3.6 RSA and Pseudoprimes

To use RSA we need primes. The probabilistic RABIN primality test solves the problem of finding them in a highly efficient, but not perfectly satisfying way: We could catch a "wrong" prime. What could happen in this case?

For an analysis of the situation let $n = pq$ be a putative RSA module where p and q are not necessarily primes, but at least coprime. For the construction of the exponents d, e with

$$de \equiv 1 \pmod{\lambda(n)} \quad (\text{or} \quad \pmod{\varphi(n)})$$

we use the possibly wrong values

$$\tilde{\varphi}(n) := (p-1)(q-1), \quad \tilde{\lambda}(n) := \mathrm{kgV}(p-1, q-1)$$

instead of the true values $\varphi(n)$ and $\lambda(n)$ of the EULER and CARMICHAEL functions.

How do the RSA algorithms work with the "false" values? Let $a \in \mathbb{Z}/n\mathbb{Z}$ be a plaintext. As usual the case $\gcd(a, n) > 1$ leads to a decomposition of the module, we ignore it because of its extremely low probability. So we assume $\gcd(a, n) = 1$, and ask whether

$$a^{de-1} \stackrel{?}{\equiv} 1 \pmod{n}$$

holds. By the chinese remainder theorem this holds if and only if

$$a^{de-1} \equiv 1 \pmod{p} \quad \text{and} \quad \pmod{q}\,.$$

A sufficient condition is

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{and} \quad a^{q-1} \equiv 1 \pmod{q}\,.$$

Thus a message a might be incorrectly decrypted only if p or q is not a pseudoprime to base a. Hence:

- If instead of a prime factor p we use a CARMICHAEL number, then RSA works correctly despite the "false" parameters, at least if a is coprime with n, though the (extremely low) probability of accidentally factorizing the module n by catching an inept plaintext a is slightly enlarged.
- Otherwise p is not a prime nor a CARMICHAEL number. Then there is a small chance that a message cannot be correctly decrypted.

For this reason many implementations of RSA execute a few trial encryptions and decryptions after generating a key pair relying on the probabilistic RABIN test. But the effect of this additional step simply boils down to a few additional pseudoprime tests. If something goes wrong, the module is rejected.

It is unknown whether this case yet occured in this universe.