# Information Security

Hitesh Dharmdasani

# Agenda

- Early days of Information Security
- Types of Encryption
- Government Interference in Encryption Strength
- Pros and Cons of securing data
- Usable Data Security

# Information Security

- We only care about access to data rather than transmission of data
- Most threats are Internal rather than External
- Data is Valuable
- Most Cyber crime is due to selling of data. Credit Cards. Passwords. etc…

# Early Days

Caesars Cipher

Vigenère cipher

“The system must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.”

– Kerckhoff

# The Key is the Important Part

- Mechanical encryptors
  (Vernam, Enigma, Hagelin, Scherbius)

- Mathematical cryptanalysis
  (Friedman, Rejewski et al, Bletchley Park)

- Machine-aided cryptanalysis
  (Friedman, Turing et al.)

- Most Encryption today is via Computing

- Encryption is our best answer in the Security World

# More about Encryption

- Encryption Algorithms are *HIGHLY* mathematical
- Don't invent your own crypto
- Brute forcing is a problem
- Need to make sure crypto systems are robust to people with significant resources (Governments)

1970

NIST calls for a Cipher

IBM Responds with DES

# Data Encryption Standard

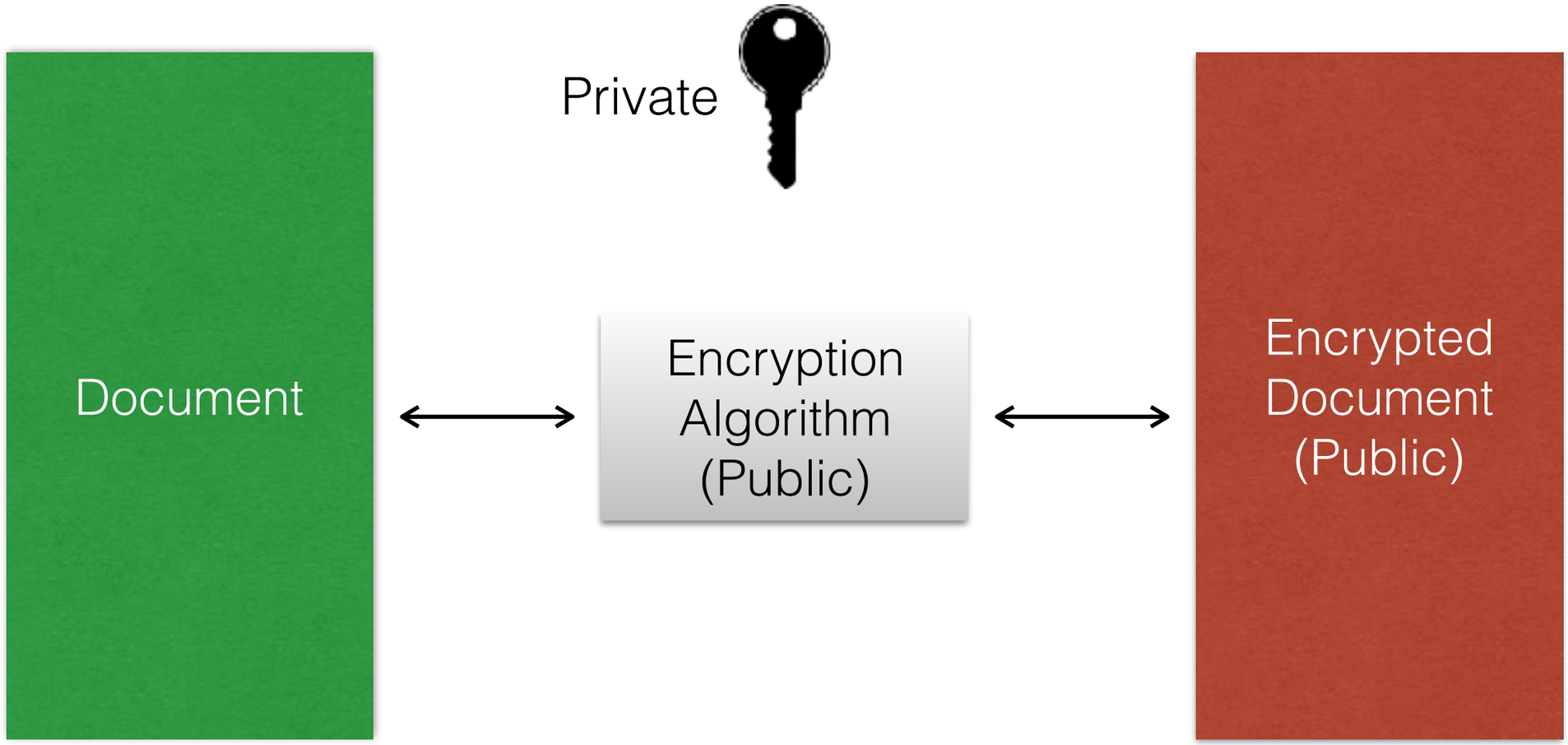
- Strongest Encryption of its time.
- In 1977, Diffie and Hellman proposed a machine costing an estimated US$20 million which could find a DES key in a single day
- In 1998 when a custom DES-cracker was built by the EFF, at the cost of approximately US$250,000
- AES supersedes DES and its the current standard

# PKI and RSA

Diffie, Hellman, Rivest, Shamir, and Adleman

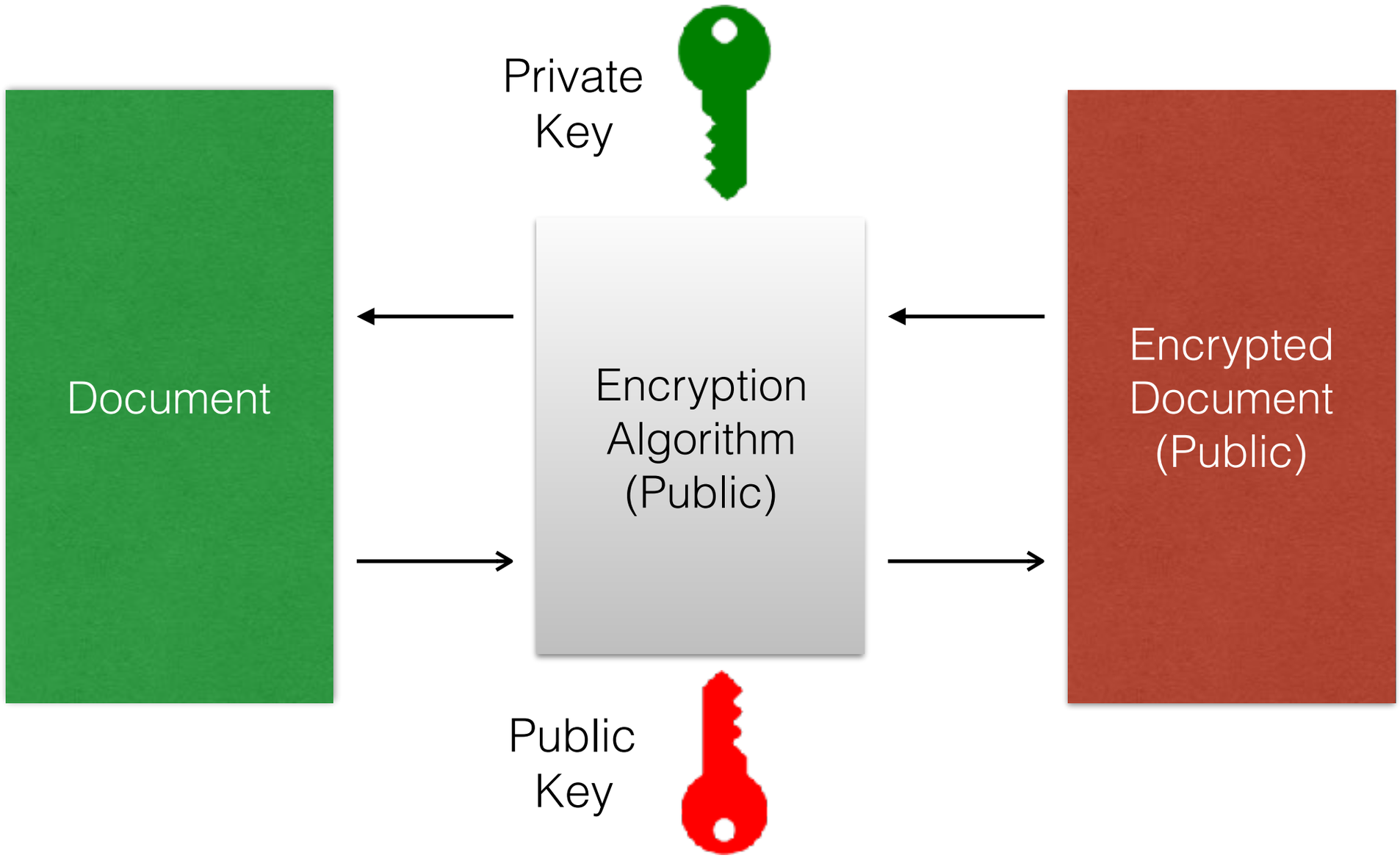
# SSL -> TLS

Taher Elgamal et. al.




# Symmetric Key

Pre Shared Key (Password)




# Asymmetric Key

# Government Survilleance

- Governments have been developing ways to break security for years
- Mostly for Law Enforcement. But trust issue prevails
- Apple vs. FBI
- Forced downgrade of security to be able to do surveillance
- The Principle of NOBUS

# Usable Security

- Make security transparent
- HTTPS, TKIP, DMARC, SPF, DNSSEC…
- Google Chrome Warning Pages
- Hard to achieve without intervention
- On-the-fly security?