The RSA-Method

Description: 1) Each user A has a public key (n_A, e_A) which is kept in a public directory. These numbers have the form

$$n_A = p \cdot q, \quad \text{where } p \neq q \text{ are large primes}$$

$$1 < e_A < n_A, \ \gcd(e_A, (p-1)(q-1)) = 1.$$

2) Each user A also has a secret key d_A (which is known only to A). It satifies the condition

$$e_A \cdot d_A \equiv 1 \pmod{(p-1)(q-1)}.$$

Usage: To send a (secret) message to A:

0) Translate your (text) message into a sequence of numbers $m_1, m_2, \ldots m_r$ with $m_i < n_A$:

– Agree on a block length (e.g. 4 char.'s/block)

– Use: $00 = blank$, $01 = A, 02 = B, \ldots, 26 = Z$.

1) Encode the message by calculating

$$M_i = \mathrm{rem}(m_i^{e_A}, n_A).$$

Transmit $M_1, M_2, \ldots, M_r$ to A.

2) The user A decodes the message by calculating

$$m_i = \mathrm{rem}(M_i^{d_A}, n_A).$$

The RSA Method

Example: $\left.\begin{aligned} n_A &= 101284087 \\ e_A &= 1234567 \end{aligned}\right\}$ public information

Then: $\left.\begin{aligned} n_A &= p \cdot q \; = \; 10061 \cdot 10067 \\ k &= (p-1)(q-1) = 101263960 \\ d_A &= 36933543 \end{aligned}\right\}$ secret

Note: $e_A d_A \equiv 1 \pmod{k}$.

Messages: to encode the message $m_1, m_2, \ldots, m_r$:

calculate $M_k = \mathrm{rem}(m_k^{e_A}, n_A)$.

to decode: calculate $m_k = \mathrm{rem}(M_k^{d_A}, n_A)$.

Message	Text	Encoded
$m1 = 20080919$	This	$M1 = 18463460$
$m2 = 00091900$	is	$M2 = 81091624$
$m3 = 20151600$	top	$M3 = 39290746$
$m4 = 19050318$	secr	$M4 = 47738594$
$m5 = 05200000$	et	$M5 = 77028351$