RSA algorithm

Each user has following keys:

- Public keys

  modulus $n = p * q$ (product of two primes)

  exponent e : $\mathrm{GCD}(e,(p-1)(q-1)) \neq 1$

- Private key exponent for decryption

  $d = e^{-1} \bmod (p-1)(q-1))$

ENCRYPTION $c = m^{e} \bmod n$

DECRYPTION $m = c^{d} \bmod n$

Example with small numbers

Alice has following keys:

Public keys : $n = 187$ (11*17) and $e = 29$

Private key $d = 29^{-1} \bmod 160 = 149$

Encrypt a message m = 101 to Alice

ENCRYPTION $c = 101^{29} \bmod 187 = 50$

DECRYPTION $m = 50^{149} \bmod 187 = 101$

RSA security

- If the enemy wants to break the cipher, he should find the decryption key.
- Finding d requires the knowledge of factors of modulus n
- It is possible to factor only 600 – 700 bit integers within a few months
- Secure modulus size is > 1024 bits

RSA performance

- RSA is too slow for encryption of large amounts of data
- It is widely used in secure protocols in key exchange and authentication
- The development of computers will soon make RSA difficult to use: it will be replaced by ECC (Elliptic Curve Cryptography)