

# Towards Public Key Cryptography

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

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  $\phi(8) = 4$

$$\phi(6) = 2$$

$$\phi(107) = 106$$

$$\phi(19) = 18$$

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

① 2 ③ 4 ⑤ 6 ⑦ 8

$$\phi(8) = 4$$

① 2 3 4 ⑤ 6

$$\phi(6) = 2$$

① ② 3 ④ ⑤ 6 ⑦ ⑧ 9

$$\phi(9) = 6$$

① ② 3 ④ 5 6 ⑦ ⑧ 9 10

$$\phi(15) = 8$$

⑪ 12 ⑬ ⑭ 15

① 2 3 4 ⑤ 6 ⑦ 8 9 10 ⑪ 12

$$\phi(12) = 4$$

⑬ 14 15 16 ⑰ 18 ⑱ 20 21

22 ⑳ 24

$$\phi(24) = 8$$

$$\phi(3 \cdot 3) = \phi(9) = 6$$

$$\phi(9) = 6$$

$$\phi(3) = 2 \quad 2 \cdot 2 \neq 6$$

$$\phi(3) = 2$$



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

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

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

$$\phi(3) = 2$$

$$\phi(5) = 4$$

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

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

Example

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

$$\phi(4) = 2$$

$$\phi(6) = 2$$

Example

$$\phi(220) = \phi(2^2 \cdot 5 \cdot 11)$$

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

$$= (2^2 - 2^1) (5 - 1) (11 - 1)$$

$$= 2 \cdot 4 \cdot 10$$

$$= 80$$



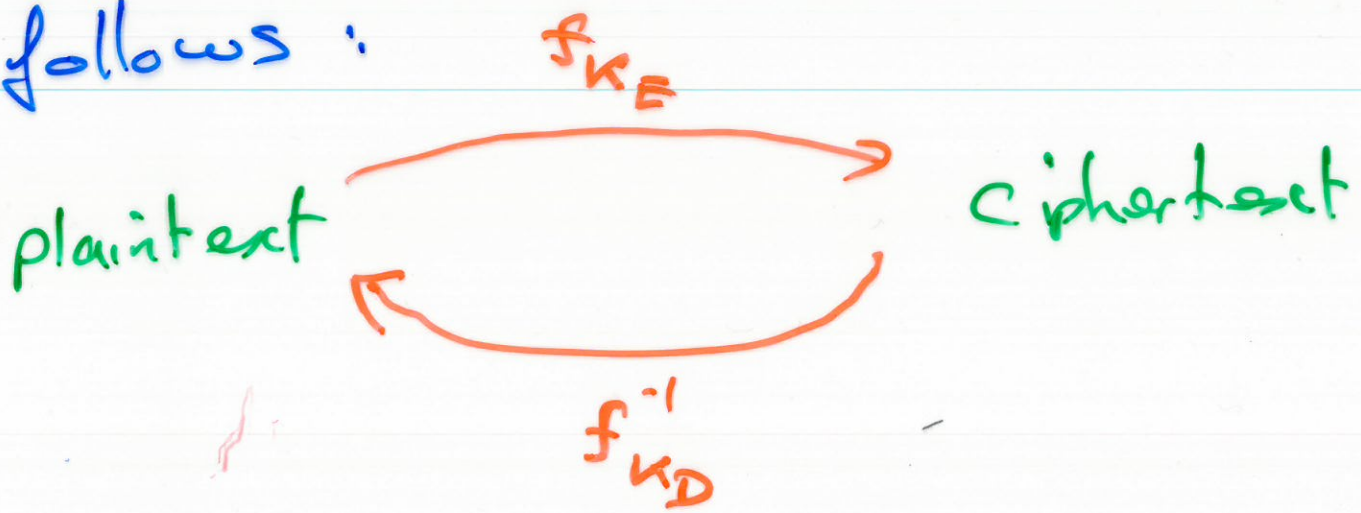
# Public Key Cryptography

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 lengthy" computation) discover how to decipher.

At times 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 encyphering key.

The bank emails me  
the test

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

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

$$f_{k_D}^{-1}(f_{k_E}(\text{RABBIT}))$$

$$= \text{RABBIT.}$$

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