Design Features of RSA Keys

**Basic Task for RSA keys:** The user $A$ has to generate a public key $(n_A, e_A)$ and a private key $d_A$ such that $n_A = pq$, where $p, q$ are primes, and

\[ e_A d_A \equiv 1 \pmod{(p - 1)(q - 1)}. \] (1)

**Key Generation:**
1) Pick a random number $p \in [a, b]$ and use a primality test to determine whether $p$ is prime. If not, repeat until a prime $p$ has been found. Similarly, determine $q$ and put $n_A = pq$.
2) Put $k = (p - 1)(q - 1)$, and pick a random $e_A \in [2, k]$. Check that $\gcd(e_A, k) = 1$. Solve for $d_A$ in (1) by using the extended Euclidean algorithm.

**Design Rules:**
1) $p - q$ must be large ($\rightarrow$ Fermat Factorization).
2) $p - 1$ and $q - 1$ should each have a large prime factor ($\rightarrow$ Pollard’s $p - 1$ Method).
3) $\gcd(p - 1, q - 1)$ should be small.
4) $d_A$ must be large: $d_A > n_A^{1/4}$ ($\rightarrow$ continued fraction method).