Two integers m, n are coprime if $\gcd(m, n) = 1$.

e.g. 3, 7 are coprime

4, 9 are coprime

6, 21 are not coprime

Defn We let $\phi(n)$ denote the number of integers in the range $1, 2, 3, \ldots, n$ that are coprime to n.

Example $\phi(8) = 4$

$\phi(6) = 2$

$\phi(107) = 106$

$\phi(19) = 18$

We call $\phi(n)$ Euler's Phi function or Euler's Totient function.

Proposition 1 If p is a prime number then

$$\phi(p) = p - 1.$$

$\phi(2^2) = 2 = 2^2 - 2^1$

$\phi(3^2) = 6 = 3^2 - 3^1$

$\phi(2^4) = 8 = 2^4 - 2^3$

Proposition 2 If p is prime then

$$\phi(p^n) = p^n - p^{n-1}$$

$\phi(3 \cdot 5) = \phi(15)$ 8

$\phi(3) = 2$

$\phi(5) = 4$

Proposition 3 If $\gcd(m,n) = 1$ then

$$\phi(m.n) = \phi(m)\,\phi(n)$$

Example

$$\phi(4.6) = \phi(24) = 8$$

$$\phi(4) = 2$$

$$\phi(6) = 2$$

Example

$$\phi(220) = \phi(2^2.5.11)$$

$$= \phi(2^2)\,\phi(5.11)$$

$$= \phi(2^2)\,\phi(5)\,\phi(11)$$

$$= 2.4.10$$

$$= 80$$

1 2 3 4 5 6 7 8 9

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

1 2 3 4 5 6 7 8 9 10 11 12

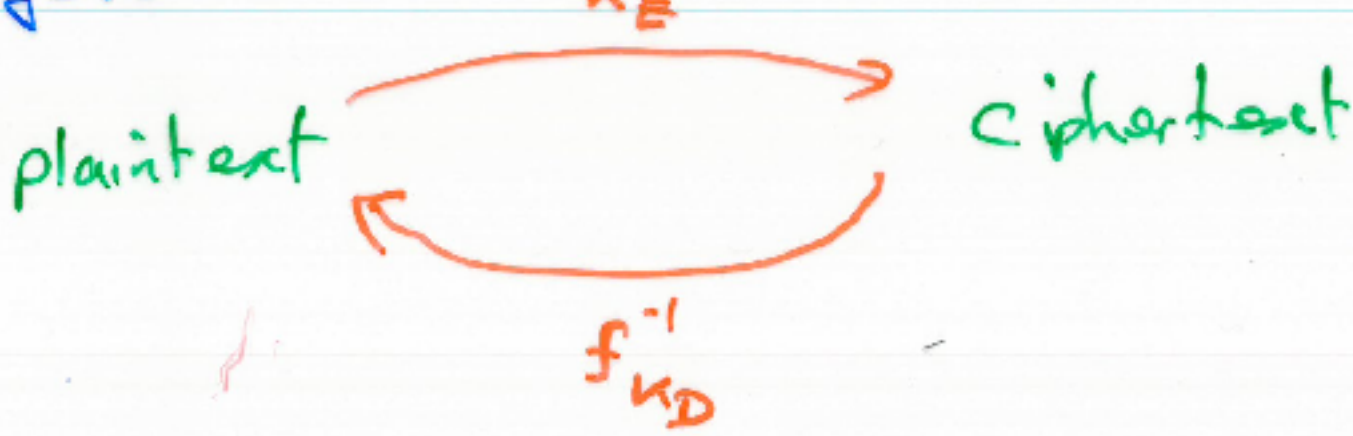
13 14 15 16 17 18 19 20 21 22 23 24

Public Key Cryptography

Defn (Diffie & Hellman 1976)
A public key cryptosystem is a cryptosystem with the property that someone who knows only the enciphering key can not (without a prohibitively length computation) discover how to decipher.

Affine cryptosystems are not public key.

Example We could use a public key cryptosystem as follows:



K_E = enciphering key (public)

K_D = deciphering key (secret).

I want to email my bank for €1000. The bank needs to verify that I really am Graham Ellis. To do this the bank chooses a secret word

RABBIT

The bank looks at my webpage and looks up my public enciphering key.

The bank emails me the text

$$f_{K_E}(\text{RABBIT})$$

I then have to tell the bank (by phone or email) that their secret word is

$$f_{K_D}^{-1}\left(f_{K_E}(\text{RABBIT})\right)$$

$$= \text{RABBIT}.$$

Only Graham Ellis knows how to do this, as only he knows K_D.