The RSA* encryption algorithm

* Rivest - Shamir - Adleman, 1977
(Also developed in 1973 by British intelligence, declassified 1997.)

Basic premise:

- Multiplying is easy, but
- Factoring is hard.

(A) Here's how RSA encoding works:

(1) First convert the message to numbers, in some simple way (e.g. $A \to 11$, $B \to 12$, $C \to 13, \ldots$. Convert punctuation etc. similarly). E.g. MATH $\to$ 23113018.

(2) Take the resulting message (e.g. 23113018) - call it n. Raise n to a very large natural number k.

(3) Take the result, and compute its remainder after division by a large integer m. That is, write

$$n^k = mq + r \quad \text{where } 0 \le r < m.$$

Then r is the coded message you send. It's a coded version of n.

(B) Decoding:

(1) under certain conditions, if you

know how m factors, you can recover the original message n from its coded version r. That is, you can decode r. How? We'll answer before long.

(2) But: if you don't know how m factors, you can't decode. Unless you can determine how m factors – but remember, factoring is hard.

(C) "Public key."

The RSA algorithm is public key. This means: knowing how to encode doesn't tell you how to decode.

Specifically: I can give everyone k and m (and the "easy" translation $A \to 11$, $B \to 12$, etc.), and then anyone can encode a message n (by writing $n^k = mq + r$ with $0 \leq r < m$: then r is the coded message). But if I don't say how m factors (and you can't figure it out), you can't decode!

(D) Some number theory.

If we write
$$n^k = mq + r \qquad (0 \leq r < m),$$
then
$$n^k - r = mq, \text{ so } m \mid (n^k - r).$$
So:

it will be useful to study situations where $m \mid (a-b)$, for integers a, b, m.

<u>Definition.</u>

Let $a, b, m \in \mathbb{Z}$. We say "a is congruent to b mod m," and write

$$a \equiv b \pmod{m},$$

if $m \mid (a-b)$.

<u>Examples</u>

$122 \equiv 87 \pmod{5}$ (since $5 \mid 35 = 122 - 87$,

$-13 \equiv 8 \pmod{7}$,

$241137 \equiv 137 \pmod{1000}$,

$k \equiv 1 \pmod{2}$ for any odd $k \in \mathbb{Z}$;

$n \equiv 0 \pmod{2}$ for any even $n \in \mathbb{Z}$;

$3^5 \equiv 3 \pmod{10}$

$3^5 \equiv 3 \pmod{15}$

$3^5 \equiv 3 \pmod{24}$

(since $3^5 - 3 = 240 = 10 \cdot 24 = 15 \cdot 16$),

For any $n \in \mathbb{Z}$,

$$n \equiv r \pmod{7}$$

for some $r \in \mathbb{Z}$ with $0 \leq r < 7$;

For any $n \in \mathbb{Z}$ and $m \in \mathbb{N}$,

$$n \equiv r \pmod{m}$$

for some $r \in \mathbb{Z}$ with $0 \leq r < m$ (by the division algorithm).

$59^{1013} \equiv 59 \pmod{1013}$,

etc.

Properties of "mod m:"

<u>Proposition</u>. Let $a, b, c, d, m \in \mathbb{Z}$.
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

(i) $a+c \equiv b+d \pmod{m}$.
(ii) $a-c \equiv b-d \pmod{m}$.
(iii) $ac \equiv bd \pmod{m}$.

<u>Proof</u> of (i).
Let $a, b, c, d, m \in \mathbb{Z}$; assume $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then $m \mid (a-b)$ and $m \mid (c-d)$, so $m \mid ((a-b)+(c-d))$. So $m \mid ((a+c)-(b+d))$, so

$$a+c \equiv b+d \pmod{m}. \qquad \square$$

<u>E.g.</u> $25 \equiv 4 \pmod{7}$ and $75 \equiv -2 \pmod{7}$, so $100 \equiv 2 \pmod{7}$.

Proof of parts (ii) and (iii): see HW 10.