CRYPTOLOGY

In this section we discuss two so-called public key ciphers, which are based on the difficulties of factorizing integers and the finding of discrete logarithms. We first need to introduce a few number theorical concepts and results.

Let m and a be integers with $0 < a < m$. Recall that there exist unique integers q and r with $0 \leq r < a$ such that $m = aq + r$.

Proposition 1

If $m = aq + r$, then $\gcd(m,a) = \gcd(a,r)$.

Proof: If d divides m and a, then d divides $m - aq = r$. Conversely, if d divides a and r, then d divides $aq + r = m$. ∎

Repeated application of this result provides a method for calculating $\gcd(m,a)$ — this method is known as the Euclidean algorithm.

An example illustrating the Euclidean algorithm

Determine $\gcd(2406, 654)$, using Proposition 1 repeatedly:

$$2406 = 654 \times 3 + 444 \quad \therefore \gcd(2406, 654) = \gcd(654, 444)$$
$$654 = 444 \times 1 + 210 \quad = \gcd(444, 210)$$
$$444 = 210 \times 2 + 24 \quad = \gcd(210, 24)$$
$$210 = 24 \times 8 + 18 \quad = \gcd(24, 18)$$
$$24 = 18 \times 1 + 6 \quad = \gcd(18, 6)$$
$$18 = 6 \times 3 + 0 \quad = 6$$

In general, if m and a are integers with $0 < a < m$, then we can find $\gcd(m, a)$ by recursively defining q_i and r_i by

$$m = aq_1 + r_1 \quad \text{with } 0 \leq r_1 < a$$
$$a = r_1 q_2 + r_2 \quad \text{with } 0 \leq r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3 \quad \text{with } 0 \leq r_3 < r_2$$
$$\vdots$$
$$r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} \quad \text{with } 0 \leq r_{k-1} < r_{k-2}$$
$$r_{k-2} = r_{k-1} q_k + r_k \quad \text{with } r_k = 0.$$

Since $r_k = 0$, $\gcd(m, a) = r_{k-1}$.

From the calculations above that were used to determine gcd(2406, 654), we have the following — working backwards from the second last equation to the first:

$$6 = 24 - 18 \times 1 \qquad = (1)24 + (-1)18$$

$$= 24 - (210 - 24 \times 8) \qquad = (-1)210 + (9)24$$

$$= -210 + 9(444 - 210 \times 2) \qquad = (9)444 + (-19)210$$

$$= 9 \times 444 - 19(654 - 444 \times 1) \qquad = (-19)654 + (28)444$$

$$= -19 \times 654 + 28(2406 - 654 \times 3) \qquad = (28)2406 + (-103)654$$

In general, without further proof, we state that...

Proposition 2

If m and a are integers with $0 < a < m$ and $d = \gcd(m, a)$, then there are integers c and k such that $d = cm + ka$.

Definition Integers m and a are relatively prime if $\gcd(m, a) = 1$.