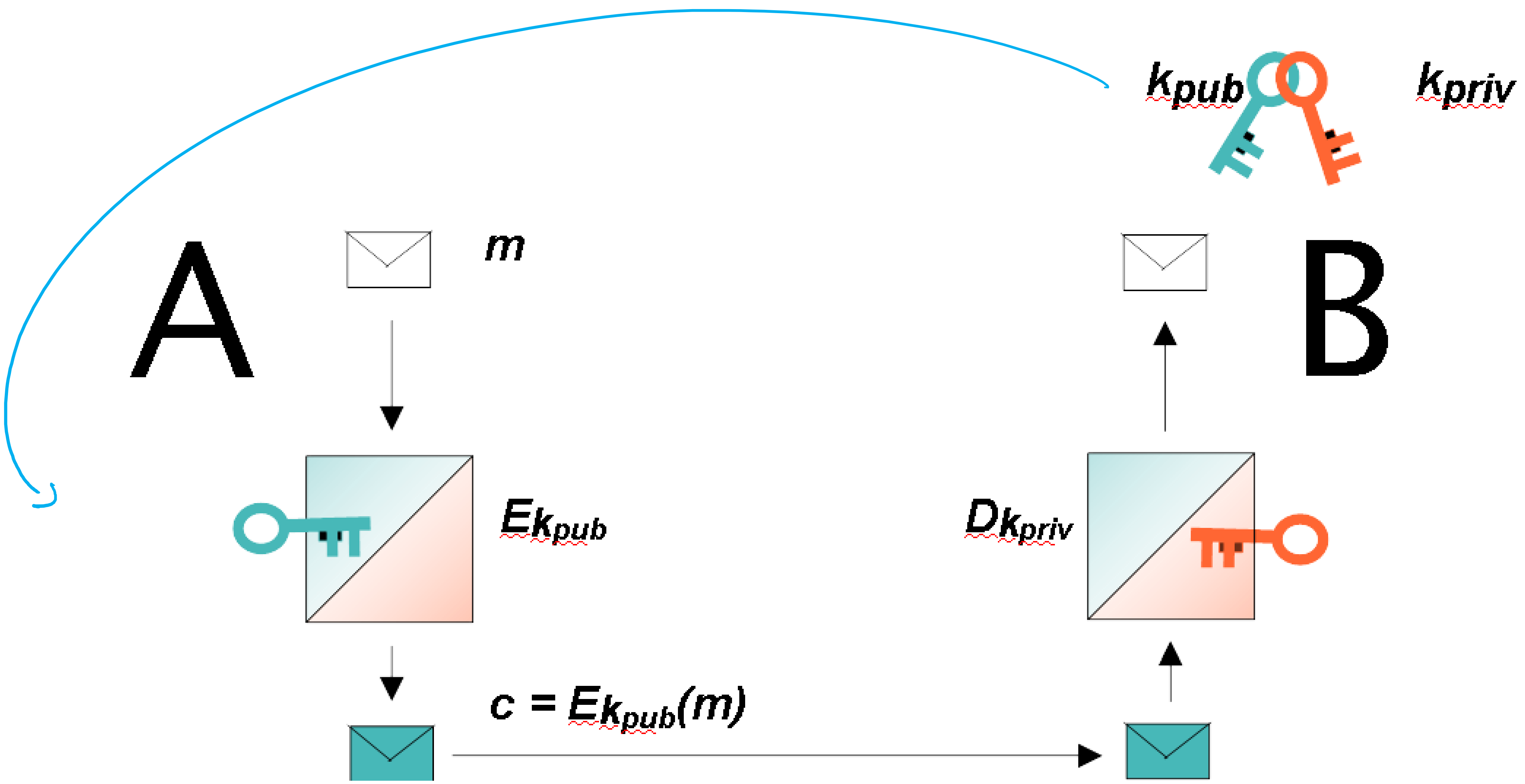
Asymmetric Ciphers



RSA public key encryption scheme

- Public key encryption scheme proposed by **R.L. Rivest, A. Shamir, L.M. Adleman** in ***A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*** (1978)
- Depends on the mathematical (computational) problem of **factorizing integers**.

If p is a prime number and z any number coprime to p, $\Leftrightarrow p \nmid z$

i.e. gcd(p,z) = 1, then

$$z^{p-1} \equiv 1 \pmod{p} \quad \Leftrightarrow \quad p \mid (z^{p-1}-1)$$

$\Leftrightarrow_{(p \nmid z)}$ $\boxed{z^p \equiv z \pmod{p}}$

$\mathbb{Z}_p = \{0,1,\ldots,p-1\}$

$z \in \mathbb{Z}_p^*$

$o(z) \mid (p-1)$

by F3(i)

$p-1 = o(z) \cdot b$

$\mathbb{Z}_p$: $z^{p-1} = z^{o(z)\cdot b}$

$= (z^{o(z)})^b = 1^b = 1$

[Proof F3(i)]

Proof:

- Put: $t = (1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)) \bmod p$ $\neq 0$ (in $\mathbb{Z}_p$)
- Multiplication with z defines a bijective mapping:

  $m_z: \mathbb{Z}_p \to \mathbb{Z}_p,\ m_z(x) = (x \cdot z) \bmod p$ $\qquad m_z: \mathbb{Z}_p^* \to \mathbb{Z}_p^*$
- It follows that:

  $t \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv (1 \cdot z) \cdot (2 \cdot z) \cdot (3 \cdot z) \cdot \ldots \cdot ((p-1) \cdot z) \equiv t \cdot z^{p-1} \pmod{p}$
- Division in $\mathbb{Z}_p$ by $t \neq 0$ gives the claimed identity.

Let p,q be prime numbers ($p \neq q$) and $r \in \mathbb{Z}$ with:

$$r \equiv 1 \ (\textbf{mod}\ \mathrm{lcm}(p\text{-}1,\ q\text{-}1))$$

$\iff \mathrm{lcm}(p-1, q-1) \mid (r-1)$

$\iff \begin{cases} (p-1) \mid (r-1) \ (*) \\ \text{and } (q-1) \mid (r-1) \end{cases}$

Then:

$$z^r \equiv z \ \ (\textbf{mod}\ (p \cdot q)) \quad \text{for all } z \in \mathbb{Z}$$

$\iff \begin{cases} z^r \equiv z \mod p \\ z^r \equiv z \mod q \end{cases}$

Proof:

- If $z \equiv 0$ (**mod** p), then $z^r \equiv 0$ (**mod** p).
- If p does not divide z and $r = 1 + n(p\text{-}1)$, then:

$r - 1 \overset{(*)}{=} n \cdot (p-1)$ for some $n \in \mathbb{N}$

$$z^r = z \cdot (\underbrace{z^{(p\text{-}1)}}_{1 \text{ (Fermat's Lemma)}})^n \equiv z \ (\textbf{mod}\ p)$$

- Similarly:

$$z^r \equiv z \ (\textbf{mod}\ q)$$

- Chose two random primes p and q $(> 2^{1000})$ with $e \nmid (p-1)$ and $e \nmid (q-1)$
- Put $n = pq$, $v = lcm\,(p - 1, q - 1)$
- Define a <u>public exponent</u> e with:

$$\gcd(e, v) = 1$$

typically $e = 2^{16}+1 = 10\ldots01$ a 4-th Fermat primes $2^{2^n}+1$ $(3, 5, 17, 65537, \ldots)$ with $65537 = e$

- Determine the <u>private exponent</u> d with:

$$ed \equiv 1 \ (\mathbf{mod}\ v)$$

$[d = e^{-1} \text{ in } \mathbb{Z}_v]$

- Key pair (k_{pub}, k_{priv}):

$$k_{pub} = (n,e) \qquad k_{priv} = (n,d)$$

modul — public exponent — private exponent

- **Encryption** of a message m ($< n$):

$$c = \mathrm{E}(m) = m^e \bmod n$$

$k_{pub} = (n,e)$

- **Decryption** of c:

$$\mathrm{D}(c) = c^d \bmod n$$

$k_{priv} = (n,d)$

- $\mathrm{D}(c) = m$ follows from $e \cdot d \equiv 1 \pmod{v}$ and conseq. of Fermat's lemma:

$$\mathrm{D}(c) = c^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n = m \bmod n = m$$

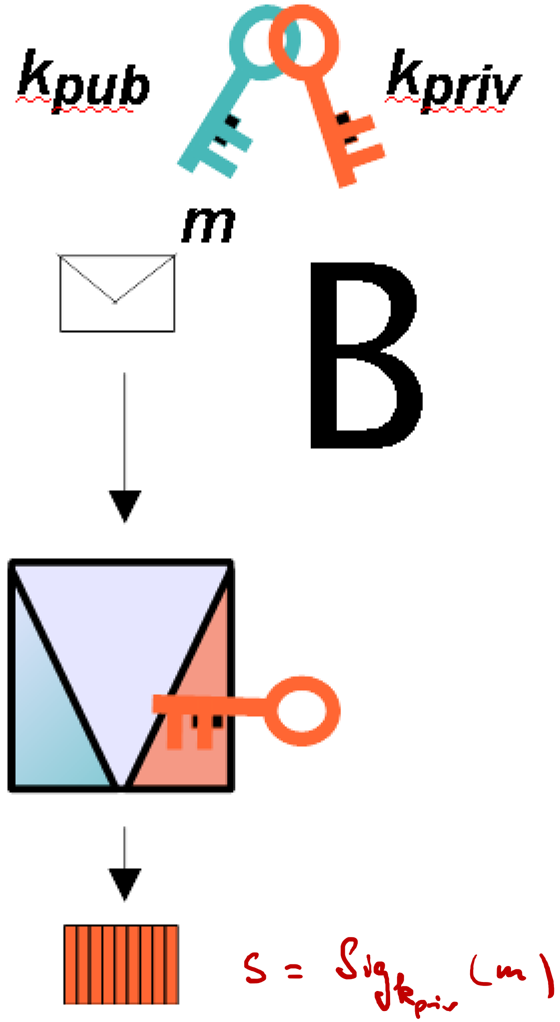
$= (m^e \bmod n)^d \bmod n$

Digital Signatures

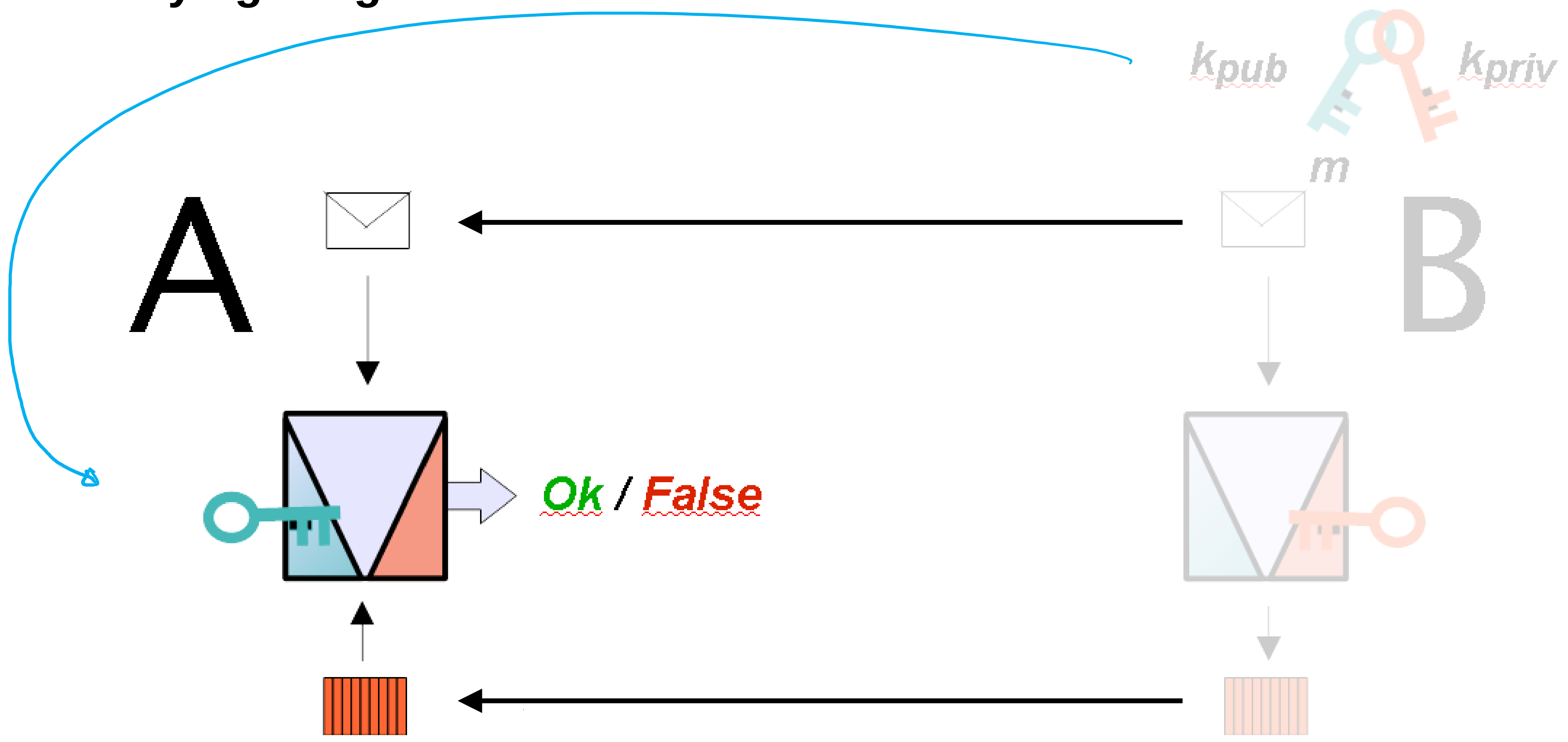
- FIPS PUB 186-4: Digital Signature Standard (DSS)
  - Chapter 4: The Digital Signature Algorithm (DSA)
  - Chapter 5: The RSA Digital Signature Algorithm
  - Chapter 6: The Elliptic Curve Digital Signature Algorithm (ECDSA)

Digital Signature Algorithms

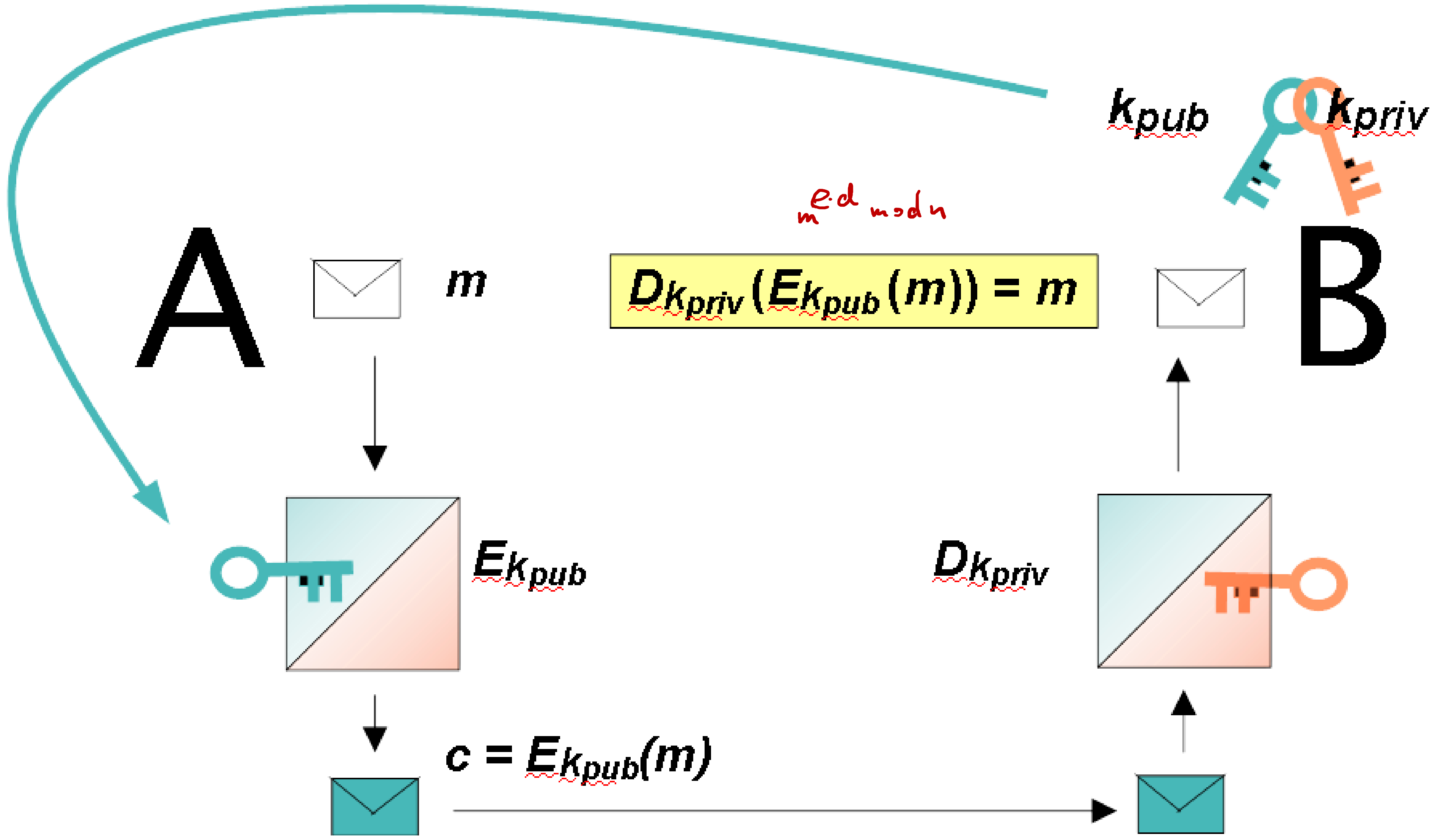
- **Signing a message**



- **Verifying a signature**

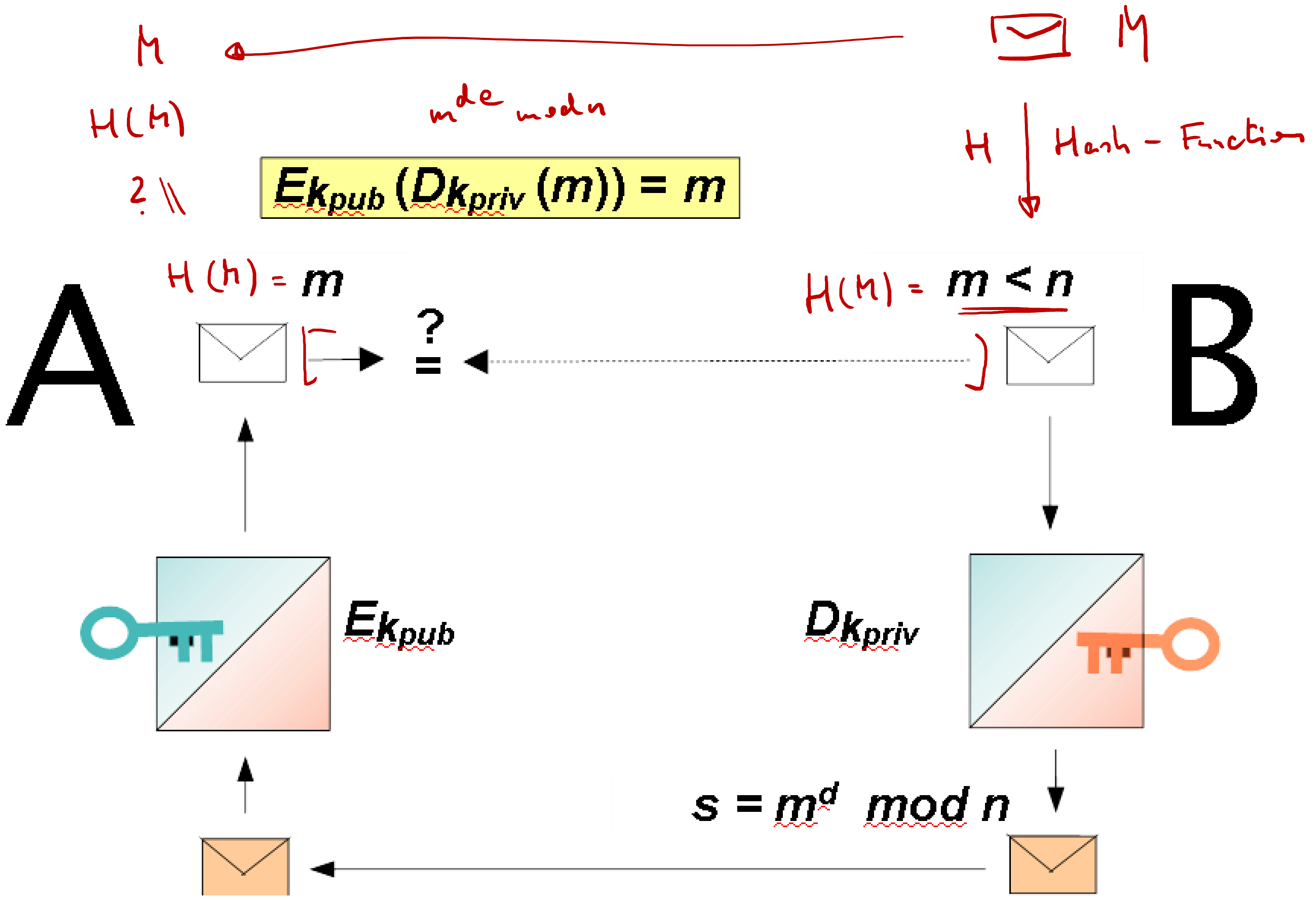


RSA encryption and decryption



RSA signature algorithm

$$E_{k_{pub}}(D_{k_{priv}}(m)) = m$$



- **DSA Domain Parameters**
  - ***p*** : prime number of bit length ***L***
  - ***q*** : a prime divisor of ***p*-1** of bit length ***N*** $p-1 = q \cdot b$
  - ***g*** : element of **GF(*p*)*** with **o(*g*) = *q***

  $\mathbb{Z}_p^*$, let $h \in \mathbb{Z}_p^*$ with $o(h) = p-1 = q \cdot b \Rightarrow g := h^b$, $o(g) = q$

  - Selection of Parameter Sizes and **Hash** Functions for DSA:
    - L = 1024, N = 160 SHA-1
    - L = 2048, N = 224 SHA-224
    - L = 2048, N = 256 SHA-256
    - L = 3072, N = 256 – " –

- **DSA Domain Parameters**
  - ***p*** : prime number of bit length ***L***
  - ***q*** : a prime divisor of ***p*-1** of bit length ***N***
  - ***g*** : element of **GF(*p*)*** with **o(*g*) = *q***

$GF(p)^* \supseteq \langle g \rangle = \{ g, g^2, g^3, ..., g^q = 1 \}$

- **DSA Key Pairs**
  - ***x*** : private key with $\mathbf{0 < x < q}$
  - ***y*** : public key $\mathbf{y = g^x}$ mod ***p***

- Domain Parameters: p, q, g
- Key Pair: x, y
- **Signature Generation for message *M***
  - k : per message newly generated secret random number, $0 < k < q$
  - $r := (g^k \bmod p) \bmod q$
  - z : Hash(M) (leftmost N bits)
  - $s := (k^{-1}(z + \cancel{x}r)) \bmod q$
  - $\mathrm{Sig}_x(M) := (r, s)$

- **Domain Parameters:** p, q, g
- **Key Pair:** x, y $= g^x \bmod p$
- **Signature for M:** $\mathrm{Sig}_x(M)=(r, s)$, $r = (g^k \bmod p) \bmod q$, $s = (k^{-1}(z + xr)) \bmod q$
- **Signature Verification (given M, $\mathrm{Sig}_x(M) = (r, s)$, y)**
  - $w := s^{-1} \bmod q$ in $\mathbb{Z}_q$: $w = s^{-1} = k \cdot (z + xr)^{-1} \bmod q$
  - z : Hash(M) (leftmost N bits)
  - $u_1 := (zw) \bmod q$
  - $u_2 := (rw) \bmod q$
  - $v := ((g^{u_1} y^{u_2}) \bmod p) \bmod q$
  - $\mathrm{Sig}_x(M)$ ok iff $v = r$

$$(g^{z \cdot w} \cdot g^{x \cdot r w}) \bmod p = g^{w(z + x \cdot r)} \bmod p$$
$$= g^{k(z+xr)^{-1}(z+xr)} \bmod p$$
$$= g^k \bmod p$$

Elliptic Curve Digital Signature Algorithm (ECDSA)

- **FIPS PUB 186-4, Ch. 6**
  - relates strongly to ANS X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Standard (ECDSA)
  - FIPS PUB 186-4, Appendix D: Recommended Elliptic Curves for Federal Government Use
- Certicom Research: Standards for Efficient Cryptography
  - SEC 1: Elliptic Curve Cryptography
  - SEC 2: Recommended Elliptic Curve Domain Parameters

Elliptic Curve Digital Signature Algorithm (ECDSA)

$o(g) = q : q \cdot G = \mathcal{O}$

$x \cdot G$ $\quad g^x \quad o(g) = q$

$(E, +) \longleftarrow (\mathbb{Z}_p^*, \cdot)$

- **ECDSA Domain Parameters**
  - ***E*** : elliptic curve over F = GF(p) or F = GF(2^m)
  - ***q*** : a large prime divisor of **|*E*| = *qh*** (with cofactor ***h***)
  - ***G*** : point of **E** with **o(G) = *q***

- **ECDSA Domain Parameters**
  - ***E*** : elliptic curve over F = GF(p) or F = GF(2^m)
  - ***q*** : a large prime divisor of **|*E*| = *qh*** (with cofactor ***h***)
  - ***G*** : point of **E** with **o(G) = q**

- **ECDSA Key Pair**
  - ***x*** : private key with $0 < x < q$
  - ***Y*** : public key $Y = x \cdot G$

Elliptic Curve Digital Signature Algorithm (ECDSA)

- Domain Parameters: E, q, G
- Key Pair: x, Y
- **Signature Generation for message *M***
  - k : per message newly generated secret random number, $0 < k < q$
  - $R := k \cdot G = (R_x, R_y)$, $\quad r := R_x \mod q$
  - z : Hash(M) (leftmost N bits)
  - $s := (k^{-1}(z + xr)) \mod q$
  - $\text{Sig}_x(M) := (r, s)$

Elliptic Curve Digital Signature Algorithm (ECDSA)

- Domain Parameters: E, q, G
- Key Pair: $x, Y = x \cdot G$
- Signature for M: $\mathrm{Sig}_x(M) = (r, s)$, $r = (k \cdot G)_x \bmod q$, $s = (k^{-1}(z + xr)) \bmod q$
- **Signature Verification (given M, $\mathrm{Sig}_x(M) = (r, s)$, Y)**
  - $w := s^{-1} \bmod q$
  - z : Hash(M) (leftmost N bits)
  - $u_1 := (zw) \bmod q$
  - $u_2 := (rw) \bmod q$
  - $V := u_1 \cdot G + u_2 \cdot Y$, $v := V_x \bmod q$
  - $\mathrm{Sig}_x(M)$ ok iff $v = r$

$$V = z \cdot w \cdot G + r \cdot w \cdot x \cdot G = (z \cdot w + r \cdot wx) \cdot G$$
$$= (w \cdot (z + rx)) \cdot G = k \cdot G$$

TH OWL Technische Hochschule Ostwestfalen-Lippe University of Applied Sciences and Arts

initial a | initial b

$A = 132$	$B = 156$		q
1	0	132	
0	1	156	0
1	0	132	1
-1	1	24	5
6	-5	12	2
		0	

initialization

STOP

$\gcd(132, 156) = 12$

$a > b$

$\gcd(a, b) = \gcd(b, a \bmod b)$, $a \bmod b = a - q \cdot b$

with $q = \frac{a}{b}$

$x \cdot A + y \cdot B = b$

$\rightarrow \quad 6 \cdot 132 - 5 \cdot 156 = 12 = \gcd(132, 156)$

Extended Euclidean Algorithm (EEA)

$p = 107$

$x = 42$

$\gcd(p, x) = 1$

107	42		q
1	0	107	
0	1	42	2
1	-2	23	1
-1	3	19	1
2	-5	4	4
-9	23	3	1
→ 11	-28	1	3
	↑	0	

$11 \cdot 107 - 28 \cdot 42 = 1$

in $\mathbb{Z}_p$ $\quad \cancel{11 \cdot 0} + 79 \cdot 42 = 1$

$42^{-1} = 79$ in $\mathbb{Z}_{107}$