Because of the widespread use in real aplications there has been **a great deal of effort expended in trying to break RSA**.

While it appears that so far it has resisted such attack these efforts have resulted in a series of 'health warnings' about **possible ways the system may be compromised**. We list some of the better known ones below.

Insecurities in RSA

When the **prime factors of either $p - 1$ or $q - 1$ are all small**, factoring techniques introduced by Pollard (1974) enable $n = pq$ to be factoring quickly.

This is also true if **the prime factores of $p + 1$ or $q + 1$ are all small**, as was shown by Williams (1982).

Insecurities in RSA

Proposition

If the primes p and q in RSA are chosen to be 'close' then RSA is insecure.

Proof.

If p and q are 'close' then $\frac{p+q}{2}$ is not much larger than $\sqrt{pq}$ (we know that it is always at least as big).
Assuming that $p > q$, we can write

$$x = \frac{p+q}{2} \quad , \quad y = \frac{p-q}{2},$$

so $n = pq = x^2 - y^2 = (x-y)(x+y)$.
Hence if Eve can express n as the difference of two squares then she can factor n — see justification below. $\square$

Insecurities in RSA

To factor $n = pq = x^2 - y^2 = (x - y)(x + y)$:

- Eve tests each number in turn form $\lceil \sqrt{n} \rceil, \lceil \sqrt{n} \rceil + 1, \cdots$ until she find a value s such that $s^2 - n$ is a square.

This happens when $s = x$ and therefore $y^2 = s^2 - n$.
Notice that $p = x + y$ and $q = x - y$.

If $p = (1 + \epsilon)\sqrt{n}$, with $\epsilon > 0$, then Eve needs to test approximately

$$\frac{p + q}{2} - \sqrt{n} = \frac{\epsilon^2 \sqrt{n}}{2(1 + \epsilon)},$$

values of s before she is successful. This is feasible if ϵ is sufficiently small.