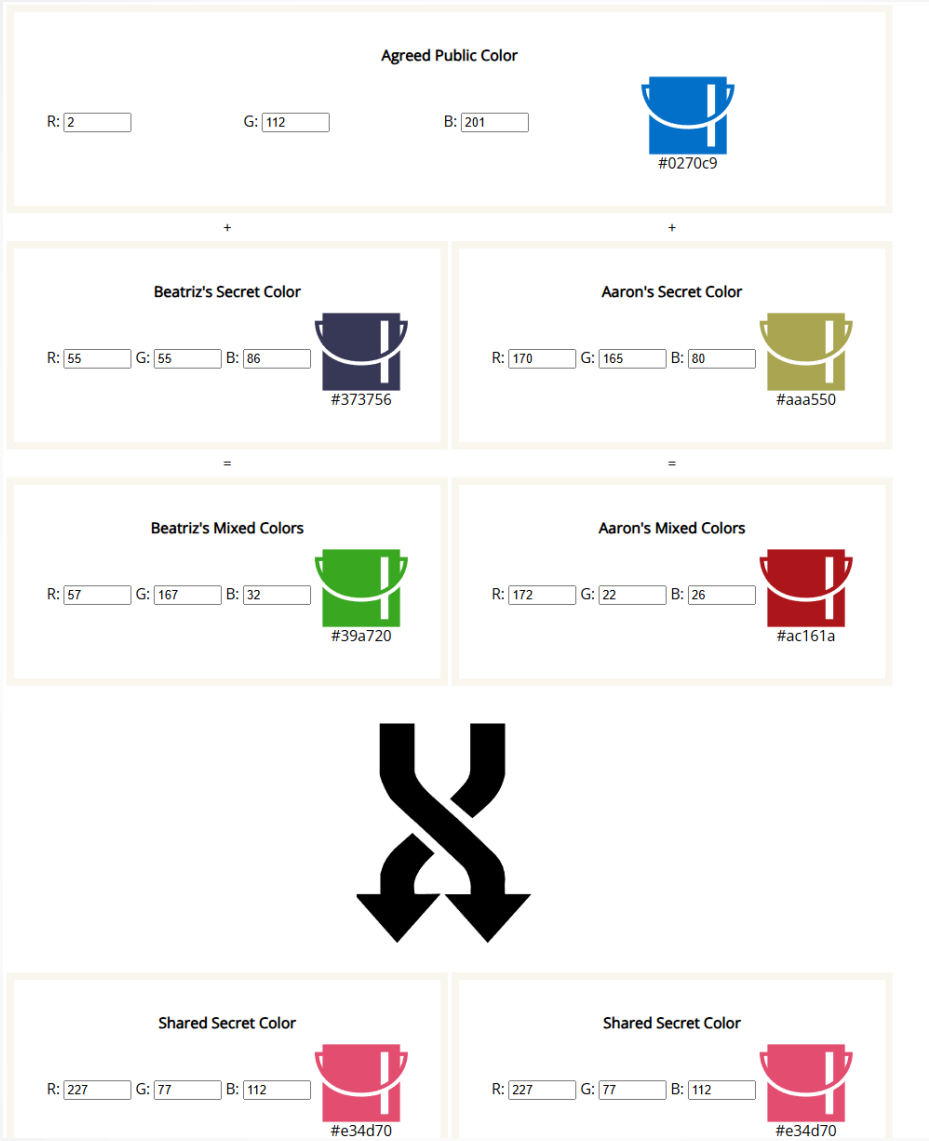
Computational Attacks: Some attacks use powerful math tricks to break the security of Diffie-Hellman, making it easier for hackers to figure out the secret key.

Mitigating Threats

Authentication: Use authenticated versions of the protocol to prevent man-in-the-middle attacks.

Strong Parameters: Use strong cryptographic parameters to resist computational attacks

1.6.3 Diffie-Hellman Key Exchange



References

- Cryptography - Diffie-Hellman Algorithm - Online Tutorials Library
- What is the Diffie–Hellman key exchange and how does it work?
- Executive Summary - D(HE)at Attack
- Frequently Asked Questions | D(HE)at Attack

Thank You!