

PIKKU-PINKKU

© P. Karanko

Julkisen avaimen salaus Public-key cryptography

English in this color, let's see how it works ü



Olen ihmetellyt miksi kryptografiassa julkista avainta sanotaan "avaimeksi"

I've been wondering why public key is called a 'key'.



Minusta julkinen lukko olisi kuvaavampi!

I think public lock would be more descriptive!

(The kind of lock you can close without a key.)

(Sellainen lukko, jonka voi naksauttaa kiinni ilman avainta)

Perusidea

(tai no, melkein, yleensä epäluotettava viestinviestä ei saa protokollan lopussa sinappia)

The Basic Idea

(...almost, usually the eavesdropper does not get mustard in the end of the protocol)

