Presumption of Innocence

The burden of proof is thus on the prosecution, which has to convince the court that the accused is guilty beyond a reasonable doubt.

entropy - a measure of randomness

"ter qik broun foujumpies ouver da layz dorg"
"QikBrOUnFoX"

Virtual Private Network (VPN)

Virtual Private Network (VPN)

CA - Certificate Authority

PKI - Public Key Infrastructure

Public-key cryptography, aka asymmetric cryptography

In general, a PKI enables the parties in a dialogue to establish confidentiality, message integrity and user authentication without having to exchange any secret information in advance, or even any prior contact.

Thunderbird & Enigmail are Great!

Key Block = encryption key
Key ID = fingerprint = checksum

Web of Trust (WoT)

TrueCrypt

brute force

social engineering

keylogging

phishing

dumpster diving