Kryptologie LAB - 4.1

Summer Semester 2020

Dr. Joshua Blinkhorn

Friedrich-Schiller-Universität Jena

Rivest-Shamir-Adleman (RSA)

- Public-key cryptosystem
- Different keys for encyption and decryption
- Keys are interpreted as (unsigned) integers
- Texts are interpreted as sequences of (unsigned) integers

Task 4 - part 1

- Implement an RSA key generation routine.
  - choose two distinct primes p and q
  - set $n = pq$, note $\phi(n) = (p-1)(q-1)$
  - public key: find an integer e with $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$
  - private key: $d := e^{-1} \pmod{\phi(n)}$, i.e. $d \cdot e \equiv 1 \pmod{\phi(n)}$
- $\phi(n)$ should be expressible as a 64-bit unsigned integer, and larger than all 32-bit unsigned integers:

$$4,294,967,295 < \phi(n) \leq 18,446,744,073,709,551,615$$

Getting the keys

- public key (easy), use $e = 3$.
- private key (harder): use Extended Euclidean Algorithm (EEA)
  - we know that $\gcd(e, \phi(n)) = 1$
  - algorithm returns integers λ and μ such that

$$\lambda \cdot e + \mu \cdot \phi(n) = 1$$

  - hence $\lambda = e^{-1} \pmod{\phi(n)}$
  - the private key is $d := \lambda$
- details for EEA can be found in the lecture slides