Lecture 5

Towards public key cryptography

Two integers m, n are **coprime** if their $\gcd(m, n)$ equals 1.

e.g. 6 and 25 are coprime

6 and 21 are not coprime

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~~

$\phi(103) = 102$

$\phi(13) = 12$

$\phi(19) = 18$

Proposition If p is a prime then $\phi(p) = p-1$.

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

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

$\phi(2^4) = 8 = 2^4 - 2^3$ 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Proposition If p is a prime then

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

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

$\phi(3) = 2 \quad \phi(5) = 4$

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

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

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

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

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

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

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

$$= 80$$

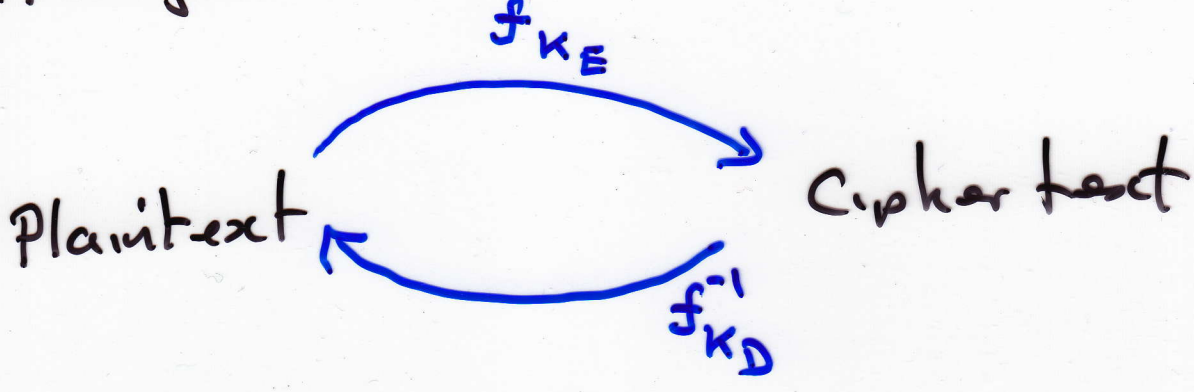
Public key Cryptography

Definition (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 matrix cryptosystems are <u>not</u> public key.

<u>Example</u> use of a public key cryptosystem:



K_E = enciphering key

K_D = deciphering key.

Suppose I e-mail my Swiss bank for €1000. They need to verify that I am Graham Ellis. So they choose some secret word

abracadabra

from my web page they find my public key K_E and send me

f_{K_E}(abracadabra)

I then tell the bank that the secret word is

$f^{-1}_{K_D}(f_{K_E}$(abracadabra))

= abracadabra

Since Graham Ellis is the only person who knows K_D this confirms my identity.