(1) $n = pq$, where $p$, $q$ are large primes;

(2) $(e, \varphi(n)) = 1$;

(3) the enciphering transformation is $\tau(x) = y$, with $y \in \mathbb{N}$ satisfying $y < n$ and

$$y \equiv x^e \pmod{n}.$$

To encipher, we group the numbers into blocks of $2m$ digits, where $m$ is the largest natural number such that any $2m$ digit number which could appear is less than $n$.

To decipher we use the deciphering key $(d, n)$, where $d$ is the inverse of $e$ modulo $\varphi(n)$:

$$de \equiv 1 \pmod{\varphi(n)}.$$

It follows that there exists $k \in \mathbb{Z}$ such that $de = 1 + k\varphi(n)$.

Note that, since $(p, q) = 1$, $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$.

Hence, if $(x, n) = 1$, Fermat's Theorem 14.8 gives that

$$\begin{aligned} y^d &\equiv (x^e)^d \pmod{n} \equiv x^{de} \pmod{n} \equiv x^{1+k\varphi(n)} \pmod{n} \equiv x \cdot x^{k(p-1)(q-1)} \pmod{n} \\ &\equiv x \cdot \left(x^{p-1}\right)^{k(q-1)} \pmod{n} \equiv x \pmod{n}. \end{aligned}$$

So $x \equiv y^d \pmod{n}$.

**Note 16.7.** The choice of $n$ means that the probability that $(x, n) = 1$ is high.

**Fast Processes**

(1) finding primes with $\sim 100$ digits,

(2) modular exponentiation with a modulus $n$ of $\sim 200$ digits.

**Slow Processes**

(1) factoring $n$ with $\sim 200$ digits,

(2) finding $\varphi(n)$ when $n$ has $\sim 200$ digits.

So to use the RSA system,

(1) choose primes $p$, $q$ with $\sim 100$ digits;

(2) choose a prime $e$ such that $e > pq$.

As an alternative to (2), choose a prime $e$ such that $2^e > pq$ and $(e, \varphi(pq)) = 1$.