VU Network Security Advanced Topics
Lecture 1

Introduction

Tanja Zseby
TU Wien

WS 2018/19

institute of telecommunications

TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

Administrative Issues

Administrative Issues

Module Communication Networks

- WS: VO Communication Networks 1
- SS: VU Communication Networks 2

Module Network Security

- SS: VU Network Security
- **WS: VU Network Security Advanced**
- SS: SE Communication Networks Seminar

VU Network Security – Advanced Topics

- Type: Lecture and Lab Exercise, 2.0 SWS, ECTS: 3.0
- Room: EI 4 Reithoffer HS, Language: English
- Time: Wednesdays, **14:15 – 15:45**
  - Next week (10.10.): 14:00-15:00
- Lab times:
  - Group A: Wednesdays 14:00 – 17:00
  - Group B: Thursdays 14:00 -17:00
- Evaluation
  - Written exam (Theory)
  - Lab Report
  - Lab Review
- Contact: *netsec-lab@tuwien.ac.at*
- Register in TISS !

Written Exam (Theory)

- Prerequisite for Lab registration !!

  MUST pass exam to attend lab

- Exam Date: Wed. **21.11.2018,** 14:00-15:00, EI4
- Alternative: Fri. 23.11.2018, 17:00-18:00, EI2
  - For those who cannot attend 21.11.

- Need to select **one** exam date
  - Those failed on 21.11. can **NOT** repeat on 23.11
  - Exams only valid for this semester
- Failed Exam ➔ failed VU (Grade “5”)

Course Overview

Topics

- Crypto Methods: CRT-RSA, Elgamal
- IPv6 Security
- Routing Security
  - BGP, MANETs
- Smart Grid Security
  - Smart Metering
  - Wide area monitoring
  - Signatures, Secure Group Communication
- Network Steganography
  - Covert Channels
  - Subliminal Channels
- Lab on Network Steganography

Lab: Network Steganography

- Groups of 2 participants
  - Check for potential partner today
- Lab Times: every group get fixed slot
  - Wednesdays 14:00-17:00 (start 28.11.)
  - **OR** Thursdays 14:00-17:00 (start 29.11.)
  - Free slots can be used by others
- Lab Introduction ➔ **28./29.11.2018**
  - Exercise sheets
  - Team assignment

- Be **on time** at first lab !!
  - If late ➔ will be assigned to team or work alone

Schedule (tentative)

T 1	03.10.2018	Theory: Introduction, Recap, Ext. Euclidean
T 2	10.10.2018	Theory: CRT, Elgamal
	17.10.2018	No lecture
T 3	24.10.2018	Theory: IPv6 Security
T 4	31.10.2018	Theory: Routing Security, MANET Security
T 5	7.11.2018	Theory: Smart Grid Security, Secure Group Communication
T 6	14.11.2018	Theory: Network Steganography
E 1	Wed 21.11.	14:00-15:00 Exam, room EI4
E2	Fr 23.11.	17:00 -18:00 Exam (Alternative), room EI2
L0	28.11./29.11.	Lab Intro (Wed/Thu group) in NetSec Lab
L1	5.12./6.12.	1st exercise (Wed/Thu group) in NetSec Lab
L2	12.12./13.12.	2nd exercise (Wed/Thu group) in NetSec Lab
L3	19.12./14.12.	3rd exercise (Wed/Thu group) in NetSec Lab
L4	9.1./10.1.	4th exercise (Wed/Thu group) in NetSec Lab
L5	16.1./17.1.	5th exercise (Wed/Thu group) in NetSec Lab
R	21.1.-25.1.	Lab Reviews, CG0506
D	30.1.	Lab Discussion, EI4

Participants

- Which Master?
- Background?
  - NetSec last semester?
  - VO Communication Networks?
  - VO Datenkommunikation?

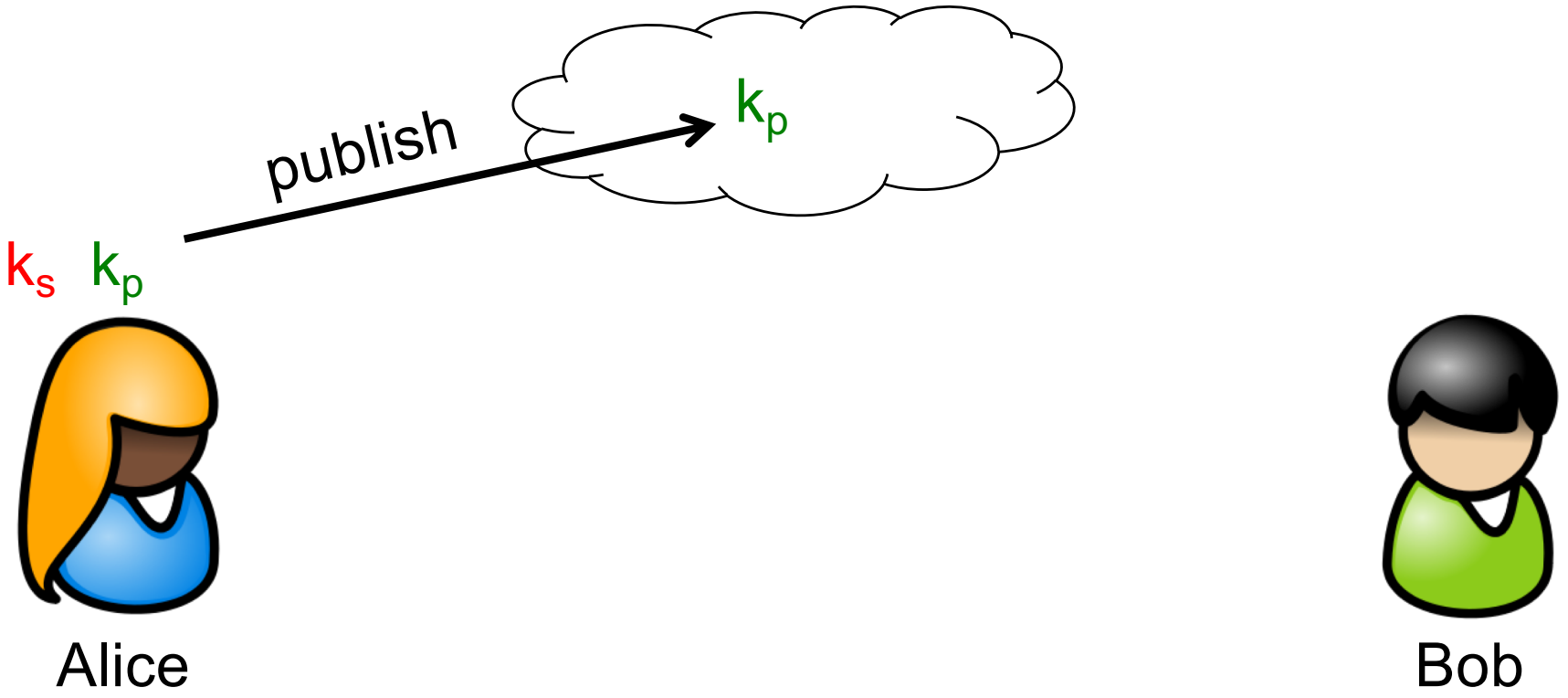
Outline Today

- Recap Algorithms
  - Asymmetric Cryptography
  - RSA

- Extended Euclidean Algorithm
  - Calculating an Inverse for RSA

Recap: Asymmetric Cryptography

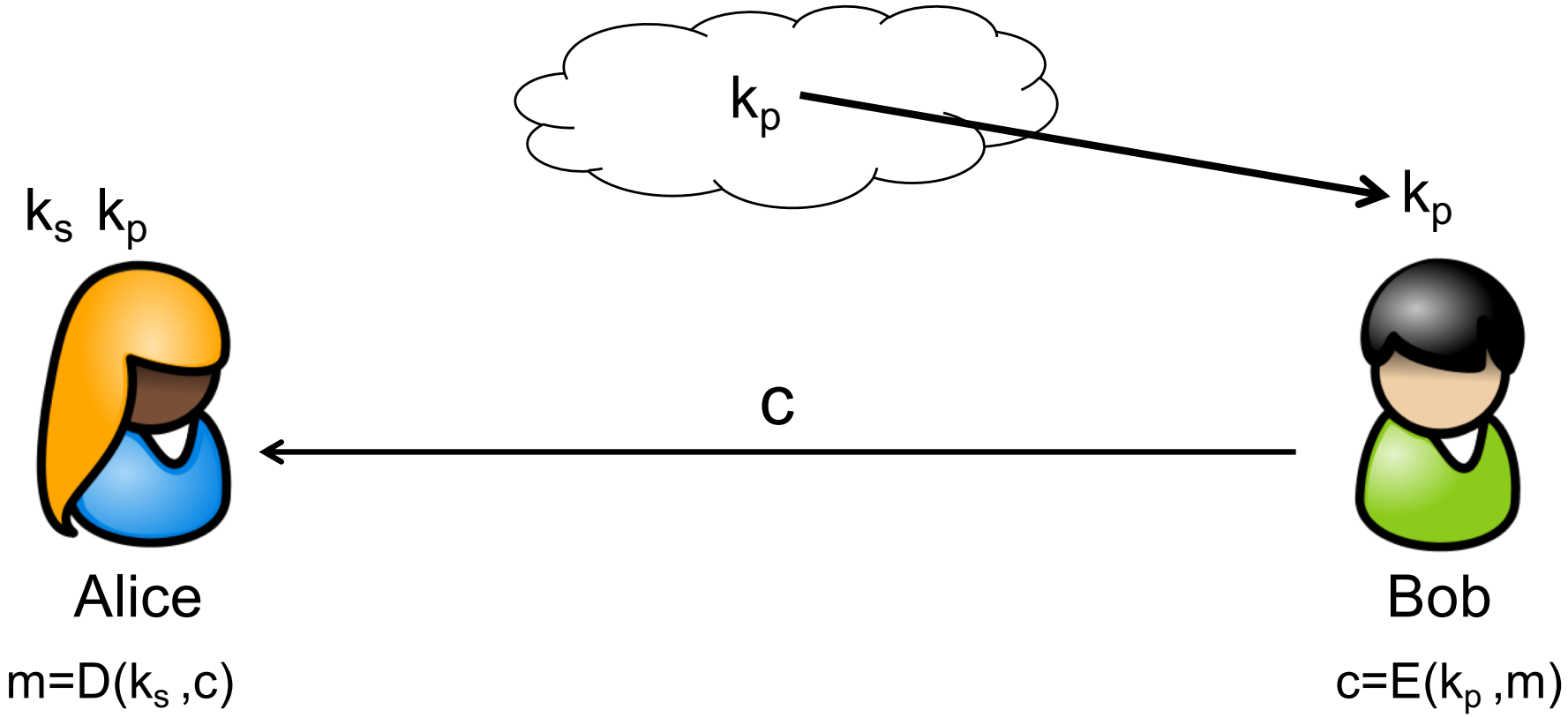
Asymmetric Cryptography



Public/private Keypair

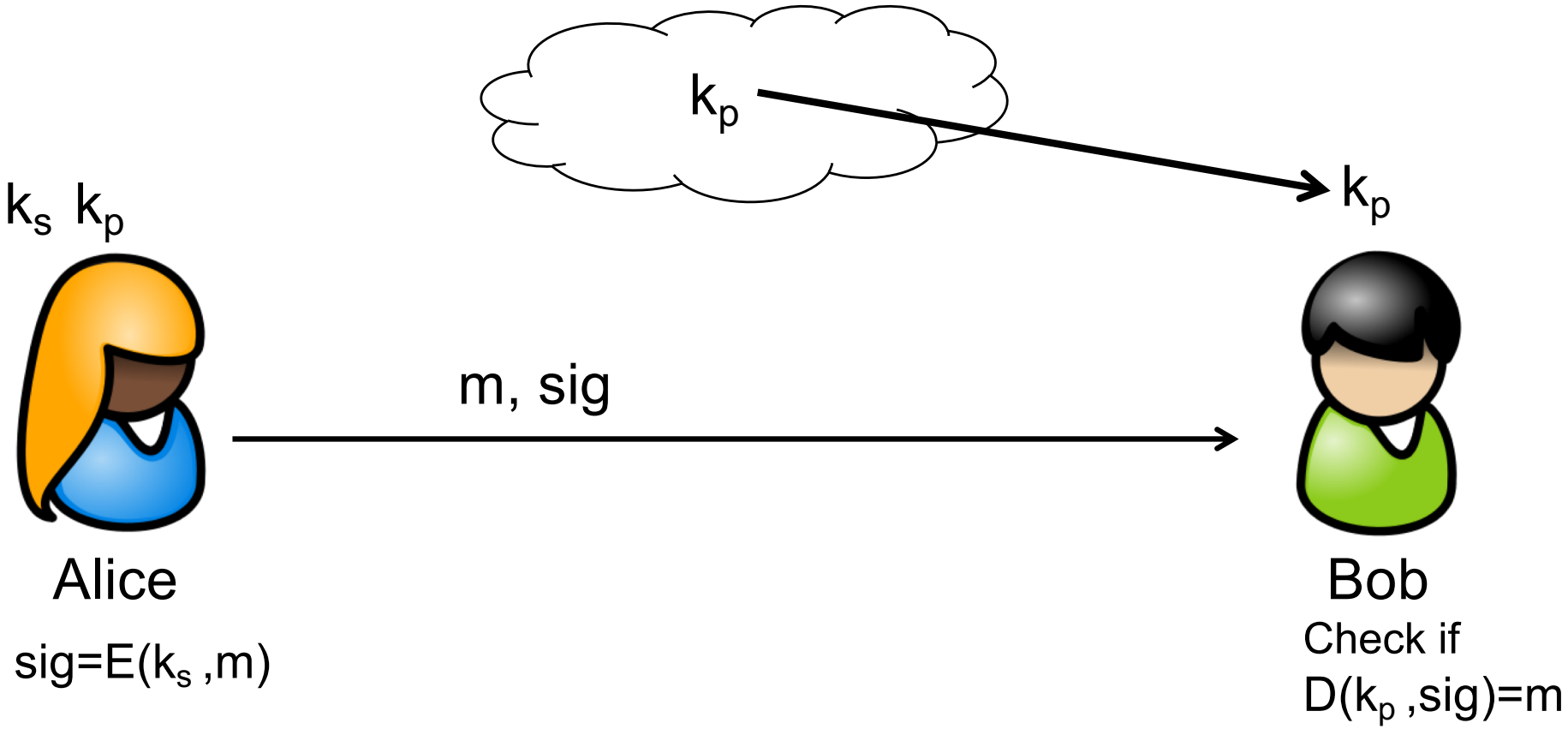
- k_s private key ➔ secret!
- k_p public key

Encryption



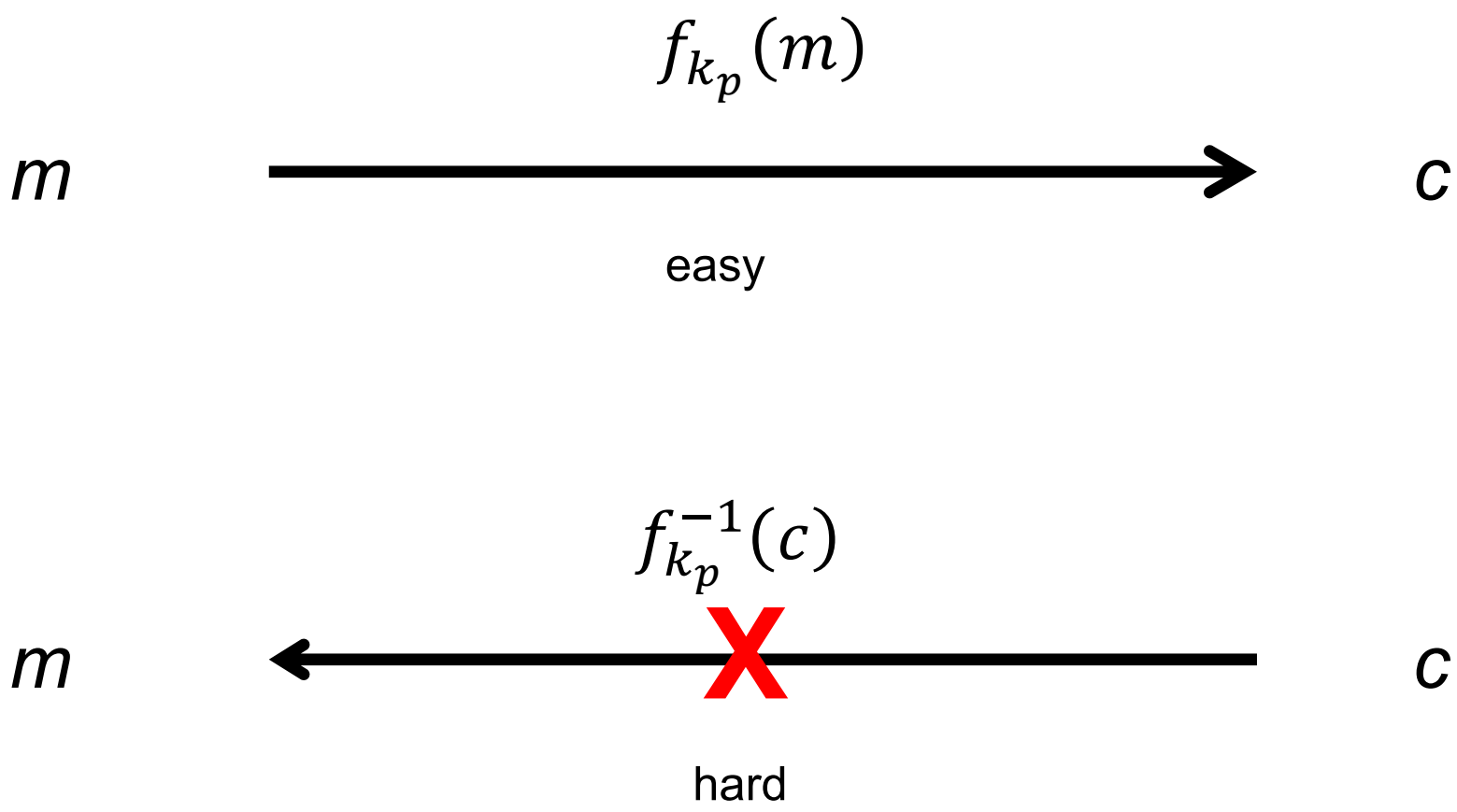
- Bob encrypts message with Alice‘s public key
- Alice decrypts message with her private key

Digital Signature



- Alice‘s signature: Message (or hash) encrypted with k_s
- Bob verifies signature with Alice‘s public key
- Only Alice can create valid signature
- ➔ Proof that message from Alice

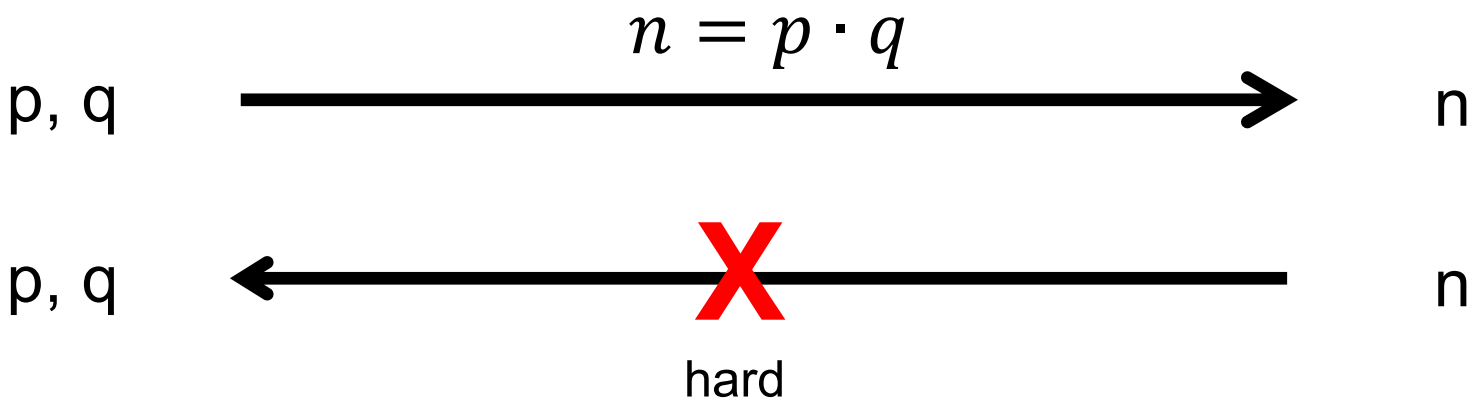
One-Way Function



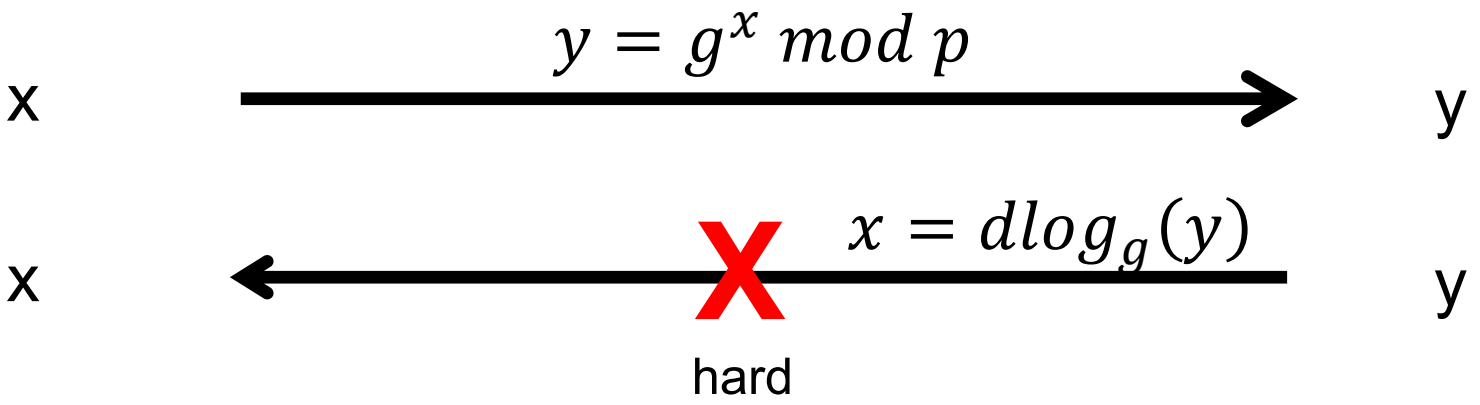
Candidates

- Prime factorization for large integers

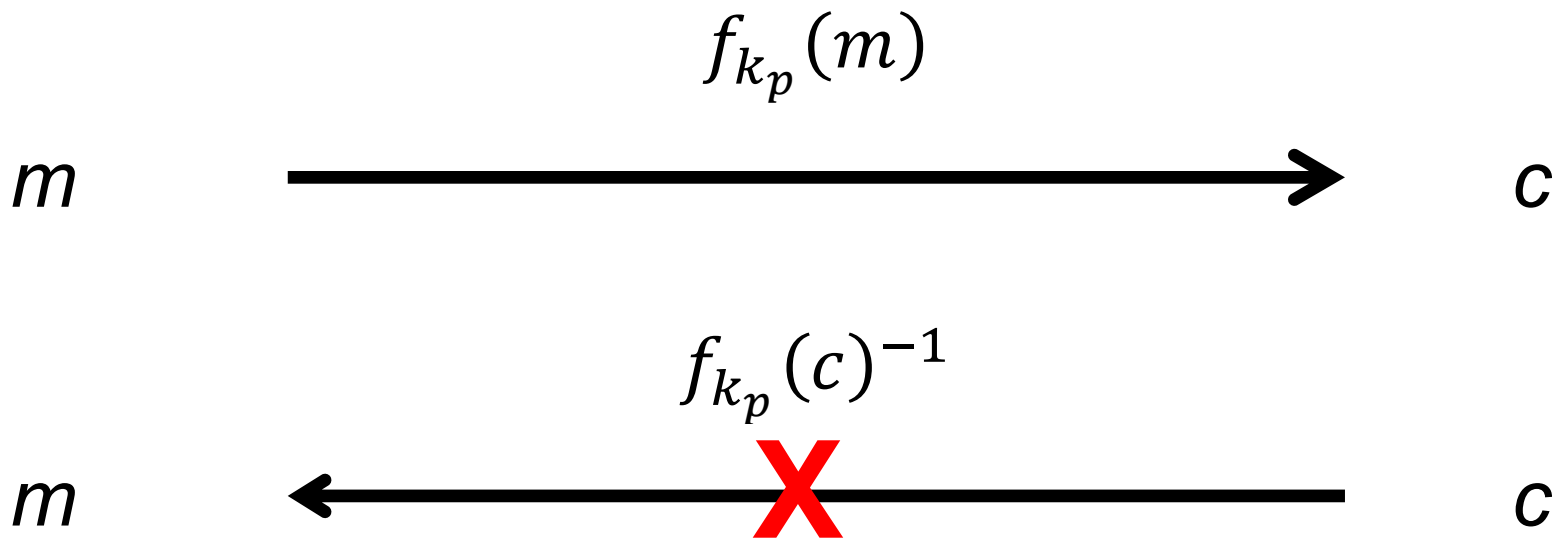
large primes



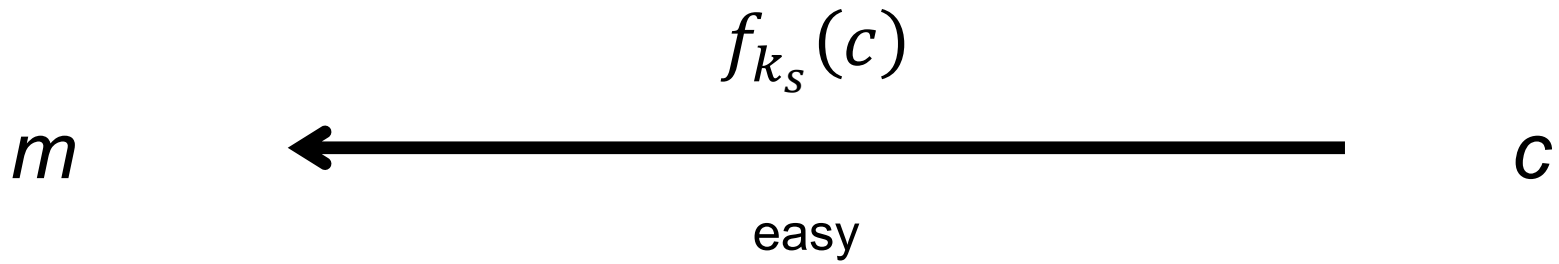
- Discrete Logarithm



Trapdoor Function



If additional Information k_s known:



Recap: RSA Encryption*

Choose large primes p, q
Compute n $n = p \cdot q$
Compute $\varphi(n)$
Choose e coprime to $\varphi(n)$
Find Inverses d (trapdoor)

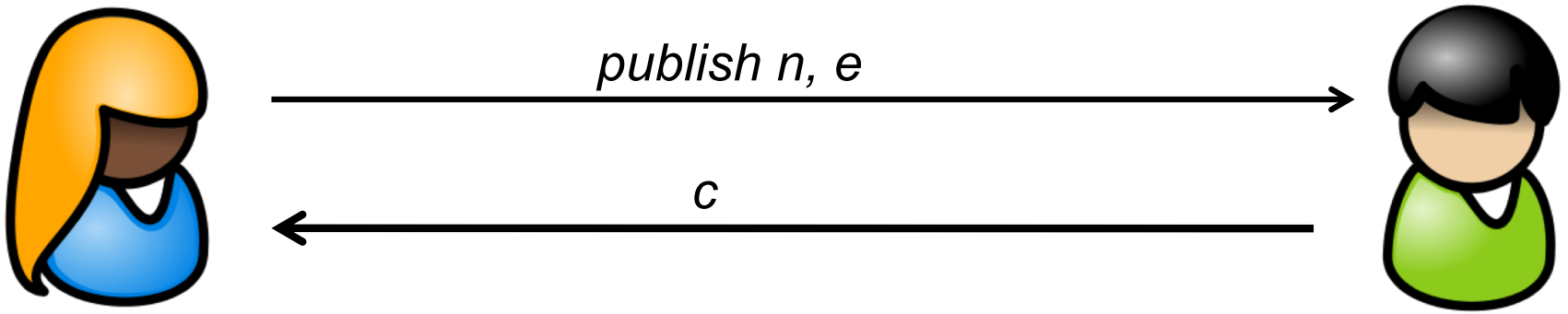
$$e \cdot d \equiv 1 \, mod \, \varphi(n)$$

Decryption with private key (Trapdoor d)

$$m = c^d \, mod \, n$$

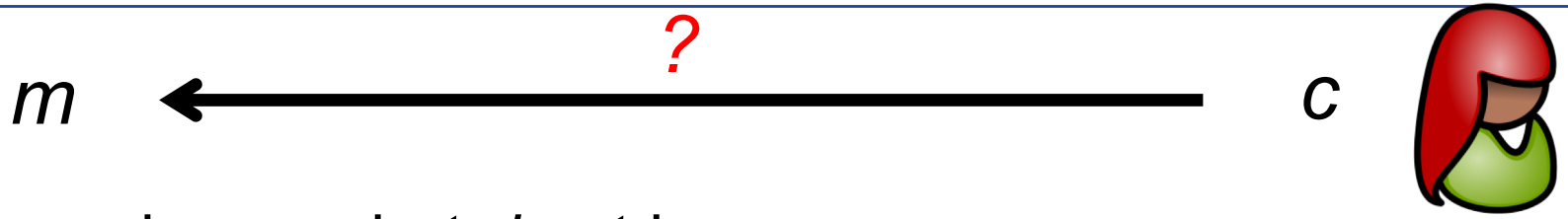
Message *m*
Encrypt with Alice's public key *e*

$$c = m^e \, mod \, n$$



* **Attention!** The pure application of RSA Trapdoor function shown here is **not secure**.
➔ a slightly modified method is used in practice.

RSA Encryption



c, n, e known, but *d* not known:

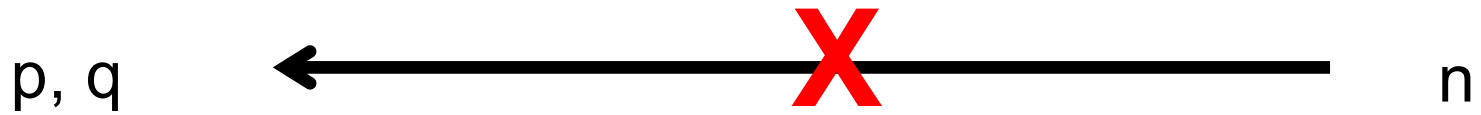
$$m = c^{d} \bmod n$$

Find d? $e \cdot d \equiv 1 \bmod \varphi(n)$

Find $\varphi(n)$? $\varphi(n) = (p-1) \cdot (q-1)$

d,p,q, $\varphi(n)$ must remain secret!!

➔ Prime faktorization for large integers: One-way Funktion



Recap: RSA Signature*

Choose p, q
Compute n $n = p \cdot q$
Compute $\varphi(n)$
Choose e coprime to $\varphi(n)$
Find inverses d (trapdoor)

$$e \cdot d \equiv 1 \, mod \, \varphi(n)$$

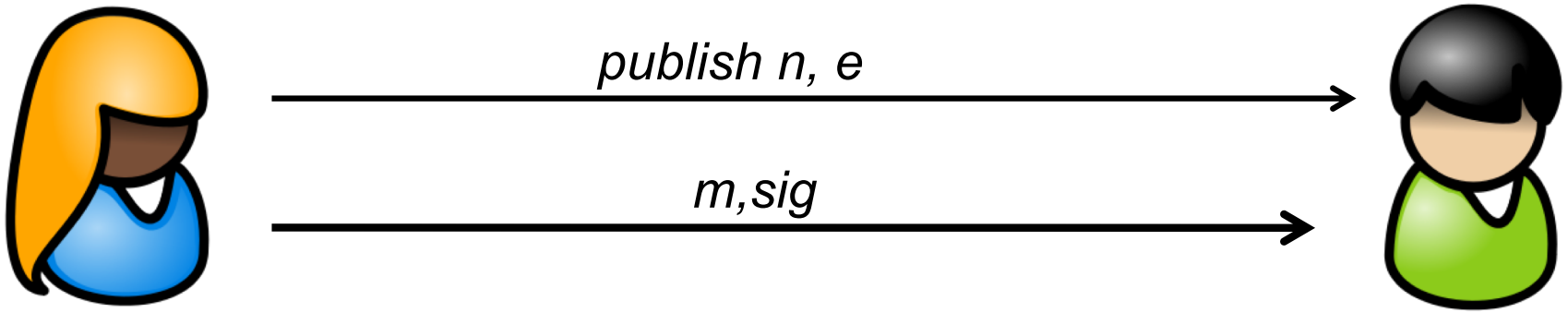
Sign with private key (Trapdoor d)

$$sig = m^d \, mod \, n$$

Verify with Alice's public key e

$$\hat{m} = sig^e \, mod \, n$$

$$\hat{m} \overset{?}{=} m$$



* **Attention!** The pure application of RSA Trapdoor function shown here is **not secure**.
➔ a slightly modified method is used in practice.

RSA: How to find the inverse d?

$$e \cdot d \equiv 1 \, mod \, \varphi(n)$$

Recap: Multiplicative Inverse

- $\mathbb{Z}_n$ set of integers mod n

$$\mathbb{Z}_{10} = \{0,1,2,3,4,5,6,7,8,9\}$$

- Multiplicative Inverse

$$x \cdot x^{-1} \equiv 1 \ mod\ n$$

- Inverse x^{-1} exists if x **relative prime** (coprime) to n
  - Greatest common divisor gcd(n,x) =1
  - Example: n=10 ➔ 1,3,7,9

- $\mathbb{Z}_n^*$ set of integers relative prime to n

$$\mathbb{Z}_{10}^* = \{1,3,7,9\}$$

x	x^{-1}	$x \cdot x^{-1}$	Remainder
1	1	1	1
3	7	21	1
7	3	21	1
9	9	81	1

Calculating the Inverse

- e is selected as coprime to $\varphi(n)$

➔ multiplicative inverse d exists

$$e \cdot d \equiv 1 \quad mod\ \varphi(n)$$

Euclidean Algorithm

Finding gcd(a,b)

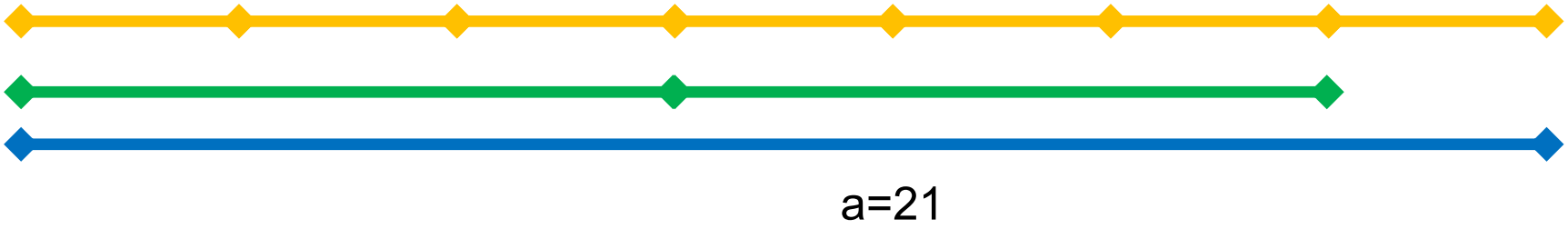
Euclidean Algorithm Example 1: a=21, b=9

$$\frac{a}{b} = q_0 \quad remainder\ r_0 \qquad a = q_0\, b + r_0$$

$$\frac{21}{9} = 2\ remainder\ 3 \qquad 21 = 2 \cdot 9 + 3$$

$$b = q_1\, r_0 + r_1 \qquad 9 = 3 \cdot 3 + 0$$

➔ gcd (21,9) =3



Euclidean Algorithm Example 2: a=113, b=25

1. Calculate gcd

a=113, b=25

$$a = q_0\, b + r_0 \qquad 113 = 4 \cdot 25 + 13$$

$$b = q_1\, r_0 + r_1 \qquad 25 = 1 \cdot 13 + 12$$

$$r_0 = q_2\, r_1 + r_2 \qquad 13 = 1 \cdot 12 + 1$$

$$r_1 = q_3\, r_2 + r_3 \qquad 12 = 12 \cdot 1 + 0$$

...

$$r_{k-2} = q_k\, r_{k-1} + r_k$$

$$r_{k-1} = q_{k+1}\, r_k + 0$$

➔ gcd (113,25) =1

➔ Multiplicative Inverse exists

Euclidian Algorithm (Table Form): Calculating gcd

$$a = q \cdot b + r$$

a=113, b=25

$$113 = 4 \cdot 25 + 13$$

$$25 = 1 \cdot 13 + 12$$

$$13 = 1 \cdot 12 + 1$$

$$12 = 12 \cdot 1 + 0$$

i	a_i	b_i	q_i
0	113	25	4
1	25	13	1
2	13	12	1
3	12	1	12
4	1	0	

$$a = q_0\, b + r_0$$

gcd(113,25)=1

Extended Euclidean Algorithm

Finding the multiplicative Inverse

Extended Euclidean Algorithm

- Goal: find gcd and find s,t who solve the equation

$$\gcd(a, b) = a \cdot s + b \cdot t$$ **Bézout's identity**

- If a, b co-primes:
  - gcd(a,b)=1 (since co-primes)

$$1 = a \cdot s + b \cdot t$$

Finding the Inverse

Use Extended Euclidian Algorithm
to find s,t who solve the equation:

$$a \cdot s + b \cdot t = 1$$

Then:

$$1 \equiv a \cdot s \mod b$$ ➔ s is inverse of a mod b

$$1 \equiv b \cdot t \mod a$$ ➔ t is inverse of b mod a

! We look for the Inverse **in** Z_n ➔ may need to add/substract

Calculate Bézout Coefficients

$$a = q_0\, b + r_0 \qquad r_0 = a - q_0\, b$$

$$b = q_1\, r_0 + r_1 \qquad r_1 = b - q_1\, r_0$$

$$r_0 = q_2\, r_1 + r_2 \qquad r_2 = r_0 - q_2\, r_1$$

$$r_1 = q_3\, r_2 + 0 \qquad \gcd(a, b) = r_2$$

$$r_1 = b - q_1\,(a - q_0\, b) = -q_1\, a + (1 + q_0\, q_1\,)b$$

$$r_2 = (a - q_0\, b) - q_2\,(-\,q_1\, a + (1 + q_0\, q_1\,)b)$$

➔ gcd as linear combination of a and b:

$$\gcd(a, b) = \underbrace{\boxed{(1 + q_1\, q_2\,)}}_{s}\, a + \underbrace{\boxed{(-q_2 - q_0\, q_1\, q_2 - q_0)}}_{t}\, b$$

Getting the Inverse

s t

$$\gcd(a,b) = (1 + q_1\, q_2\,)\, a + (-q_2 - q_0\, q_1\, q_2 - q_0)\, b$$

Inverse for a:

$$1 \equiv a \cdot s \mod b$$

$$1 \equiv a \cdot (1 + q_1\, q_2\,) \mod b$$

Check if s in Z_b:

$$if \quad s \notin \mathbb{Z}_b \rightarrow \mathrm{s} := \mathrm{s} + \mathrm{b}$$

Example

a=113, b=25

$$113 = 4 \cdot 25 + 13 \qquad q_0 = 4$$

$$25 = 1 \cdot 13 + 12 \qquad q_1 = 1$$

$$13 = 1 \cdot 12 + 1 \qquad q_2 = 1$$

$$12 = 12 \cdot 1 + 0 \qquad q_3 = 12$$

$$\gcd(a,b) = (1 + q_1\, q_2)\, a + (-q_2 - q_0\, q_1\, q_2 - q_0)\, b$$

$$1 = 2\, a - 9\, b = 226 - 225$$

Extended Euclidean Algorithm – Table Form

1. Calculate gcd (a,b)

$$a = q \cdot b + r$$

a=113, b=25

$$113 = 4 \cdot 25 + 13$$

$$25 = 1 \cdot 13 + 12$$

$$13 = 1 \cdot 12 + 1$$

$$12 = 12 \cdot 1 + 0$$

i	a_i	b_i	q_i	s_i	t_i
0	113	25	4		
1	25	13	1		
2	13	12	1		
3	12	1	12		
4	1	0			

gcd(113,25)=1

2.Calculate Bézout Coefficients: s, t

- Calculate Bézout coefficients s, t

$$gcd = s \cdot a + t \cdot b$$

$1 = 2 \cdot a - 9 \cdot b$

i	a_i	b_i	q_i	s_i	t_i
0	113	25	4	2	-9
1	25	13	1	-1	2
2	13	12	1	1	-1
3	12	1	12	0	1
4	1	0		1	0

$s_i = t_{i+1} \quad t_i = s_{i+1} - q_i \cdot t_{i+1}$

$s_4 = 1,\ t_4 = 0$

- Bézout's Identity valid at each row

3. Getting the Inverse for a (mod b)

$$gcd=1 \rightarrow 1=s \cdot a+t \cdot b$$

s is inverse for *a mod b*

$$\boxed{1 \equiv a \cdot s \mod b}$$

➔ *s* is inverse for *a mod b*

For RSA: check if s in Z_b:

$$if \quad s \notin \mathbb{Z}_b \rightarrow s := s + b$$

Getting the Inverse for a (mod b)

$$1 = a \cdot s + b \cdot t \qquad 1 = 113 \cdot 2 - 25 \cdot 9$$

$$1 \equiv a \cdot s \mod b \qquad 1 \equiv 113 \boxed{2} \mod 25$$

Set of Integers modulo 25: $\mathbb{Z}_{25} = \{0,1,2,3,4, \ldots ,24\}$

$$2 \in \mathbb{Z}_{25}$$

➔ 2 is multiplicative inverse of 113 mod 25

Getting the Inverse for b (mod a)

$$1 = a \cdot s + b \cdot t \qquad 1 = 113 \cdot 2 - 25 \cdot 9$$

$$1 \equiv b \cdot t \mod a \qquad 1 \equiv 25 \cdot (-9) \mod 113$$

Set of Integers modulo 113: $\mathbb{Z}_{113} = \{0,1,2,3,4, \ldots ,112\}$

$$-9 \notin \mathbb{Z}_{113} \quad \rightarrow \quad -9 + 113 = 104$$

$$104 \in \mathbb{Z}_{113}$$

➔ 104 is multiplicative Inverse of 25 mod 113

RSA Example

RSA

Choose large primes p, q
Compute n $n = p \cdot q$
Compute $\varphi(n)$
Choose e coprime to $\varphi(n)$
Find Inverses d (trapdoor)

Calculate $\varphi(n)$:

$$\varphi(n) = (p-1) \cdot (q-1)$$

Inverse:

$$e \cdot d \equiv 1 \, mod \, \varphi(n)$$

Calculating the multiplicative Inverse: RSA Example

- Choose prime numbers p=3, q=11 ➔ n=33

$$n = p \cdot q = 3 \cdot 11 = 33$$

$$\varphi(n) = (p-1) \cdot (q-1) = 2 \cdot 10 = 20$$

- Select e coprime to $\varphi(n)$

  e=7

- Find inverse d

$$e \cdot d \equiv 1 \; mod \; \varphi(n)$$

$$7 \cdot d \equiv 1 \;\; mod \; 20$$

1. Calculate gcd

$$a = q \cdot b + r$$

$\varphi(n)$ e

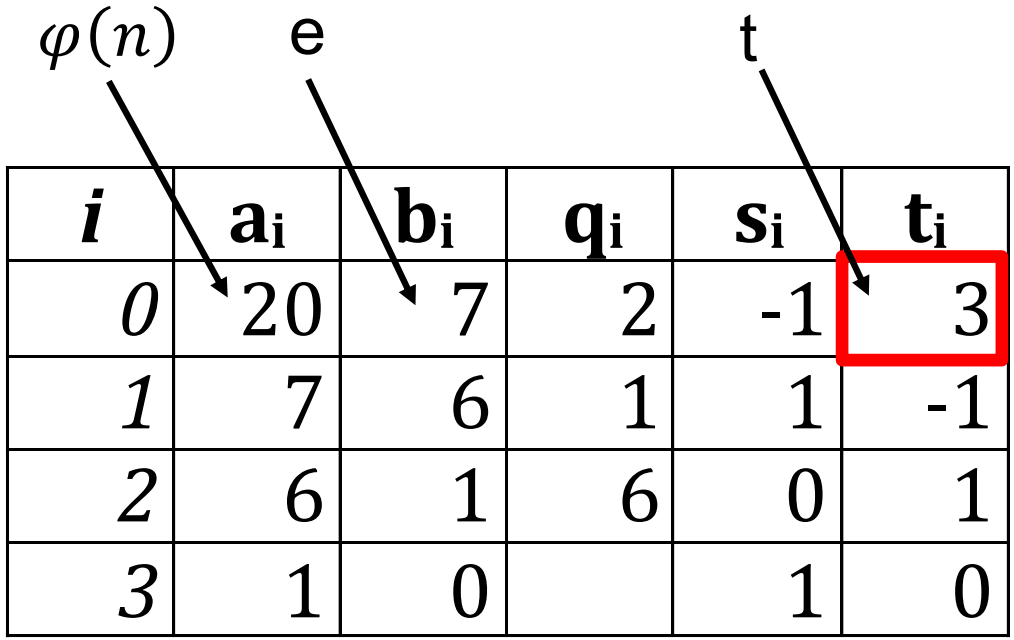
i	a_i	b_i	q_i	s_i	t_i
0	20	7	2		
1	7	6	1		
2	6	1	6		
3	1	0			

$$\gcd(20, 7) = 1$$

Remark: In RSA e is chosen as co-prime to $\varphi(n)$ ➔ already known that gcd=1

2. Calculate Bézout Coefficients

$$\gcd(\varphi(n), e) = \varphi(n) \cdot s + e \cdot \boldsymbol{t}$$



i	a_i	b_i	q_i	s_i	t_i
0	20	7	2	-1	3
1	7	6	1	1	-1
2	6	1	6	0	1
3	1	0		1	0

$$1 = \varphi(n) \cdot (-1) + e \cdot \mathbf{3}$$

$s_i = t_{i+1}$ $t_i = s_{i+1} - q_i \cdot t_{i+1}$

$s_3 = 1$, $t_3 = 0$

3. Check if t=3 in $\mathbb{Z}_{\varphi(n)}$

➔ *Private key* $d=t=3$

Alternative: Using Euler's Theorem

Alternative: Using Euler's Theorem

- If x and n are relatively prime

$$x^{\varphi(n)} \equiv 1 \quad mod\ n$$ **Euler's Theorem**

- Example n=10, x=3:

$$\varphi(n) = \varphi(2 \cdot 5) = (2-1) \cdot (5-1) = 4$$

$$x^{\varphi(n)} = 3^4 = 81$$

$$81 \equiv 1 \quad mod\ 10$$

Euler's Theorem

- Calculate an inverse

$$x^{\varphi(n)} \equiv 1 \quad mod\ n$$

$$x^{\varphi(n)} \cdot x^{-1} \equiv x^{-1} \quad mod\ n$$

$$x^{\varphi(n)-1} \equiv x^{-1} \quad mod\ n$$

But:

- Slower than extended Euclidean

RSA Example

- Choose prime numbers p=3, q=11 ➔ n=33

$$n = p \cdot q = 3 \cdot 11 = 33$$

$$\varphi(n) = (p-1) \cdot (q-1) = 2 \cdot 10 = 20$$

- Select e coprime to $\varphi(n)$ ➔ e=7
- Find inverse d $e \cdot d \equiv 1 \; mod \; \varphi(n)$

e=7, $\varphi(n) = 20$

$$x^{-1} \equiv x^{\varphi(\varphi(n))-1} \; mod \; \varphi(n)$$

Calculation only possible if prime factorization known

$$\varphi(\varphi(n)) = \varphi(20) = \varphi(5) \cdot \varphi(2^2) = (5-1) \cdot (2^2 - 2^1) = 8$$

$$x^{\varphi(\varphi(n))-1} = 7^{8-1} = 823543$$

Rule: $\varphi(p^k) = (p^k - p^{k-1})$

$$823543 \equiv 3 \; mod \; 20$$ ➔ *d=3*

Summary

- RSA parameters
  - Prime numbers: p, q ➔ $n = p \cdot q$
  - Calculate $\varphi(n) = (p-1) \cdot (q-1)$

- Select e as coprime to $\varphi(n)$
  - Coprime ➔ $\gcd\left(e, \varphi(n)\right) = 1$
  - gcd calculated with Euclidean Algorithm (table)

- Calculate multiplicative inverse d
  - Using Bézout's Identity (table)

$$\gcd(\varphi(n), e) = \varphi(n) \cdot s + e \cdot \boldsymbol{t}$$

  - Check if $t \in \mathbb{Z}_{\varphi(n)}$ ➔ Inverse d=t

Thank you!