

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  $1, 2, 3, \dots, n$  that are coprime to  $n$ .

Example  $\phi(8) = 4$

① 2 ③ 4 ⑤ 6 ⑦ 8

$\phi(6) = 2$

① 2 3 4 ⑤ 6

$\phi(107) = 106$

$\phi(19) = 18$

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

Proposition 1 If  $p$  is a prime number then

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

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

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

① ② 3 ④ ⑤ 6 ⑦ ⑧ 9

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

① 2 ③ 4 ⑤ 6 ⑦ 8 ⑨ 10 ⑪ 12 ⑬  
14 ⑮ 16

Proposition 2 If  $p$  is prime then

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

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

① ② 3 ④ 5 6 ⑦ ⑧ 9 10 ⑪ 12  
⑬ ⑭ 15

$$\phi(3) = 2$$

$$\phi(5) = 4$$

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

$$\phi(m \cdot n) = \phi(m) \phi(n)$$

Example

$$\phi(4 \cdot 6) = \phi(24) = 8$$

① 2 3 4 ⑤ 6 ⑦ 8 9 10 ⑪ 12  
⑬ 14 15 16 ⑰ 18 ⑲ 20 21 22  
⑳ 24

$$\phi(4) = 2$$

$$\phi(6) = 2$$

Example

$$\begin{aligned}\phi(220) &= \phi(2^2 \cdot 5 \cdot 11) \\ &= \phi(2^2) \phi(5) \phi(11) \\ &= (2^2 - 2) \cdot 4 \cdot 10 \\ &= 80\end{aligned}$$

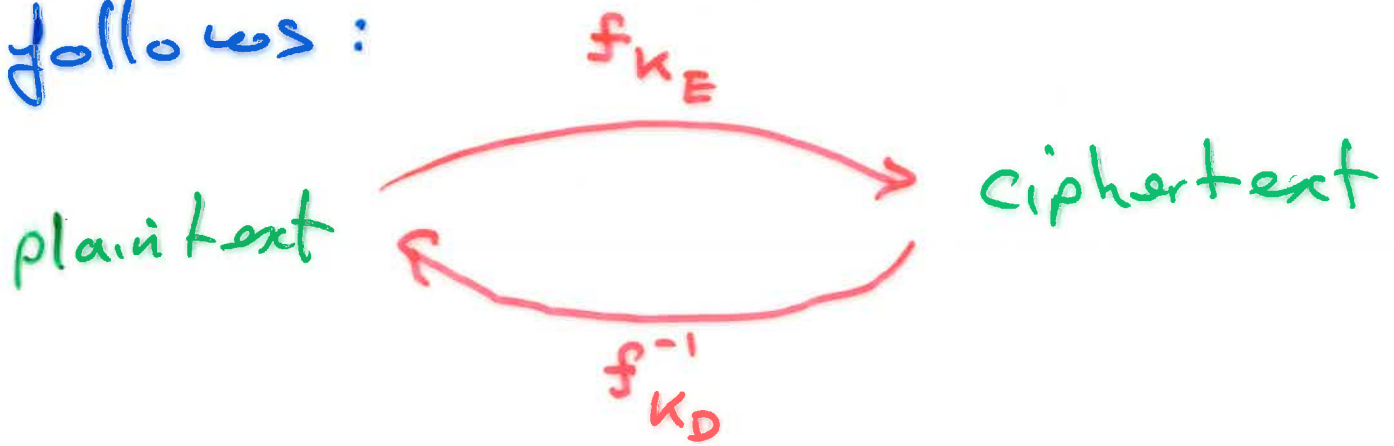
# Public Key Cryptography

Data (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 lengthy 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

HAIRY

The bank looks at my  
web page and looks up  
my public encipher key.  
The bank emails me  
the text

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

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

$$f_{K_D}^{-1}(f_{K_E}(\text{HAIRY})) \\ = \text{HAIRY}.$$

Only Graham Elks can do  
this, as only he knows  
the decyphering key  $K_D$ .