Data Security

Most Secure Data is data you. Don't. Have!

Encryption:

A reversable process that obfuscat data

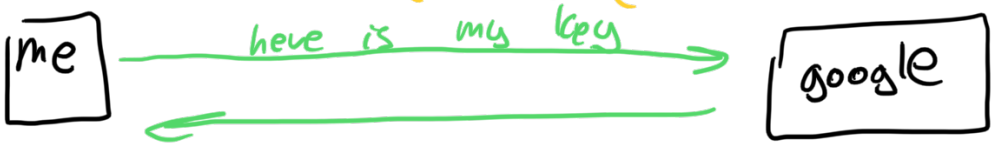
Securing Data in transit

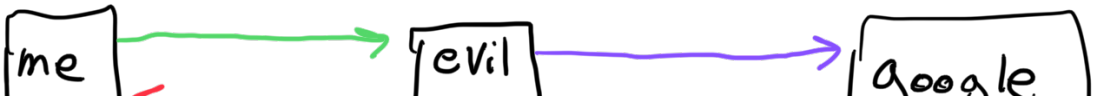
asymmetric encryption

"one key to lock, one key to unlock"

public

"man in the middle attack"





Digital Certificate:

physically verified certificate authori

they provide "root" certificates and

delegate / verify other security certifica

Securing data at Rest

Symmetric key encryption

"typical lock and key"

"same key encrypts and decrypts the data"

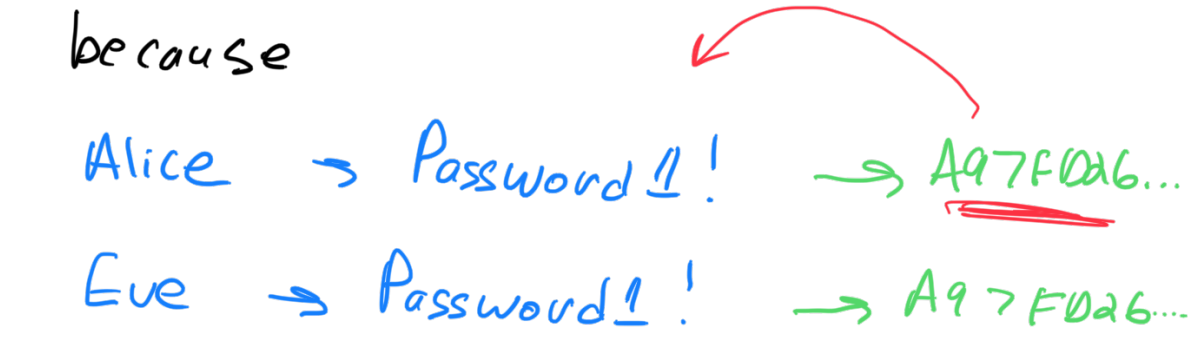
"Key rotation"

Hashing

"Proof of knowledge"

Passwords!

Hashing is a one way mathematical transformation, typically to a fixed size output



Salted hash

generate a random "salt" value for each user

Alice → "Password1!" + "B97654CD" → F952614

Eve → "Password1!" + "986F52" → B27952

---

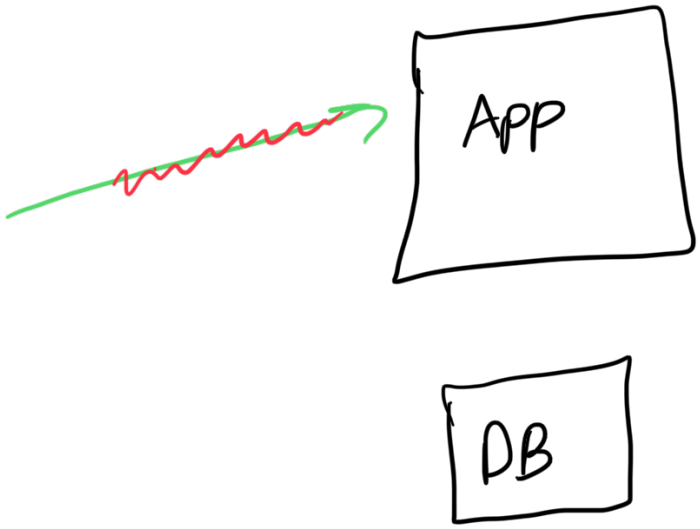
double hash

salt + hash client side

hash again on the server

Since

SQL Injection Attacks



Stopping SQL Injection:

1.) input validation ✗

2.) Limit database user privilodges ~

3.) use parameterized queries ✓