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 satisfies the condition

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

**Usage:** To send a (secret) message to $A$, proceed as follows:

1) 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.)

Rule: $00 = \text{blank}, \ 01 = A, \ 02 = B, \ldots, \ 26 = Z$.

2) **Encode** the message by calculating

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

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

3) The user $A$ **decodes** the message by calculating

$$m_i = \text{rem}(M_i^{d_A}, n_A).$$
The RSA Method

Example: \[ n_A = 101284087 \] \[ e_A = 1234567 \] \[ \{ \text{public information} \} \]

Then: \[ n_A = p \cdot q = 10061 \cdot 10067 \] \[ k = (p - 1)(q - 1) = 101263960 \] \[ d_A = 36933543 \] \[ \{ \text{secret info} \} \]

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

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

- calculate \( M_k = \text{rem}(m_k^{e_A}, n_A) \).

To decode: calculate \( m_k = \text{rem}(M_k^{d_A}, n_A) \).

<table>
<thead>
<tr>
<th>Message</th>
<th>Text</th>
<th>Encoded</th>
</tr>
</thead>
<tbody>
<tr>
<td>(m_1 = 20080919)</td>
<td>This</td>
<td>(M_1 = 18463460)</td>
</tr>
<tr>
<td>(m_2 = 00091900)</td>
<td>is</td>
<td>(M_2 = 81091624)</td>
</tr>
<tr>
<td>(m_3 = 20151600)</td>
<td>top</td>
<td>(M_3 = 39290746)</td>
</tr>
<tr>
<td>(m_4 = 19050318)</td>
<td>secr</td>
<td>(M_4 = 47738594)</td>
</tr>
<tr>
<td>(m_5 = 05200000)</td>
<td>et</td>
<td>(M_5 = 77028351)</td>
</tr>
</tbody>
</table>