Signature

"Hi, its me"

$\downarrow$ ← only I know this transformatin

D_k[signature].

send this message to my bank, embassy, etc.

Bank, ~~eng~~ Embassy encrypt D_k[signature] → signature ← everyone knows this transformation

$\downarrow$

Bank, Embassy knows that it is communicating with "me"

M = "we have wired you the funds"

$\uparrow D_k[E_k[M]]$

I receive message

this, message can be intercepted but not decrypted

$E_k[M] \leftarrow$

Bank, or Embassy

Encrypts

M= "we have wired you the funds"

THE EUCLIDEAN ALGORITHM

Given:

$$\begin{cases} A = 657 \\ B = 963 \end{cases}$$

$d = (A,B)$

g. c. d. of A & B

$$963 = \underbrace{657}_{=9\cdot 73} \times 1 + 306 \quad (963 = 9\cdot 107)$$

$$657 = 306 \times 2 + 45$$

$$306 = 45 \times 6 + 36$$

$$45 = 36 \times 1 + 9$$

this is our gcd of 963 & 657

$$36 = 9 \times 4$$

so $\exists\, x, y \in \mathbb{Z}$ st. $x\,963 + y \cdot 657 = 9$

$$9 = 45 - 36 = 45 - (306 - 45 \times 6)$$

$$= -306 + 7 \times 45$$

$$= -306 + 7(657 - 306 \times 2)$$

$$= 7 \times 657 - 15 \times 306$$

$$= 7 \times 657 - 15(963 - 657)$$

$$= 22 \times 657 - 15 \times 963$$

$$\boxed{9 = 22 \times 657 - 15 \times 963}$$

$$d = h\,A + k\,B$$

Say that

$\gcd(a, n) = 1$

$\Rightarrow$ Euclidean algorgithm gives

$h \cdot a + k \cdot n = 1$

$ha - 1 = -kn$

OR $ha \equiv 1 \pmod{n}$

h is the inverse of a mod n

$x \equiv y \pmod{n}$

means $x - y$ is divisible by n

For example, with $N = 32423333$,

$$25924917 \quad (2^{12321} \bmod N) = (2 \cdot (2^{12320} \bmod N) \bmod N)$$

$$29174125 = (2^{12320} \bmod N) = ((2^{6160} \bmod N)^2 \bmod N)$$

$$17501302 \quad (2^{6160} \bmod N) = ((2^{3080} \bmod N)^2 \bmod N)$$

$$4580275 = (2^{3080} \bmod N) = ((2^{1540} \bmod N)^2 \bmod N)$$

$$1466817 = (2^{1540} \bmod N) = ((2^{770} \bmod N)^2 \bmod N)$$

$$11868474 = (2^{770} \bmod N) = ((2^{385} \bmod N)^2 \bmod N)$$

$$24128245 = (2^{385} \bmod N) = (2 \cdot (2^{384} \bmod N) \bmod N)$$

$$28273789 = (2^{384} \bmod N) = ((2^{192} \bmod N)^2 \bmod N)$$

$$24008612 = (2^{192} \bmod N) = ((2^{96} \bmod N)^2 \bmod N)$$

$$25784918 = (2^{96} \bmod N) = ((2^{48} \bmod N)^2 \bmod N)$$

$$14374405 = (2^{48} \bmod N) = ((2^{24} \bmod N)^2 \bmod N)$$

$$16777216 = (2^{24} \bmod N) = ((2^{12} \bmod N)^2 \bmod N)$$

$$4096 = (2^{12} \bmod N) = ((2^{6} \bmod N)^2 \bmod N)$$

$$64 = (2^{6} \bmod N) = ((2^{3} \bmod N)^2 \bmod N)$$

$$8 = (2^{3} \bmod N) = (2 \cdot (2^{2} \bmod N) \bmod N)$$

There is a function called the Euler 'phi' function

$$\phi(n) = \# \text{ of integers relatively prime (i.e. } gcd(k,n)=1\text{)}$$
$$\text{and are between 1 and } n$$

n	integers between 1 and n which are relatively prime	$\phi(n)$
1	1	1
2	1	1
3	1,2	$2 = 3\cdot(1-\frac{1}{3}) = 3-1$
4	1,3	2
5	1,2,3,4	$4 = 5(1-\frac{1}{5}) = 5-1$
6	1,5	2
7	1,2,3,4,5,6	$6 = 7(1-\frac{1}{7}) = 7-1$
8	1,3,5,7	$4 = 2^3(1-\frac{1}{2}) = 2^3-2^2$
9	1,2,4,5,7,8	$6 = 3\cdot 3(1-\frac{1}{3}) = (3^2-3)$
10	1,3,7,9	$4 = 10\cdot(1-\frac{1}{2})(1-\frac{1}{5}) = (2-1)\cdot(5-1)$
11	1,2,3,4,5,6,7,8,9,10	$10 = 11\cdot(1-\frac{1}{11}) = 11-1$
12	1,5,7,11	4
14	1,3,5,9,11,13	6
16	1,3,5,7,9,11,13,15	$8 = 2^4-2^3$
25	1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24	$20 = 5^2-5$

$\phi(p) = p-1$ if p is prime

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

$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$

$\phi(n) = (p_1^{n_1} - p_1^{n_1-1})(p_2^{n_2} - p_2^{n_2-1}) \cdots (p_k^{n_k} - p_k^{n_k-1})$

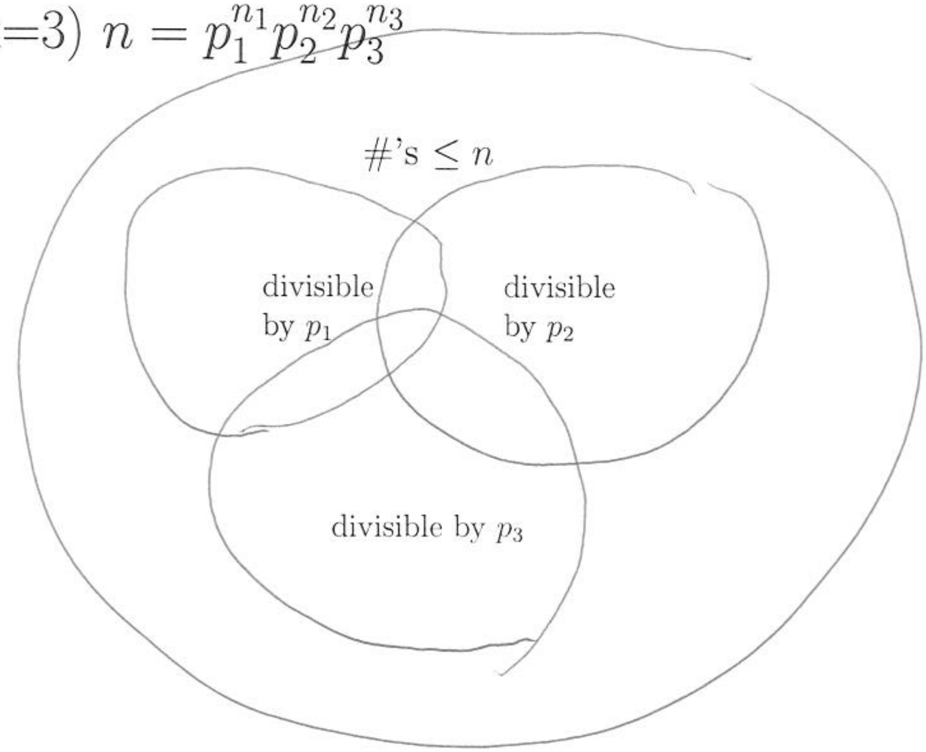
Euler ϕ-function

Definition. Let $\phi(n)$ denote the number of integers between 1 and $n-1$ that are relatively prime to n.

Theorem 1 *If* $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ *then*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Proof. (k=3) $n = p_1^{n_1} p_2^{n_2} p_3^{n_3}$



$$\begin{aligned}
\phi(n) &= n - \frac{n}{p_1} - \frac{n}{p_2} - \frac{n}{p_3} + \frac{n}{p_1p_2} + \frac{n}{p_1p_3} + \frac{n}{p_2p_3} - \frac{n}{p_1p_2p_3} \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) \\
&= \left(p_1^{n_1} - p_1^{n_1-1}\right)\left(p_2^{n_2} - p_2^{n_2-1}\right)\left(p_3^{n_3} - p_3^{n_3-1}\right)
\end{aligned}$$