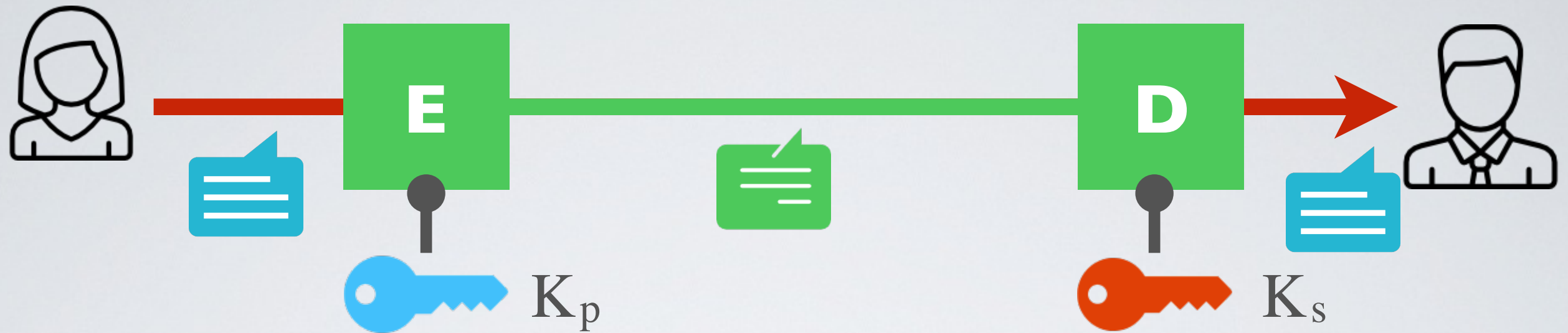


# Asymmetric Encryption

Thierry Sans

# Functional Requirements



➡ The public key  $K_p$  for encryption

➡ The private key  $K_s$  for decryption

1.  $D_{K_s}(E_{K_p}(m))=m$  for every pair  $(K_p, K_s)$
2.  $E_{K_p}(m)$  is easy to compute (either polynomial or linear)
3.  $D_{K_s}(C)$  is easy to compute (either polynomial or linear)
4.  $p = D_{K_s}(C)$  finding  $m$  is hard without  $K_s$  (exponential)
5. Generating a pair  $(K_p, K_s)$  is easy to compute (polynomial)
6. Finding a matching key  $K_s$  for a given  $K_p$  is hard (exponential)

# RSA - Rivest, Shamir and Alderman

Key Size	1024 - 4096
Speed	~ factor of $10^6$ cycles / operation
Mathematical Foundation	Prime number theory

# Number Theory - Prime numbers

## Prime Numbers

- $p$  is prime if 1 and  $p$  are its only divisors e.g 3, 5, 7, 11 ...
  - $p$  and  $q$  are relatively prime (a.k.a. coprime) if  $\gcd(p,q) = 1$   
e.g  $\gcd(4,5) = 1$
- ➡ There are infinitely many primes

## Euler-Fermat Theorem

If  $n = p \cdot q$  and  $z = (p-1) \cdot (q-1)$

and  $a$  such that  $a$  and  $n$  are relative primes

Then  $a^z \equiv 1 \pmod{n}$



# Computational Complexity

## **Easy problems** with prime numbers

- Generating a prime number  $p$
- Addition, multiplication, exponentiation
- Inversion, solving linear equations

## **Hard problem** with prime numbers

- Factoring primes  
e.g. given  $n$  find  $p$  and  $q$  such that  $n = p \cdot q$

# RSA - generating the key pair

1. Pick  $p$  and  $q$  two large prime numbers and calculate  $n = p \cdot q$   
(see primality tests)
2. Compute  $z = (p-1) \cdot (q-1)$
3. Pick a prime number  $e < z$  such that  $e$  and  $z$  are relative primes  
➔  $(e, n)$  is the **public key**
4. Solve the linear equation  $e * d = 1 \pmod{z}$  to find  $d$   
➔  $(d, n)$  is the **private key**  
however  $p$  and  $q$  must be kept secret too

# RSA - encryption and decryption

Given  $K_p = (e, n)$  and  $K_s = (d, n)$

➡ Encryption :  $E_{kp}(m) = m^e \bmod n = c$

➡ Decryption :  $D_{ks}(c) = c^d \bmod n = m$

➡  **$(m^e)^d \bmod n = (m^d)^e \bmod n = m$**

# The security of RSA

**RSA Labs Challenge** : factoring primes set

Key length	Year	Time
140	1999	1 month
155	1999	4 months
160	2003	20 days
200	2005	18 months
768	2009	3 years

Challenges are no longer active



# Key length and Key n-bit security

- RSA has very long keys, 1024, 2048 and 4096 are common
- Is it more secure than asymmetric crypto with key lengths of 56, 128, 192, 256 ?

➔ Key lengths **do not compare !**

RSA Key length	Effective key length
1,024	80
2,048	112
3,072	128
7,680	192
15,360	256

# Asymmetric vs Symmetric

	Symmetric	Asymmetric
pro	Fast	No key agreement
cons	Key agreement	Very slow

The best of both worlds

- ➡ Use RSA to encrypt a shared key
- ➡ Use AES to encrypt message

$$E_{K_p}(m) = \text{RSA}_{K_p}(k), \text{AES}_k(m)$$

Naive  
approach

# Other asymmetric cryptography schemes

## **Diffie-Hellman** (precursor)

- ➡ No Authentication but good for key-exchange

## **El-Gamal**

- ➡ Good properties for homomorphic encryption

## **Elliptic Curve Cryptography** (trending nowadays)

- ➡ Fast and small keys (190 bits equivalent to 1024 bits RSA)