# Kryptologie LAB - 4.2

# Summer Semester 2020

## Dr. Joshua Blinkhorn

Friedrich-Schiller-Universität Jena

# Rivest-Shamir-Adleman (RSA)

- Public-key cryptosystem

- Different keys for encryption and decryption

- Keys are interpreted as (unsigned) integers

- Texts are interpreted as sequences of (unsigned) integers

# Key generation recap

- choose two distinct primes $p$ and $q$
- set $n = pq$, note $\phi(n) = (p-1)(q-1)$
- public key: $e := 3$
- private key: $d := e^{-1} \pmod{\phi(n)}$ (compute with EEA)

- $n$ should be expressible as a 64-bit unsigned integer, and larger than all 32-bit unsigned integers:

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

# Encryption and Decryption with RSA

- main concept: $(m^e)^d \equiv m \,(\text{mod } n)$

- given a plaintext $m_1, \ldots, m_r$:

    - encryption: $c_1, \ldots, c_r := m_1^e \,(\text{mod } n), \ldots, m_r^e \,(\text{mod } n)$

    - decryption: $m_1, \ldots, m_r := c_1^d \,(\text{mod } n), \ldots, c_r^d \,(\text{mod } n)$

- to compute $m^e \,(\text{mod } n)$:

$$c := 1, \; e' := 0$$
$$\text{while } e' < e$$
$$\quad c := m \cdot c \,(\text{mod } n)$$
$$\quad e' := e' + 1$$
$$\text{return } c$$

# Task 4 - part 2

- Implement RSA encryption and decryption routines.

    - assume the plaintext is ASCII encoded text

    - break up the text into 32-bit blocks

    - if necessary, pad out the final block with whitespace

- Perform a runtime comparison between:

    (a) encryption and decryption of plaintext with RSA

    (b) encryption and decryption of DES key with RSA, together with encryption and decryption of plaintext with DES

    - try to produce a plaintext for which (b) is fast (e.g. $< 30$ seconds) but (a) is slow (e.g. $> 3$ mins)

# Examination format

- Demonstrate your tools:
  - Additive cypher
  - Vigenère
  - DES
  - RSA

- Demonstrate an RSA/DES runtime comparison

## Guidelines

- Bring your laptop
- Try to polish your user interface (rather than your code)
- Be creative: if your tools have extra features - show them!
- Prepare your demonstration
- Demonstrate what you have – even if it is unfinished