Towards public key cryptography

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

e.g.
6 and 25 are coprime because
$\gcd(6,25) = 1$.

6 is not coprime to 21
because $\gcd(6,21) \neq 1$

Defn We let

$$\phi(n)$$

denote the number of integers in the range $1, 2, 3, \ldots, n$ which are coprime to n.

Examples

$\phi(6) = 2$ (1, 2, 3, 4, 5, 6)

$\phi(103) = 102$

$\phi(7) = 6$ (1 2 3 4 5 6 7)

$\phi(19) = 18$

Proposition if p is a prime number then

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

$\phi(2^2) = 2$

$\phi(3^2) = 6$ (1 2 3 4 5 6 7 8 9)

$\phi(2^4) = 8$

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

$\phi(3^4) =$

Proposition If p is prime then

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

check:

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

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

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

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

$$= 3^3(3-1) = 54$$

$\phi(3.5) = \phi(15) = 8$

$\phi(3).\phi(5) = 2.4 = 8$

1 2 ~~3~~ 4 ~~5~~ ~~6~~ 7 8 ~~9~~ ~~10~~

11 ~~12~~ 13 14 ~~15~~

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

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

Example

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

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

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

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

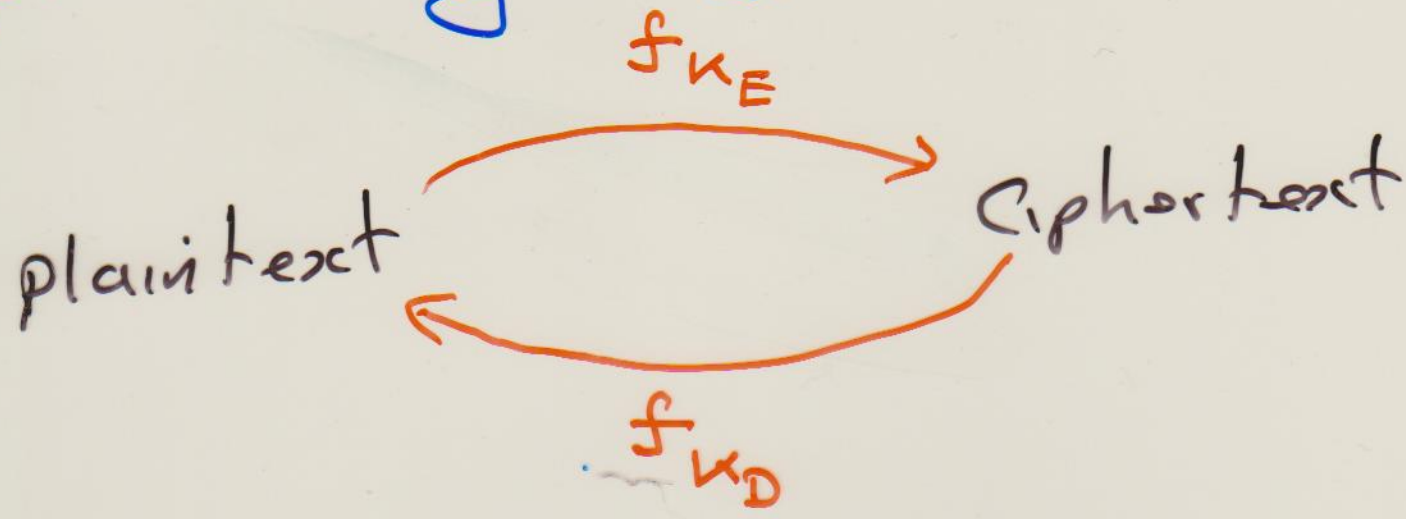
$$= 2.4.10 = 80$$

Public key Cryptography

Defn (Diffie & Hellman, 1976)

A public key cryptosystem is one with the property that a knowledge of the enciphering key does not "easily" lead to a knowledge of the deciphering key.

Example use of a public key cryptosystem



K_E = enciphering key

K_D = deciphering key

Suppose I e-mail my Swiss bank for €10 000. They need to verify that I really am Graham Ellis.

They choose a secret word

ABRACADABRA

From my web page they find my public key f_{K_E}.

They send me

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

I now tell the bank the secret word

$$f_{K_D}\left(f_{K_E}(\text{ABRACADABRA})\right)$$

$$= \text{ABRACADABRA}$$

Only Graham Ellis could know the secret word.