

openHPI – Internet Security
RSA

Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

RSA - Most Popular 2-Key Encryption (1/6)

RSA encryption is the most popular and widely used 2-key encryption method

- Developed in 1977 by:
Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman
- RSA is based on the mathematical problem of **factorization of very large numbers** which cannot be solved practically (i.e., in a realistic timeframe):
 - product of two very large, randomly chosen primes can not be factored in a realistic timeframe without knowledge of the two primes ...

RSA - Most Popular 2-Key Encryption (2/6)

Numerical example (with small numbers) **of RSA encryption:**

Starting point:

1. Choice of two prime numbers, e.g., $p = 17$ and $q = 31$
2. Calculate their product:
 - $N = p * q$
 - *Example:* $N = 17 * 31 = 527$
3. Calculate the so-called Euler phi function:
 - $\varphi(N) = \varphi(p) * \varphi(q) = (p-1)*(q-1)$
For prime numbers: $\varphi(\text{prime number}) = (\text{prime number} - 1)$
 - *Example:* $\varphi(N) = 16 * 30 = 480$

Generation of a key pair for participants ...

RSA - Most Popular 2-Key Encryption (3/6)

Numerical example (with small numbers) of RSA encryption

Generation of a key pair for participant A:

4. Select a number $e < \phi(N)$ which is prime to $\phi(N)$
 - *Example:* $e = 13$
 - $(e, N) = (13, 527)$ is **the public key of A**
5. Calculation of the multiplicative inverse d to e with respect to $\phi(N)$, i.e., $e * d \bmod \phi(N) = 1$
 - *Example:*
 $d = 37$, since $e * d \bmod \phi(N) = 13 * 37 \bmod 480 = 1$
 - $(d, N) = (37, 527)$ is **the private key of A**

RSA - Most Popular 2-Key Encryption (4/6)

Comment:

- In the end, only e , d and N are needed to create a
 - public key (e, N)
 - private key (d, N)

Application of the method:

- Encrypt/decrypt with public/private key
 - Cipher = $(\text{message})^e \bmod N$
 - Message = $(\text{cipher})^d \bmod N$
- Encrypt/decrypt with private/public key
 - Cipher = $(\text{message})^d \bmod N$
 - Message = $(\text{cipher})^e \bmod N$

RSA - Most Popular 2-Key Encryption (5/6)

Application of the method – our example

Communication partner B wants to send A the message "456":

- B gets public key from A $(e, N) = (13, 527)$ and uses it to encrypt message "456":

$$456^e \bmod N \rightarrow 456^{13} \bmod 527 = 447$$

- B sends "447" over the Internet to A
- A can decrypt "447" with his/her private key $(d, N) = (37, 527)$:

$$447^d \bmod N \rightarrow 447^{37} \bmod 527 = 456$$

RSA - Most Popular 2-Key Encryption (6/6)

The correctness of the RSA method is based on a well-known theorem of the number theory:

Fermat's Little Theorem

- For any a and prime p :

$a^{p-1} \equiv 1 \pmod{p}$, if a is not a multiple of p

- Argument:

If it is true that $e * d \equiv 1 \pmod{(p-1)*(q-1)}$

Then there exists an x with $e * d - 1 = x * (p-1) * (q-1)$