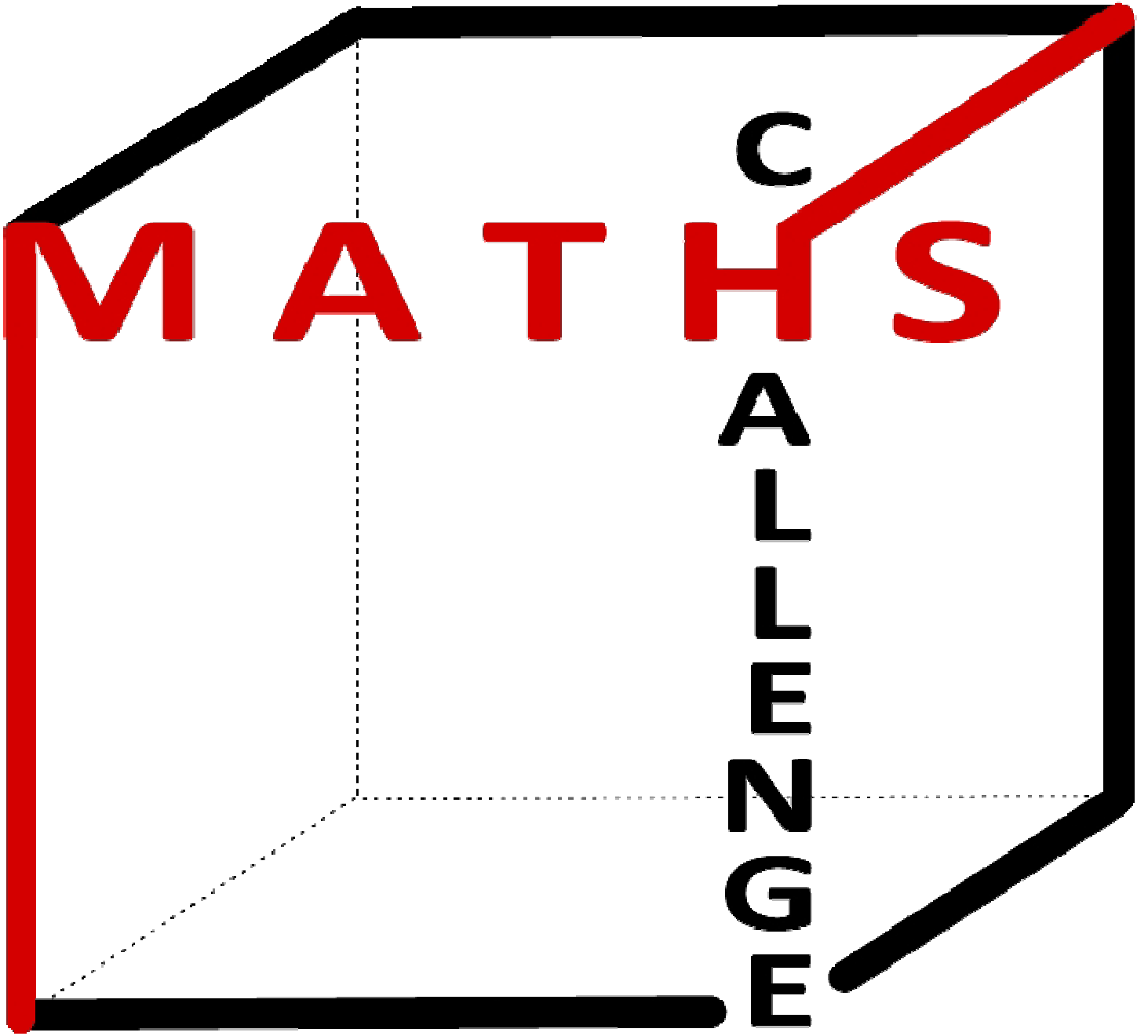

MATHS
CHALLENGE

20th January 2008
University College London

Welcome!

What will happen today?

Lecture

- bear with us, will start in a minute!

Tour around UCL

will give you a taste of an academic life.

Workshops:

try to use what you've learnt.

Cryptography

Better don’t get confused!

First things first

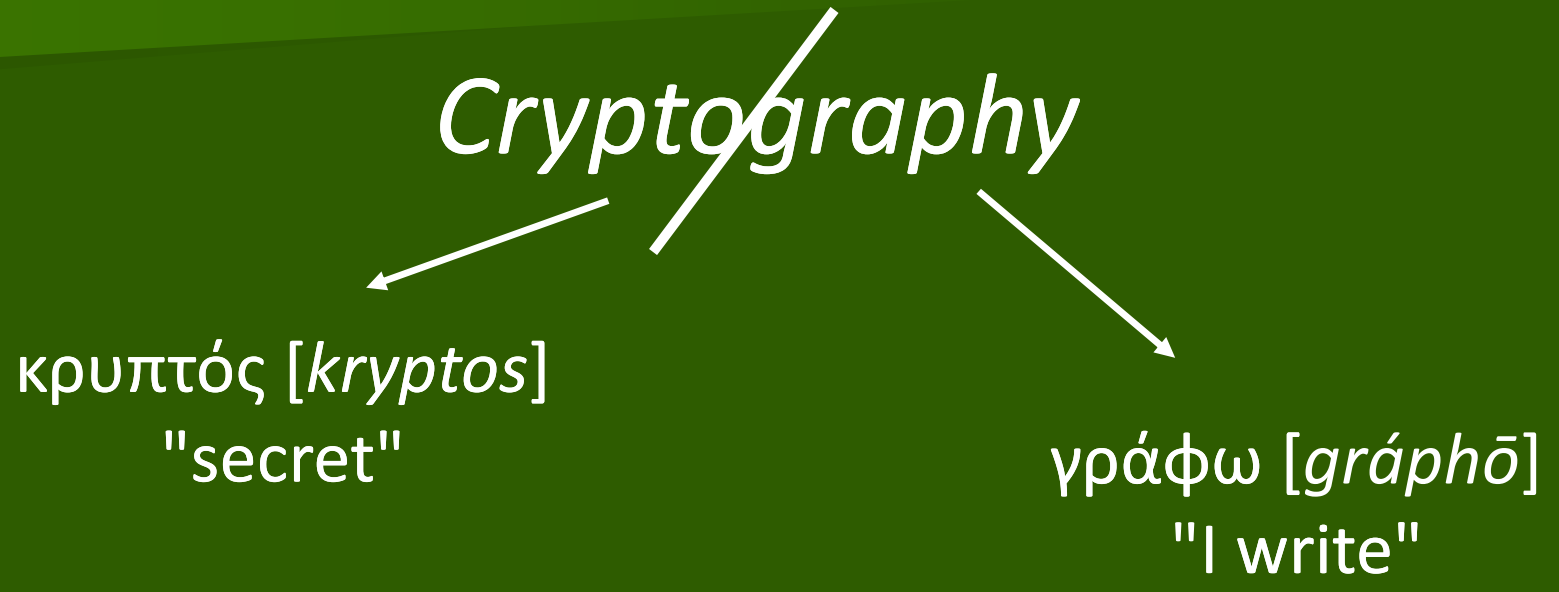
First things first

Cryptography

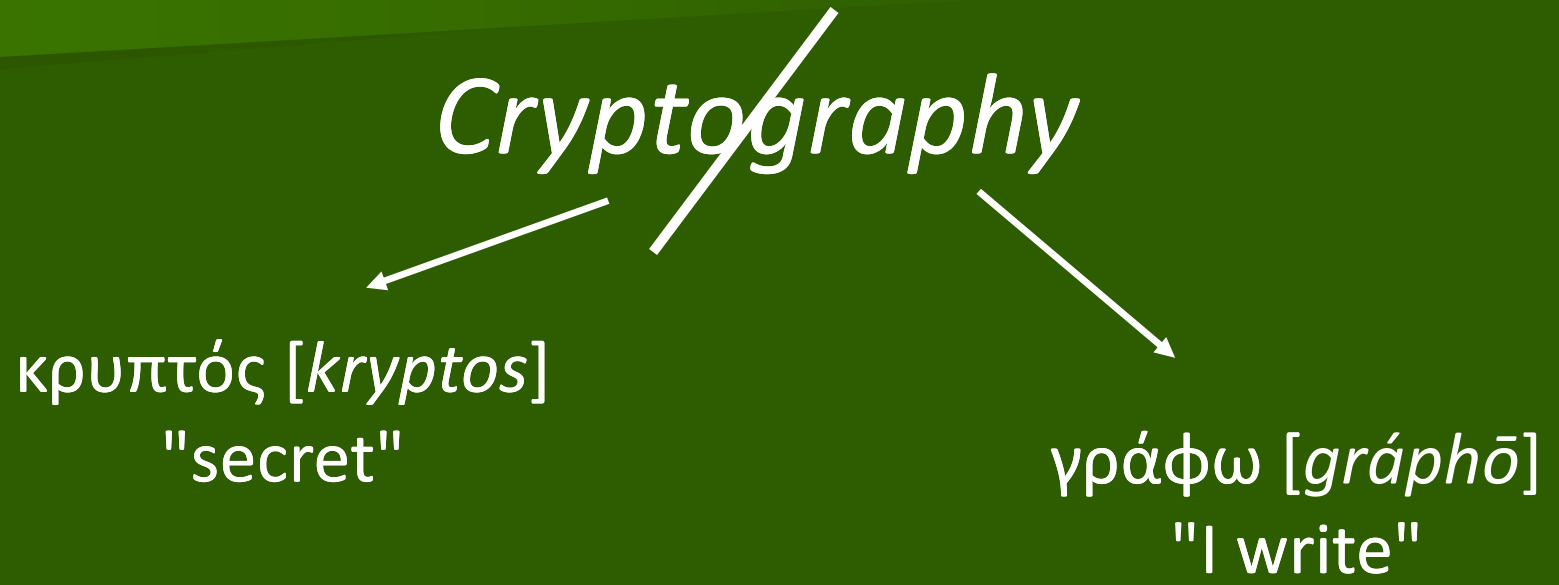
First things first

Cryptography

First things first

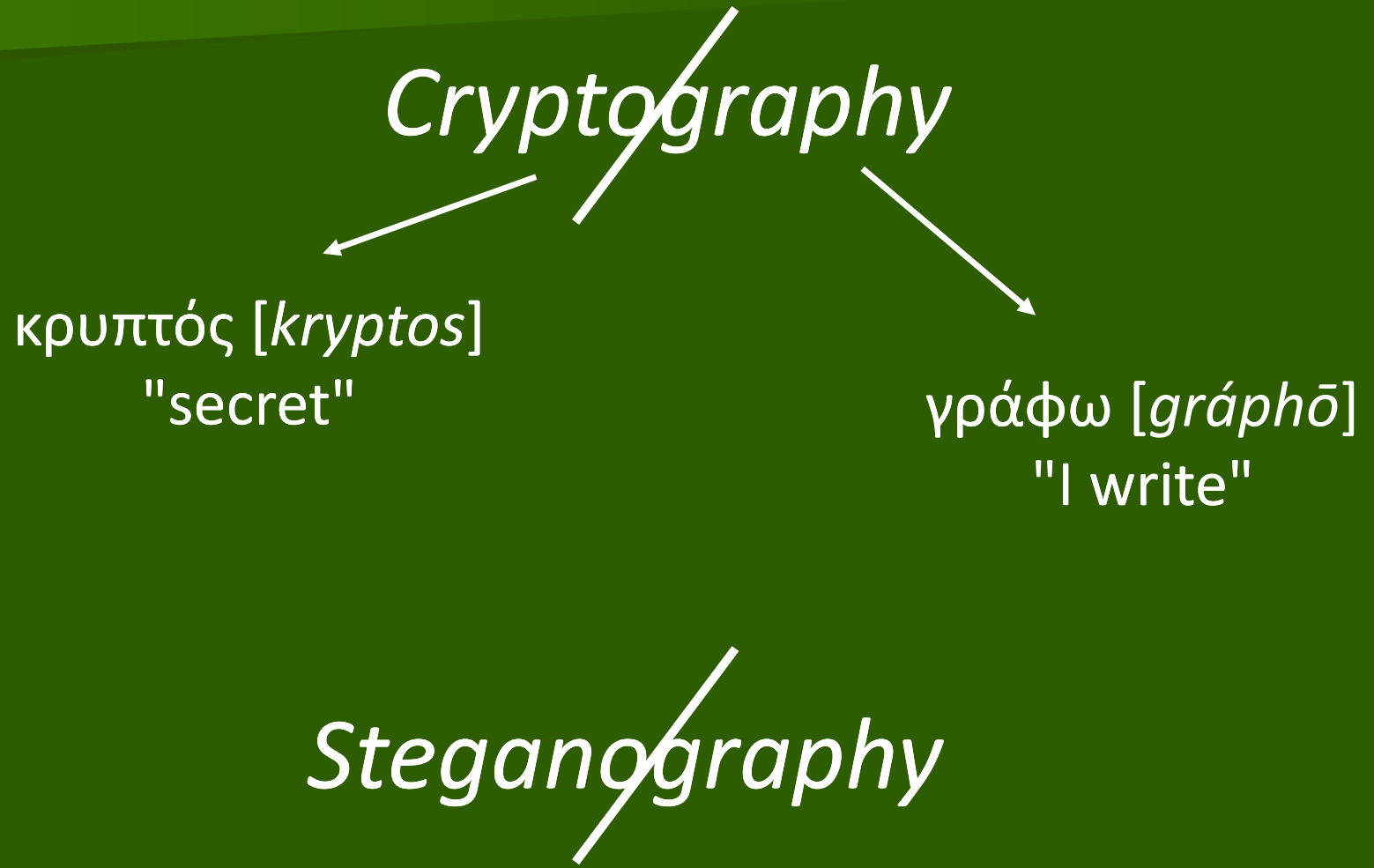


First things first

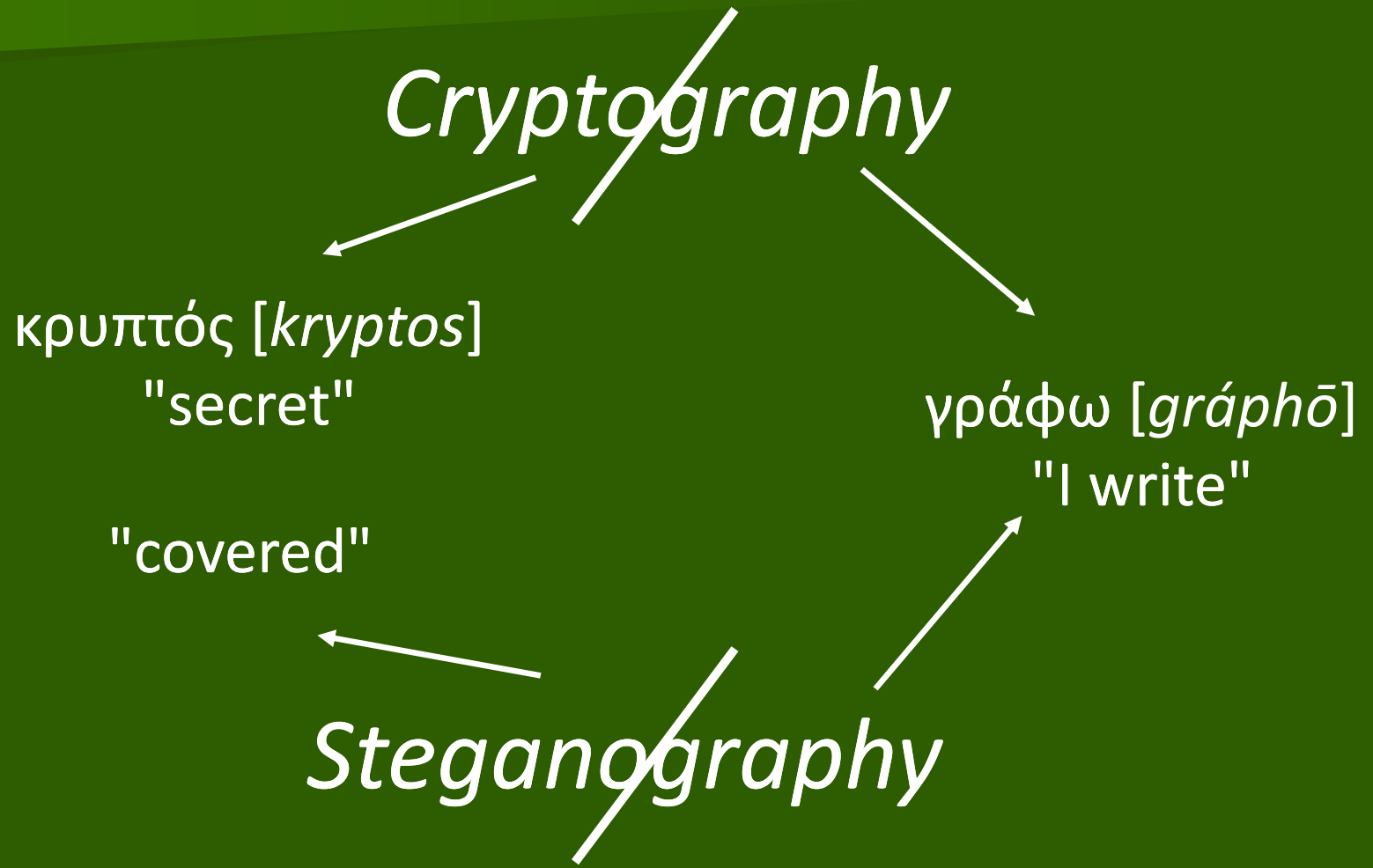


Steganography

First things first



First things first



Steganography - examples

Steganography - examples

http://www.mcbworld.com/mcbworld/gadget-c-3.html

Steganography - examples

http://www.mcbworld.com/mcbworld/gadget-c-3.html

http://lawngospel.wordpress.com/2008/10/12/the-redeemed-tattoo-if-were-gonna-ink-wed-better-think/

More about cryptography

More about cryptography

- ✓ CODE WORDS

More about cryptography

- ✓ CODE WORDS
  apple pie = prepare the attack
  mum’s favourite broom = enemies

More about cryptography

- ✓ CODE WORDS
- ✓ TRANSPOSITION CIPHER

More about cryptography

- ✓ CODE WORDS

- ✓ TRANSPOSITION CIPHER
  need a break = ende a rbaek

More about cryptography

- ✓ CODE WORDS
- ✓ TRANSPOSITION CIPHER
- ✓ SUBSTITUTION CIPHER

More about cryptography

- ✓ CODE WORDS

- ✓ TRANSPOSITION CIPHER

- ✓ SUBSTITUTION CIPHER
  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B…
  fly = ekx (1 place to the left)
  rainbow = udlqerz (3 places to the right)
  → Caesar cipher

More about cryptography

- ✓ CODE WORDS
- ✓ TRANSPOSITION CIPHER
- ✓ SUBSTITUTION CIPHER
- ✓ SYMBOLIC CIPHER

More about cryptography

- ✓ CODE WORDS
- ✓ TRANSPOSITION CIPHER
- ✓ SUBSTITUTION CIPHER
- ✓ SYMBOLIC CIPHER

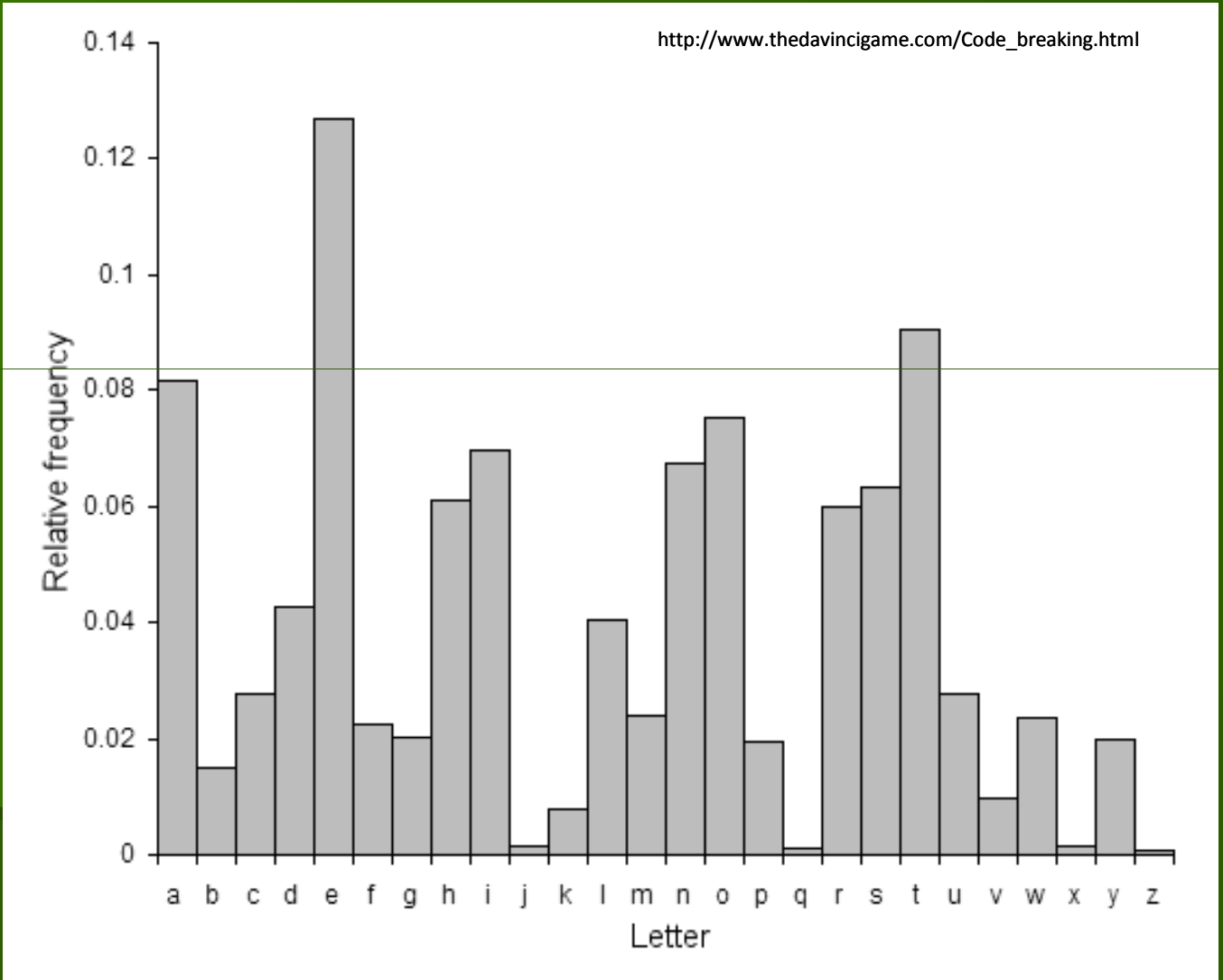
I am hungry = 

More about cryptography

- ✓ CODE WORDS
- ✓ TRANSPOSITION CIPHER
- ✓ SUBSTITUTION CIPHER
- ✓ SYMBOLIC CIPHER
- ✓ many more…

Right… but how to crack the code?

Right… but how to crack the code?



Kid-RSA

RSA creators: Ron Rivest,
Adi Shamir
Leonard Adleman

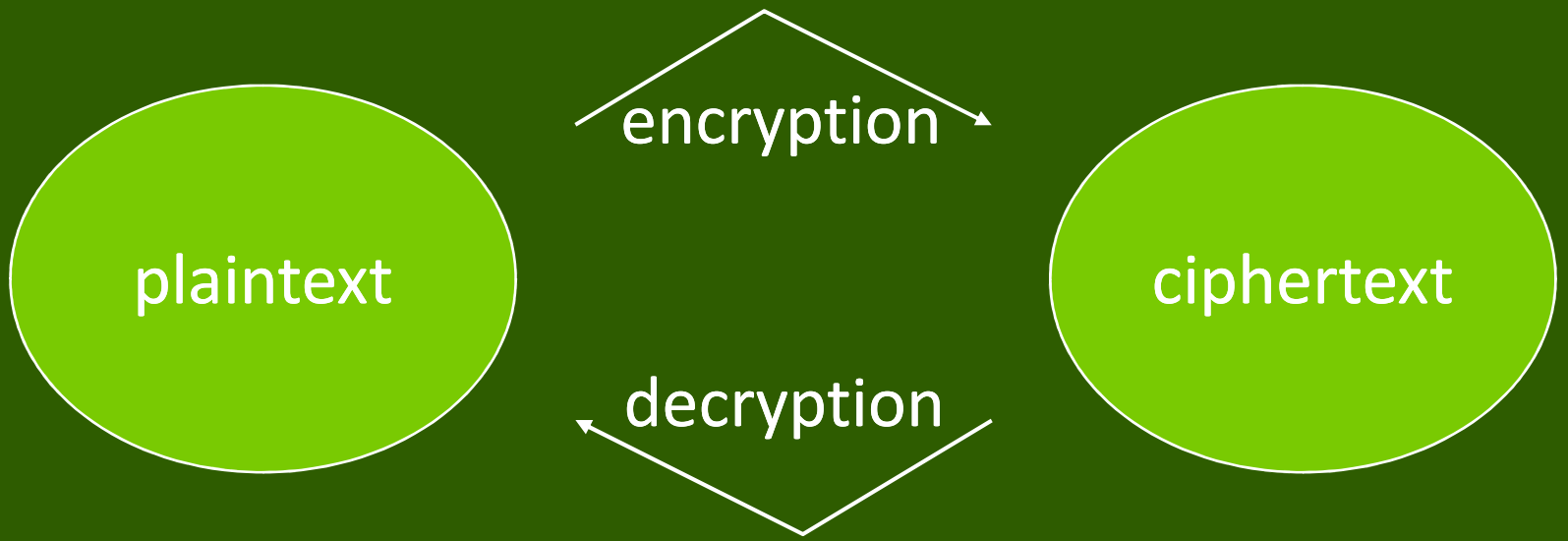
RSA was first described in 1977.

One of the two most popular ways of coding a message.

Kid-RSA: proposed by Neal Koblitz

Quick recap

- ✓ integer
- ✓ modulo
- ✓ public key and private key



Here it comes… !

Here it comes… !

Remember: letters are just symbols,
you can use pictures if you find it easier!

$$M = a * b - 1$$

is essentially the same as:

Bibliography

1. http://www.scribd.com/doc/2345053/Modular-Arithmetic-RSA-Encryption
2. http://www.math.washington.edu/~koblitz/crlogia.html
3. http://www.cs.uri.edu/cryptography/publickeykidkrypto.htm
4. http://www.mathaware.org/mam/06/Sauerberg_PKC-essay.html
5. http://axion.physics.ubc.ca/crypt.html#RSA
6. http://www.answers.com/RSA
7. http://www.mcld.co.uk/decipher/
8. http://www.exploratorium.edu/ronh/secret/secret.html
9. http://en.wikipedia.org/wiki/Cryptography
10. http://en.wikipedia.org/wiki/Steganography
11. http://en.wikipedia.org/wiki/Public_key