# Cycle Structure of RSA with Small Moduli

Philip Winkler
Fernuniversität in Hagen

Jörg Keller
Fernuniversität in Hagen

32nd Crypto Day, 15 January 2021

The RSA function $RSA(x) = x^e \mod n$ realizes a permutation on the set of integers $[0, ..., n-1]$. Therefore, all numbers $x < n$ are mapped onto each other in a cyclical manner: $x = RSA(RSA(...RSA(x))) = RSA^i(x)$. The length $i$ of each of these cycles is a divisor of the iterated Carmichael function $\lambda(\lambda(n))$ of the modulus $n$ (Katzenbeisser (2001)). The cycle lengths have been studied theoretically in Friedlander, Pomerance & Shparlinski (2001) and Kurlberg & Pomerance (2005). However, these mathematical results do not convey an intuitive understanding of the cycle length distribution for a given $n$. In this work, the cycle lengths have been analyzed experimentally for small moduli $n \leq 2^{30}$. This involves a study of the magnitude of the maximum cycle length $\lambda(\lambda(n))$ compared to $n$ and an investigation of which divisors of $\lambda(\lambda(n))$ actually occur as cycle lengths.

It has been shown that the range of $\lambda(\lambda(n))$ is $\sqrt{n} \leq \lambda(\lambda(n)) \leq \frac{1}{8}n$ with an average value of $n^{0.8}$. Furthermore, the average cycle length is approximately $0.2\lambda(\lambda(n))$.

The RSA-function could be used as a state-transition function for pseudo-random number generators. The estimates for the cycle lengths show that this might be advantageous compared to non-bijective transition functions, which on average have a cycle length $\sqrt{\frac{\pi n}{2}}$ (Flajolet & Odlyzko (1990)) and therefore require larger state spaces to achieve similar cycle lengths.

## References

Philippe Flajolet & Andrew M. Odlyzko (1990). Random Mapping Statistics. In *Advances in Cryptology — EUROCRYPT '89*, Jean-Jacques Quisquater & Joos Vandewalle, editors, 329–354. Springer Berlin Heidelberg, Berlin, Heidelberg. ISBN 978-3-540-46885-1.

John Friedlander, Carl Pomerance & Igor Shparlinski (2001). Period of the power generator and small values of Carmichael's function. *Math. Comput.* **70**, 1591–1605.

Stefan Katzenbeisser (2001). *Recent Advances in RSA Cryptography*, volume 3. ISBN 978-1-4613-5550-2.

Paer Kurlberg & Carl Pomerance (2005). On the period of the linear congruential and power generators. *Acta Arithmetica - ACTA ARITHMET* **119**, 149–169.

**crypto day matters 32** (2021)
Beiträge vom 32. Kryptotag, 15.01.2021, online.
doi:10.18420/cdm-2021-32-12