Public Key Signing

Developing a web of trust for encrypting messages

Greg Gardner, Chris Sims

28 October 2013

What is Public Key Encryption?

PKE is asymetrical, meaning that the same message will never be encrypted the same way twice.

- Confidentiality: encipher using public key, decipher using private key
- Integrity/authentication: encipher using private key, decipher using public one
- Symmetric Key distribution
- It is computationally infeasible for an opponent knowing only the public key to determine the private key. It is computationally infeasible for an oponent knowing the public key and a ciphertext to recover the original message.

Public Key

a key that everyone can see

Private Key

Steps

1. generate key keypair
2. encrypt a message your recipient's public key.
3. decrypt a message using your private key

What is PKI?

An **infrastructure** of people, servers, policies, and procedures for the management of **certificates**.

- proves you aren't a phony
- many methods for certification

Certification

- Certificate Authorities
- Validation Authorities
- **Web of Trust**