Cryptography Basics

Basics of Cryptography

What is it?

- tranform information
- so only legitimate users can read it
- although transported in the open
- all by mathematical means

Encoding vs. Encryption

- Encoding is any transformation of an alphabet (eg. letters, numbers, pictures) into a binary code (eg. ASCII)

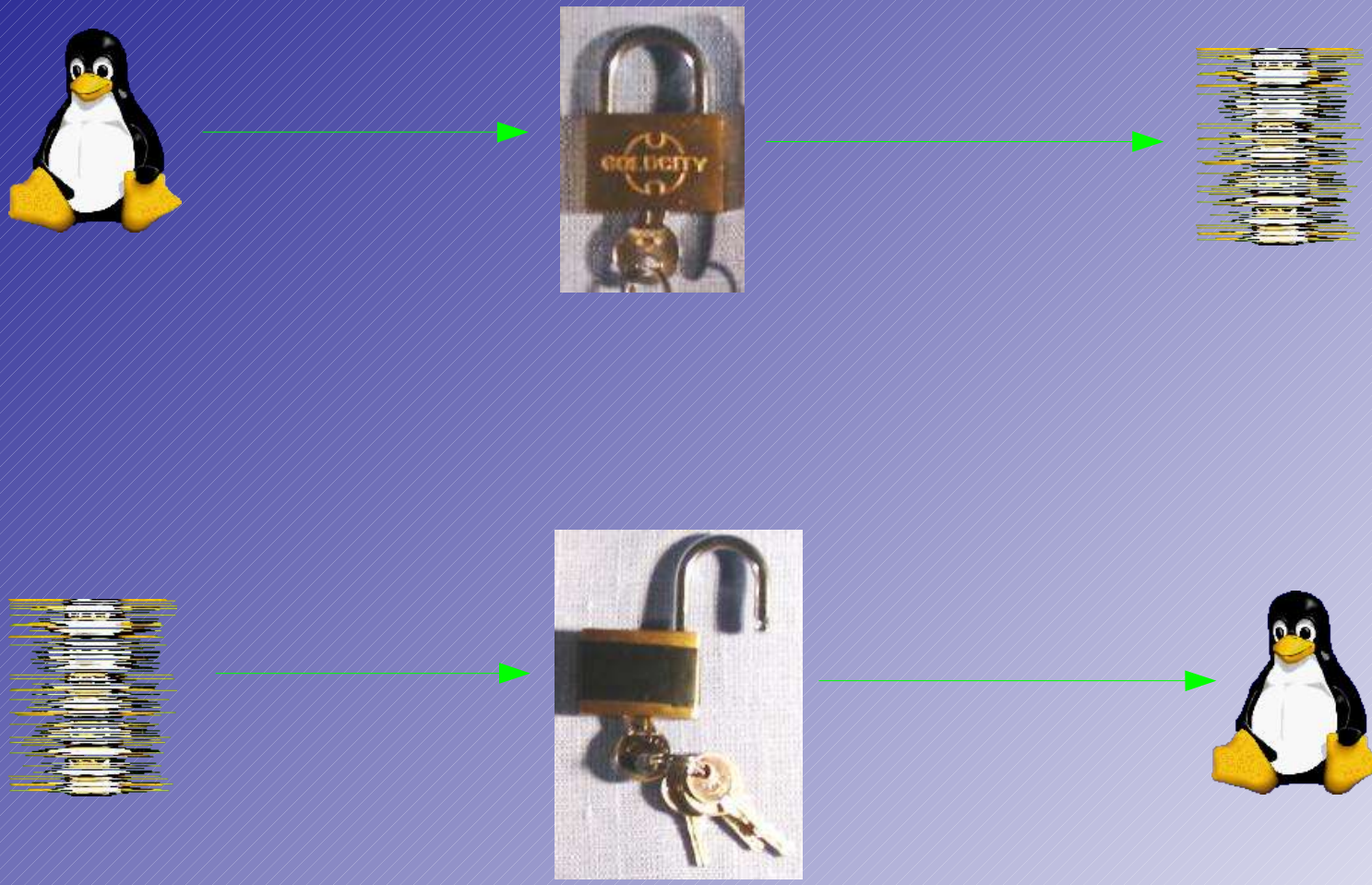
- Encryption is the transformation of readable binary data into unreadable binary data

Cryptanalysis

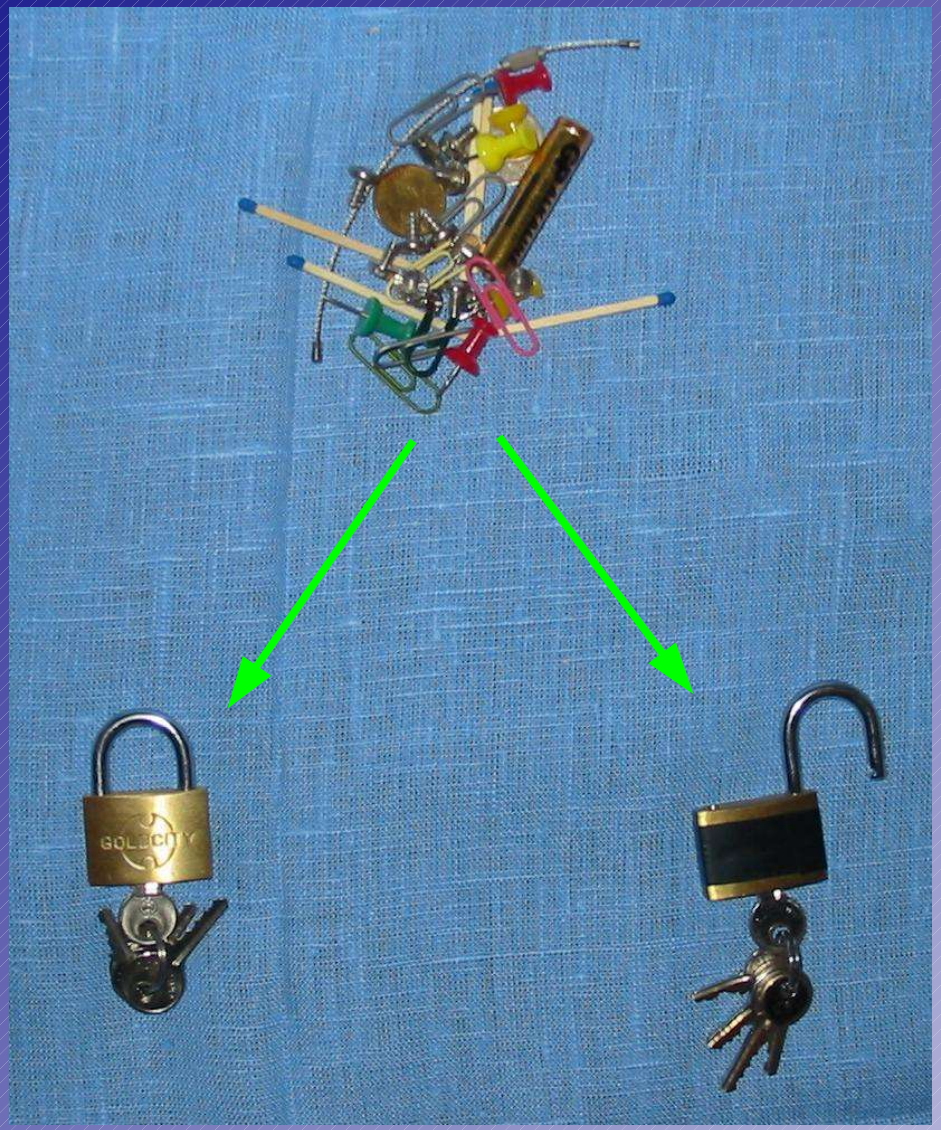
- Attack: try to crack an encryption
- Brute Force Attack: try ALL possible keys/variants to find a match
- Secure: any algorithm for which there is no better attack than “brute force”
- Cryptanalysis: trying to find better attacks with scientific methods
  - very important to analyse an algorithms strength

Symmetric Algorithms

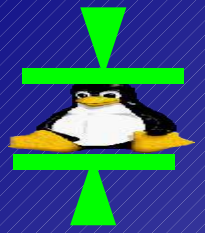
Asymmetric Algorithms



Key Generation



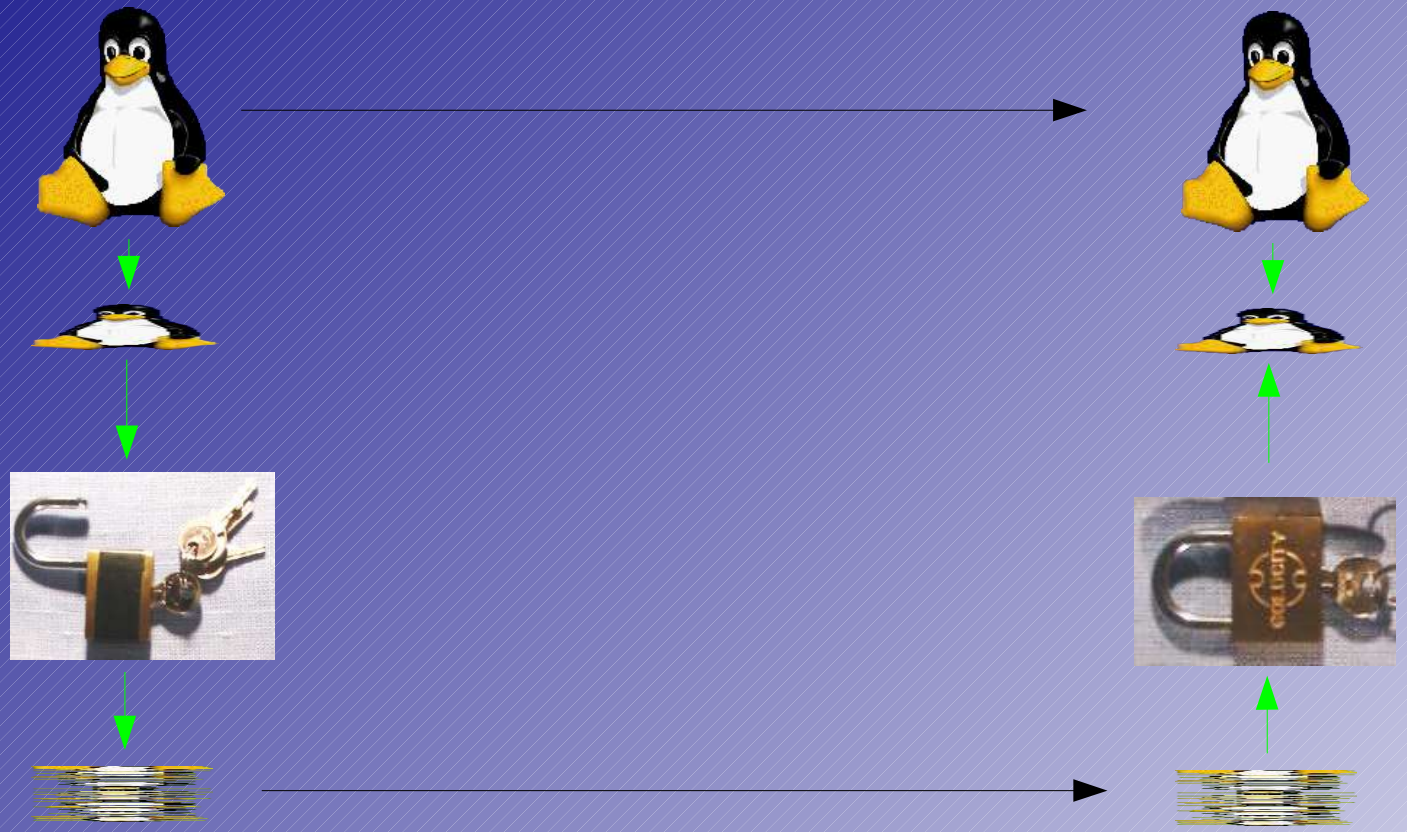
- Random data is transformed into two complementary keys
- transformation back is a hard to solve mathematical problem



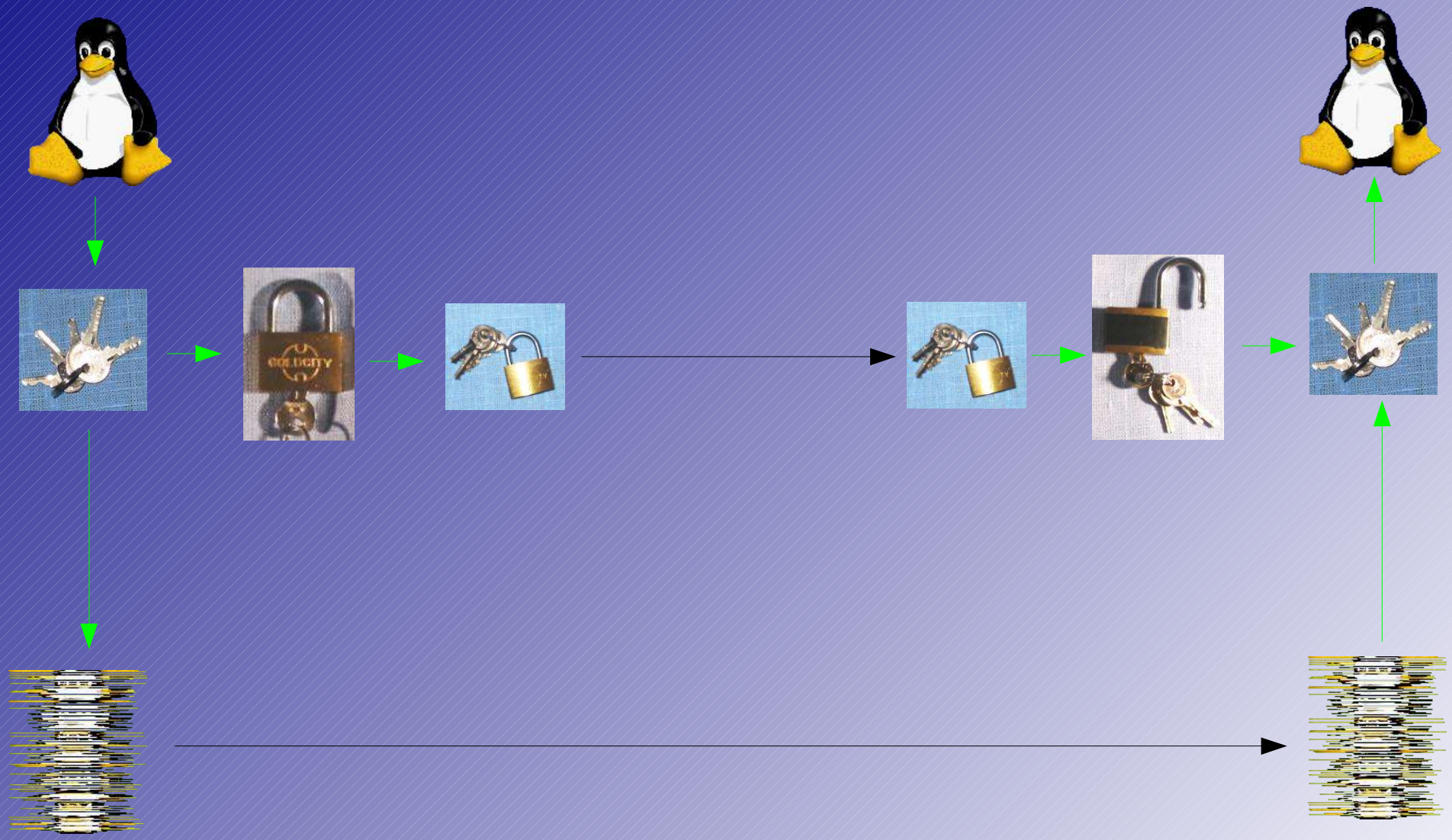
Message Digest

- Hash sum
  - comparatively small value (sum) mathematically derived from a bigger value (message)
  - a message has exactly one sum, but a sum can be derived from several different messages
- Message Digest
  - non-reversable hash sum

Signatures



Speedup



Questions?

?