

## *Exercise 2 - Cryptography*



Mobile Business II (SS 2023)

Dr. Ahad Niknia

Chair of Mobile Business and Multilateral Security  
Goethe University Frankfurt a. M.

## Exercise 1: Caesar Cipher

- Decrypt the following word, encrypted with the Caesar cipher:

JYFWAVNYHWOF

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

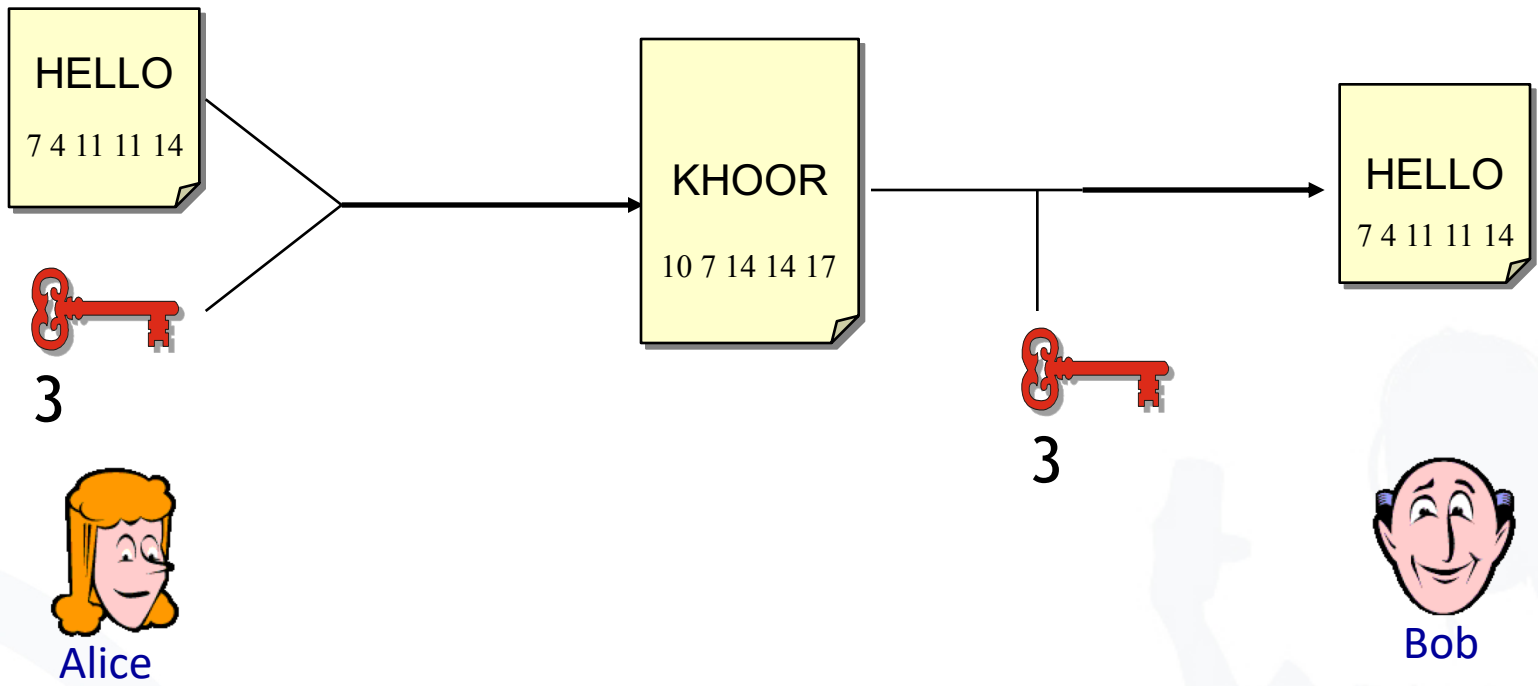
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- We assign a number for every character.
- This enables us to calculate with letters as if they were numbers.

- Encryption:
  1. Assign numbers to characters (A=0, B=1,...)
  2. Choose key  $k$  (0,..., 25)
  3. Compute  $(\text{num}(\text{char}) + k) \bmod 26$ , where char is the character to encrypt and  $\text{num}(x)$  the number assigned to character  $x$  (e.g.  $\text{num}(A) = 0$ )

- How to decrypt?
- Decryption:
  1. Choose key  $k$  (0,..., 25)
  2. Assign numbers to characters (A=0, B=1,...)
  3. Compute  $(\text{num}(\text{char}) - k) \bmod 26$ , where  $\text{char}$  is the character to encrypt and  $\text{num}(x)$  the number assigned to character  $x$
  4. Repeat steps for all characters
  5. Stop, if decrypted word makes sense

# Caesar Cipher: Example



- Let's try:

Key	J	Y	F	W	A	V	N	Y	H	W	O	F
1	I	X	E	V	Z	U	M	X	G	V	N	E
2	H	W	D	U	Y	T	L	W	F	U	M	D
3	G	V	C	T	X	S	K	V	E	T	L	C
4	F	U	B	S	W	R	J	U	D	S	K	B
5	E	T	A	R	V	Q	I	T	C	R	J	A
6	D	S	Z	Q	U	P	H	S	B	Q	I	Z
7	C	R	Y	P	T	O	G	R	A	P	H	Y

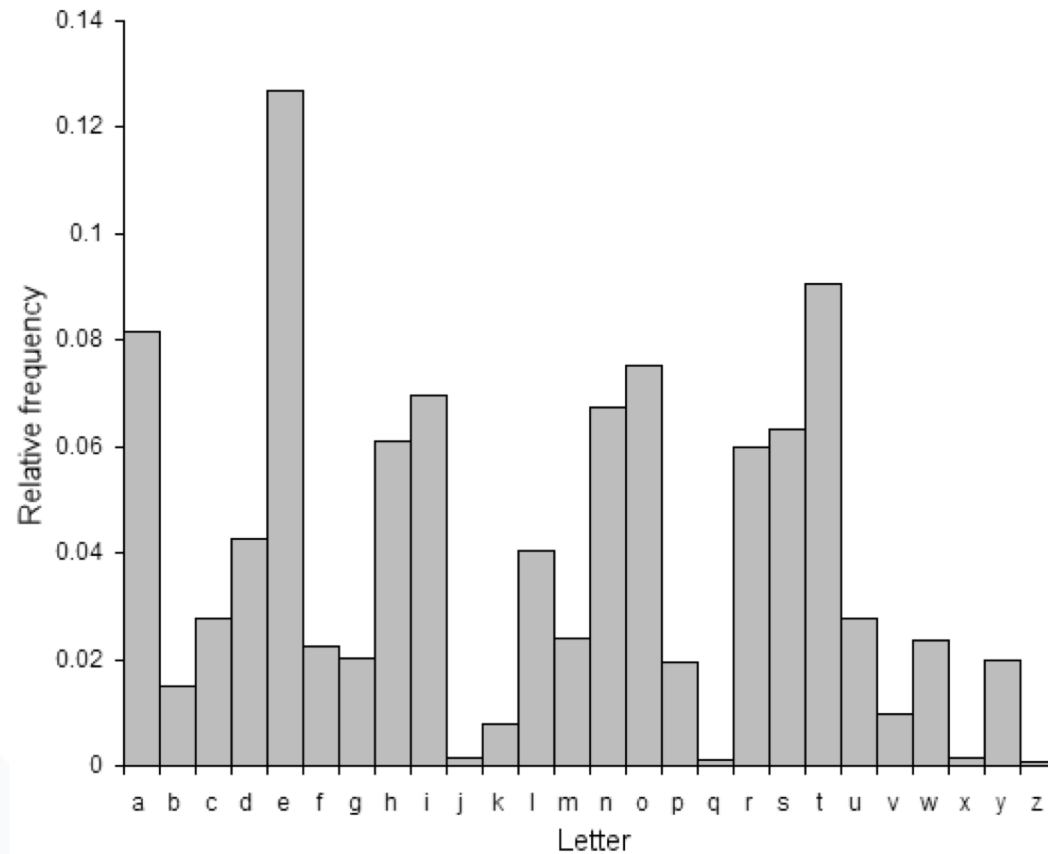
- Very simple form of encryption.
- The encryption and decryption algorithms are very easy and fast to compute.
- It uses a very limited key space ( $n=26$ )
- Therefore, the encryption is very easy and fast to compromise.



pelcgbtencul cevbe gb gur zbqrea ntr jnf rssrpgviryl flabalzbhf jvgu rapelcgvba, gur pbairefvba bs vasbezngvba sebz n ernqnoyr fgngv gb nccnerag abafrafr. gur bevtvangbe bs na rapelcgrq zrffntr funerq gur qrpqbvat grpuavdhr arrqrq gb erpbire gur bevtvany vasbezngvba bayl jvgu vagraqr erpvcvragf, gurrol cerpyhqvat hajnagrq crefbaf gb qb gur fnzr. fvapr jbeyq jne v naq gur nqirag bs gur pbzchgre, gur zrgubqf hfrq gb pneel bhg pelcgybtl unir orpbzr vapernfvatyl pbzcyrk naq vgf nccyvpngvba zber jvqrfcernq. zbqrea pelcgbtencul vf urnivyl onfrq ba zngurzngvpy gurbel naq pbzchgre fpvrapr cenpgvpr; pelcgbtenculp nytbevguzf ner qrfvtarq nebhaq pbzchngvbany uneqarff nffhzcgvbaf, znxvat fhpu nytbevguzf uneq gb oernx va cenpgvpr ol nal nqirefnel. vg vf gurbergvpyl cbffvoyr gb oernx fhpu n flfgrz ohg vg vf vasrnfvoyr gb qb fb ol nal xabja cenpgvpy znaf. gurfr fpurzrf ner gurersber grezrq pbzchngvbanyyl frpher; gurbergvpy nqinapr, r.t., vzcebirzragf va vagtre snpgbevmngvba nytbevguzf, naq snfgre pbzchgvat grpuabybtl erdhver gurfr fbyhgubaf gb or pbagvahnyl nqncgrq. gurer rkvgf vasbezngvba-gurbergvpyl frpher fpurzrf gung cebinoyl pnaabg or oebxra rira jvgu hayvzvrq pbzchgvat cbjre-na rknzcyr vf gur bar-gvzr cnq-ohg gurfr fpurzrf ner zber qvssvphyg gb vzcyzrag guna gur orfg gurbergvpyl oernxnoyr ohg pbzchngvbanyyl frpher zrpunavfzf.



<http://nayuki.eigenstate.org/page/automatic-caesar-cipher-breaker-javascript>



English letters frequency

# Exercise 2: Cryptosystems

1. Imagine the following situation: Alice wants to share a secret with Bob and therefore sends an encrypted message to Bob.
  - 1.1 Sketch the process by using symmetric encryption/decryption.
    - a. Complete the illustration by highlighting each step and adding all missing elements – such as keys, involved 3<sup>rd</sup> parties,...



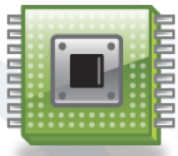
# Exercise 2: Cryptosystems - Symmetric Encryption



Alice



Bob



Key  
generator

Area of attack

Area of Trust

# Exercise 2: Cryptosystems - Symmetric Encryption



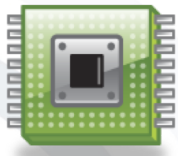
Alice



Bob



1. Generate key  $k$

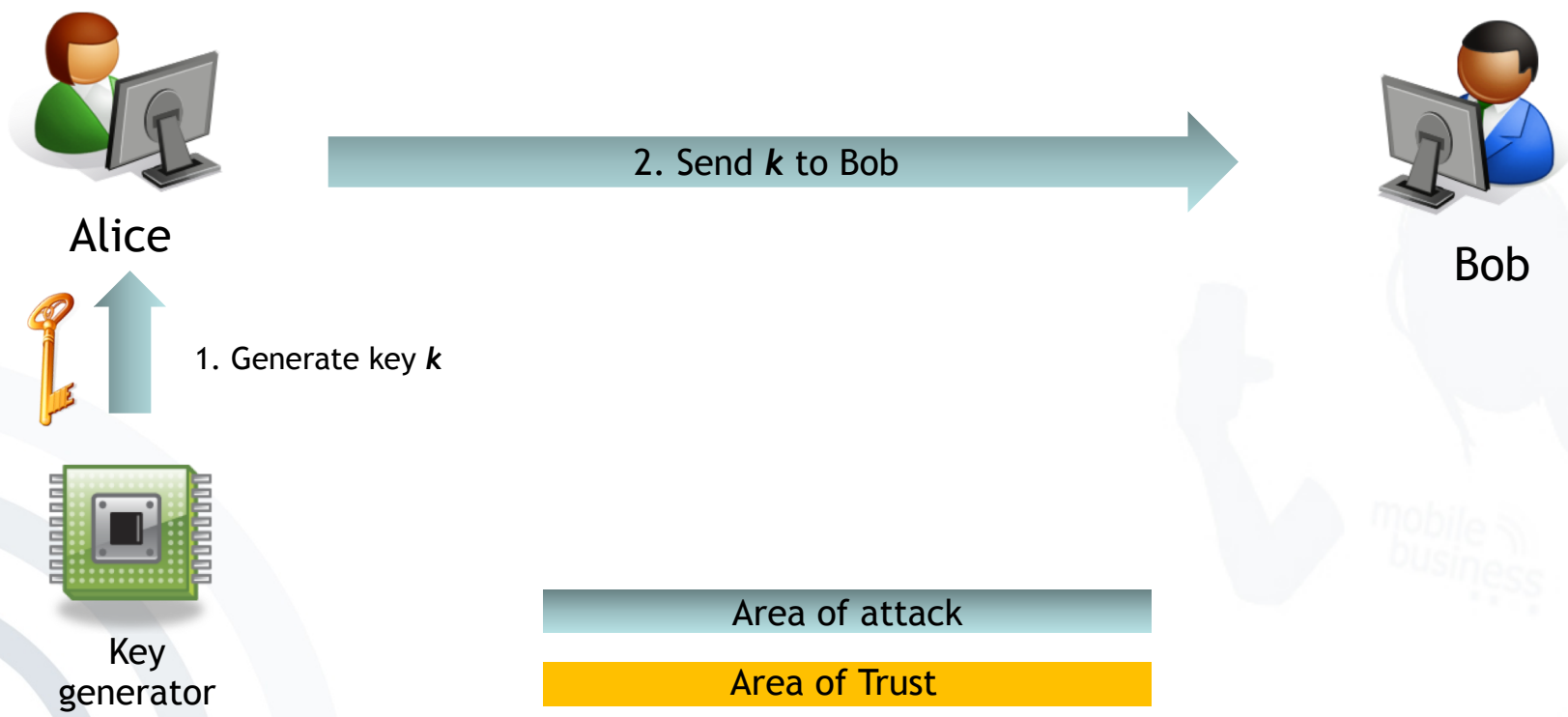


Key  
generator

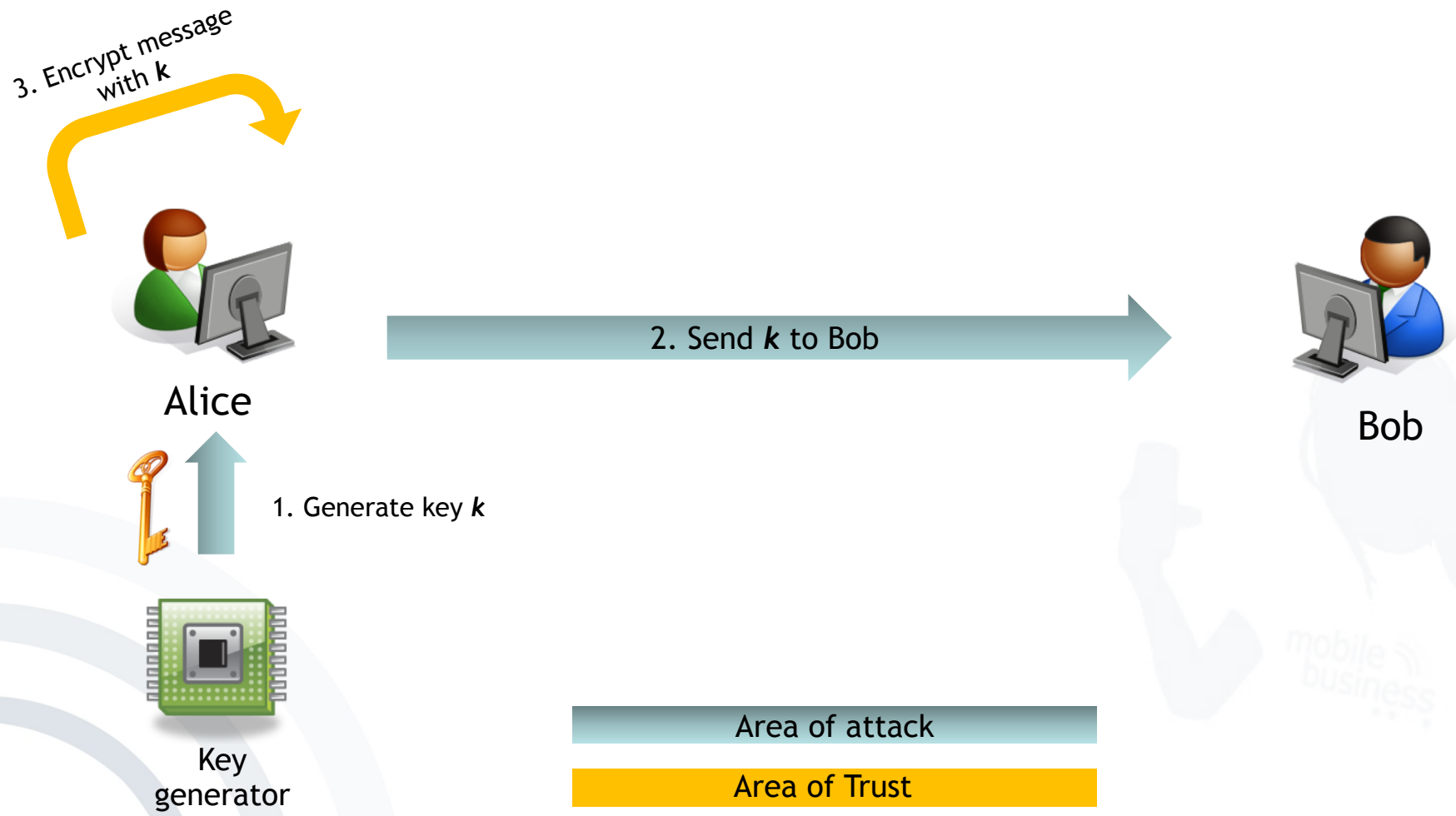
Area of attack

Area of Trust

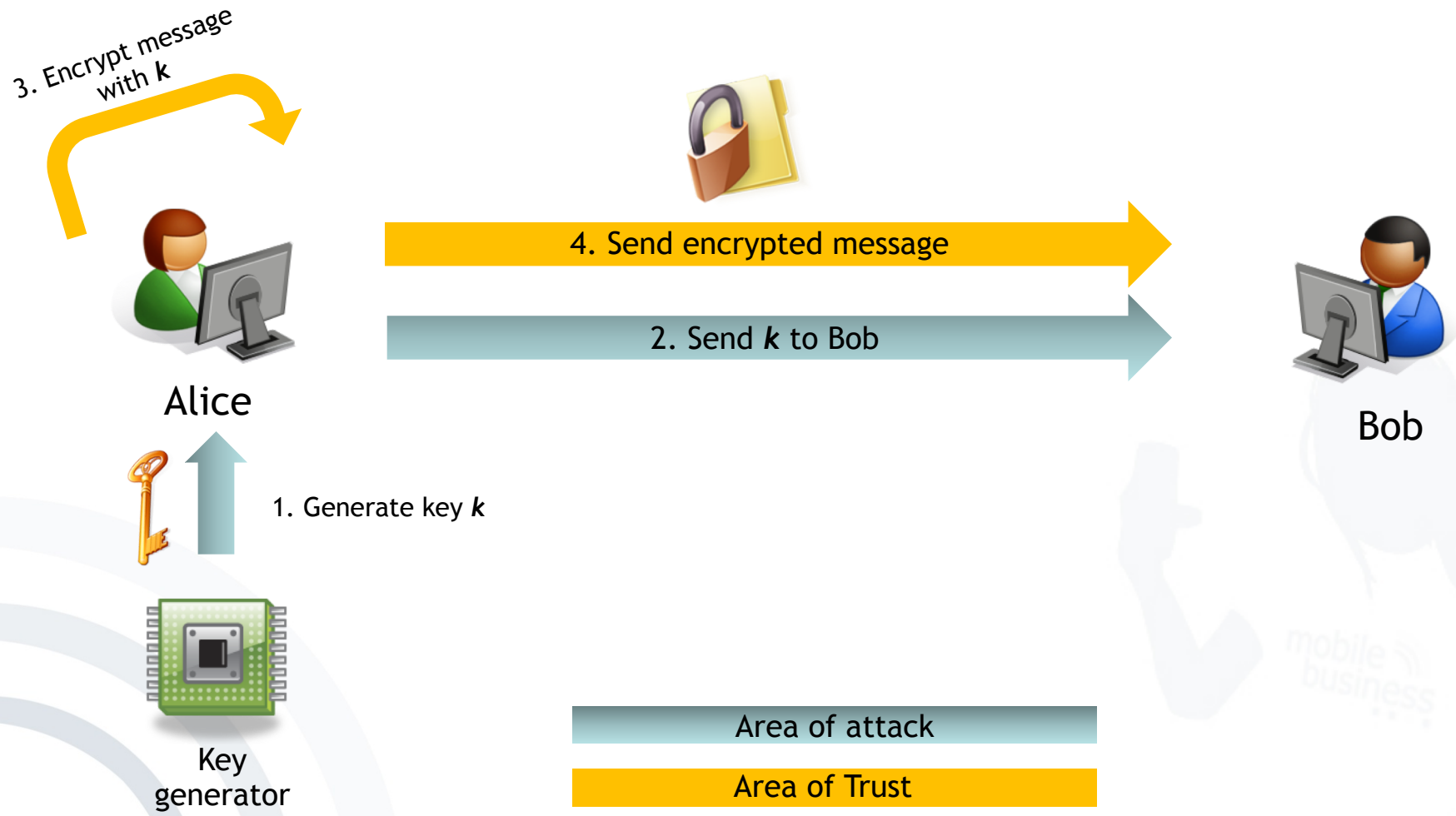
# Exercise 2: Cryptosystems - Symmetric Encryption



# Exercise 2: Cryptosystems - Symmetric Encryption

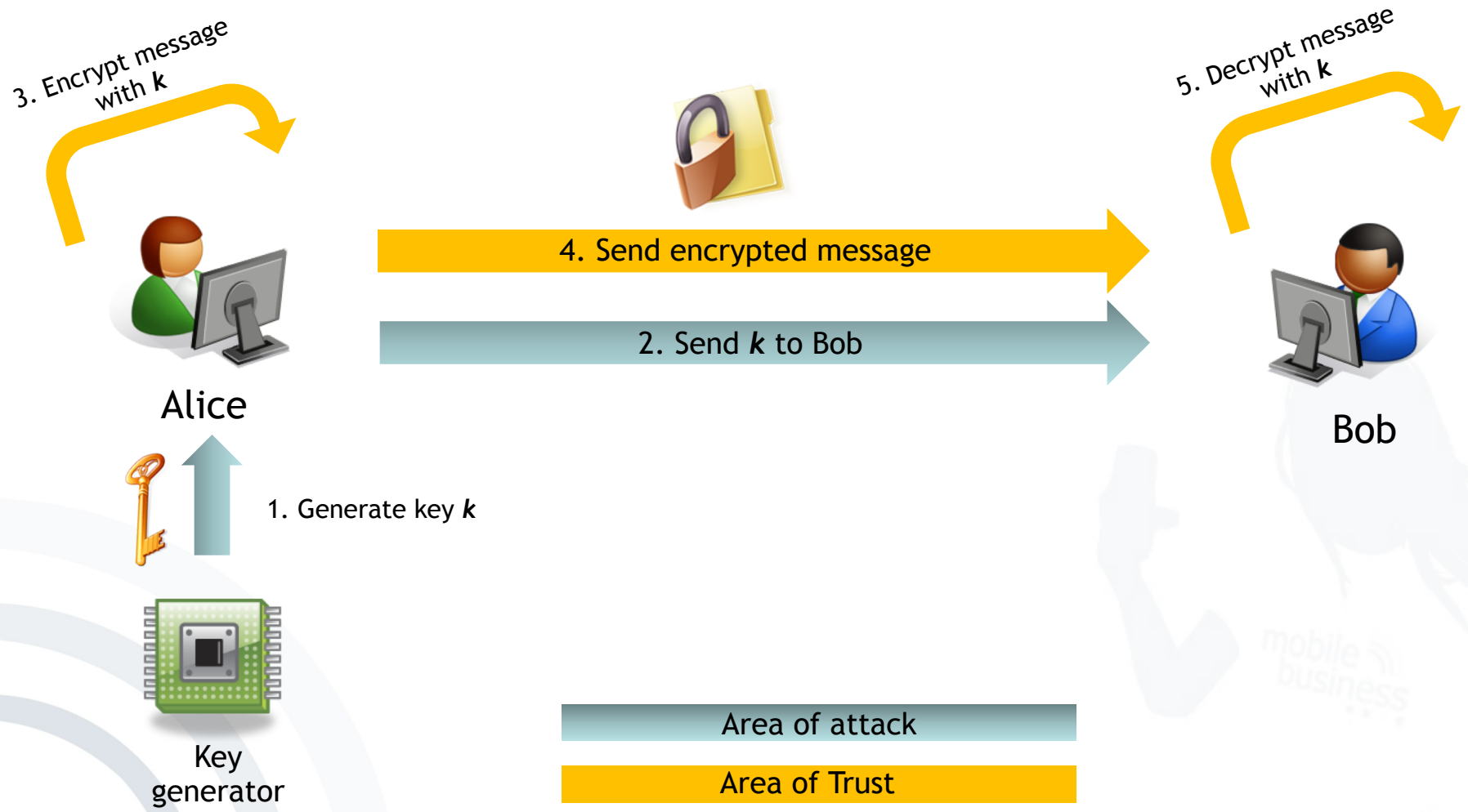


# Exercise 2: Cryptosystems - Symmetric Encryption





# Exercise 2: Cryptosystems - Symmetric Encryption



b. What are pre-conditions for this approach?

b. What are pre-conditions for this approach?

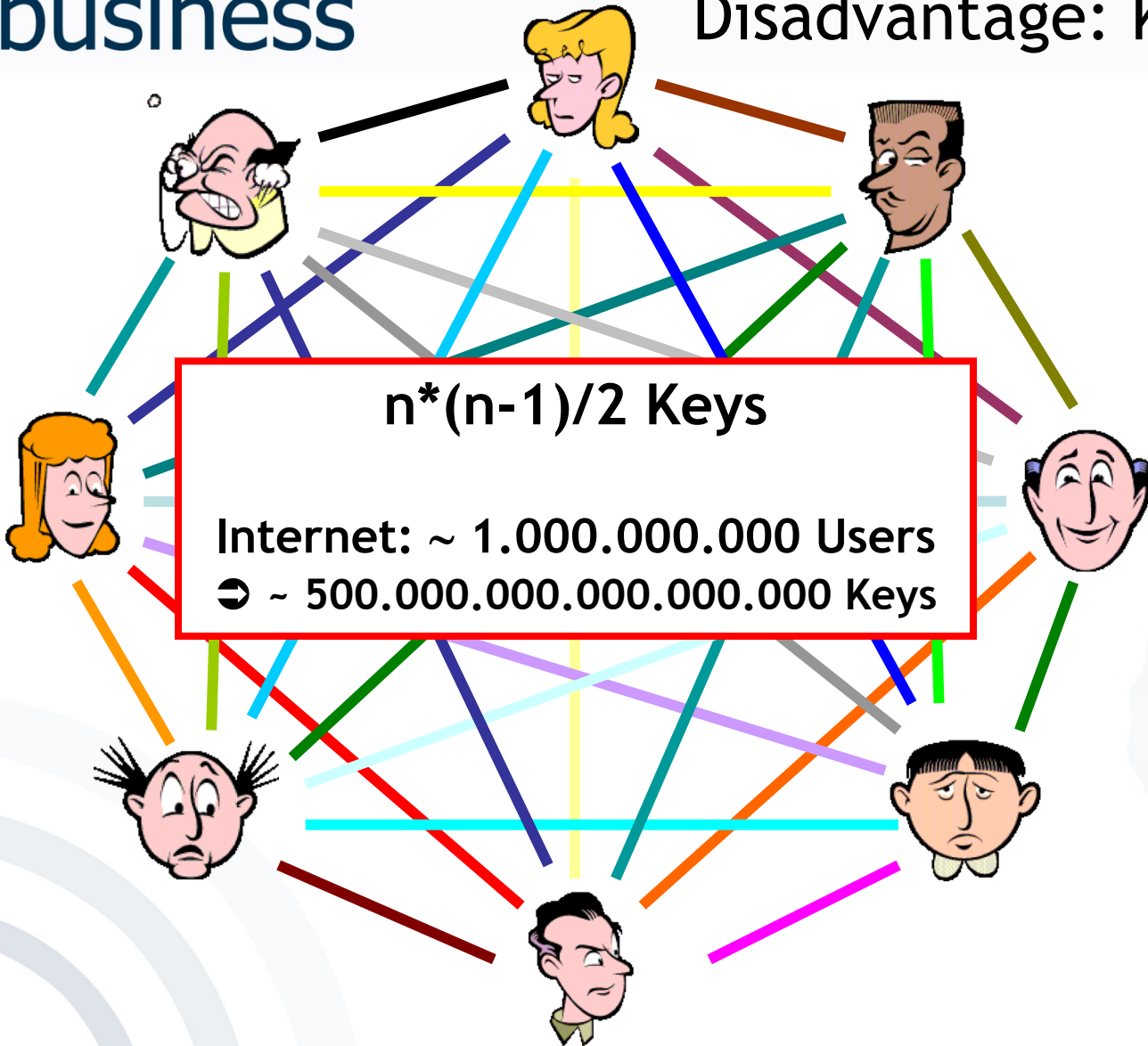
- Generation of shared symmetric key
- Exchange of (secret) shared key
  - Need for secure channel

c. What are advantages and disadvantages of symmetric encryption/decryption?

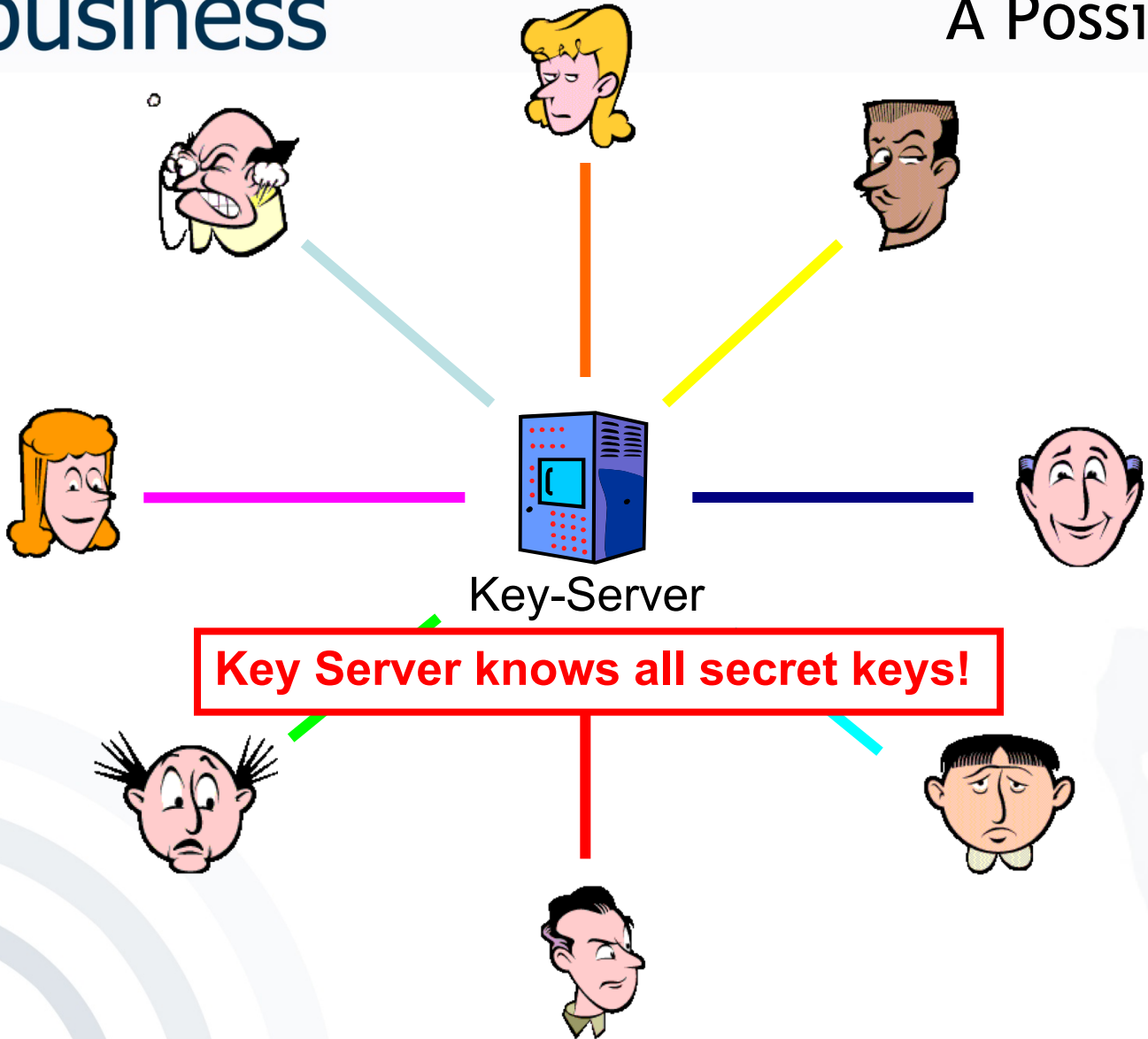
## Advantage: Algorithms are very fast

Algorithm	Performance*
RC6	138 ms
AES	173 ms
SERPENT	200 ms
IDEA	288 ms
MARS	394 ms
TWOFISH	697 ms
DES-edc	726 ms

\*) Encryption of 1 MB-blocks with an Athlon 1GHz processor



[adopted from J. Buchmann 2005: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]



# Exercise 2 - Asymmetric Encryption

1.2 Sketch the process by using asymmetric encryption/decryption.

- a. Complete the illustration by highlighting each step and adding all missing elements – such as keys, involved 3<sup>rd</sup> parties,...





# Exercise 2: Cryptosystems - Asymmetric Encryption



Alice



Bob



Public key  
server

Area of Trust

# Exercise 2: Cryptosystems - Asymmetric Encryption



Alice



Bob



Public key  
server



1. Generate asym.  
key pair ( $k_{pub}$ ,  $k_{priv}$ )

# Exercise 2: Cryptosystems - Asymmetric Encryption



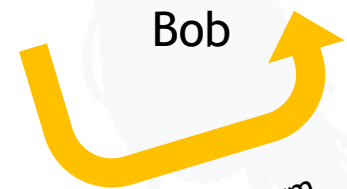
Alice



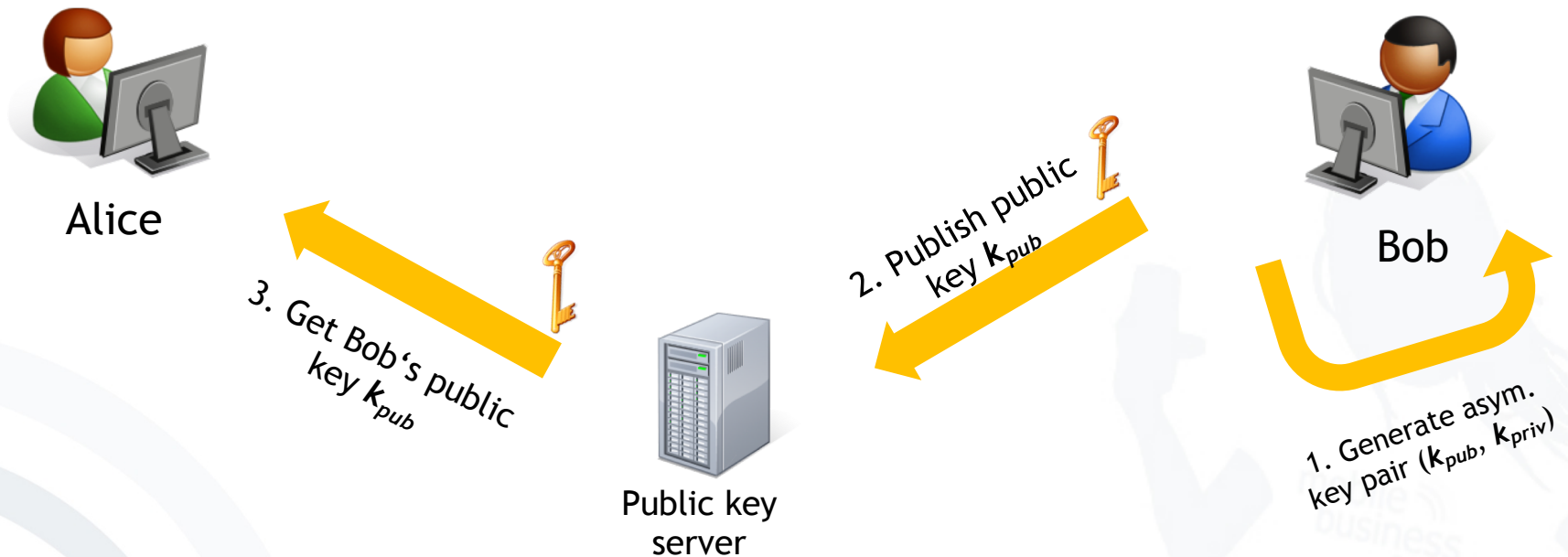
Public key server



Bob

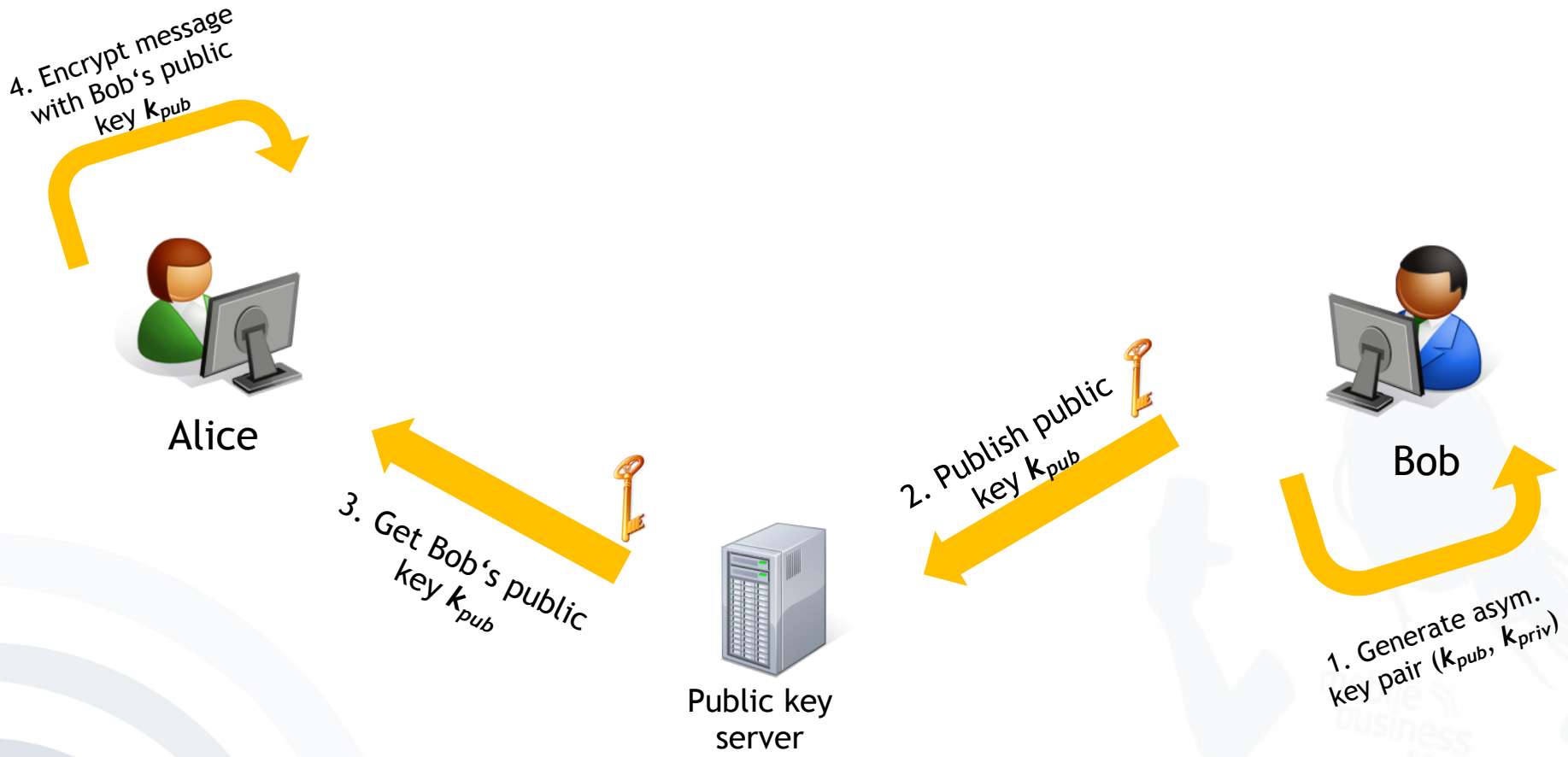


# Exercise 2: Cryptosystems - Asymmetric Encryption



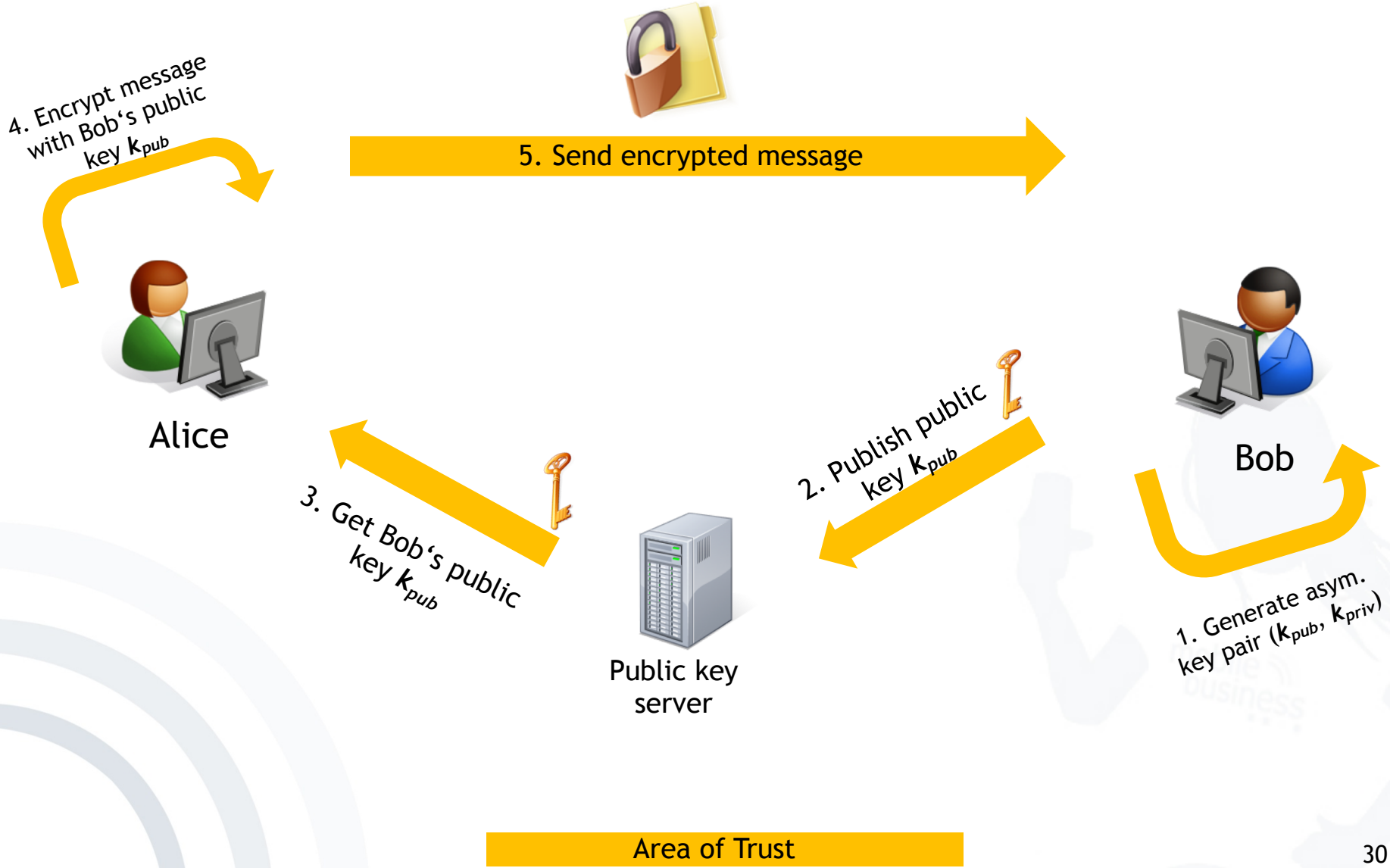
Area of Trust

# Exercise 2: Cryptosystems - Asymmetric Encryption

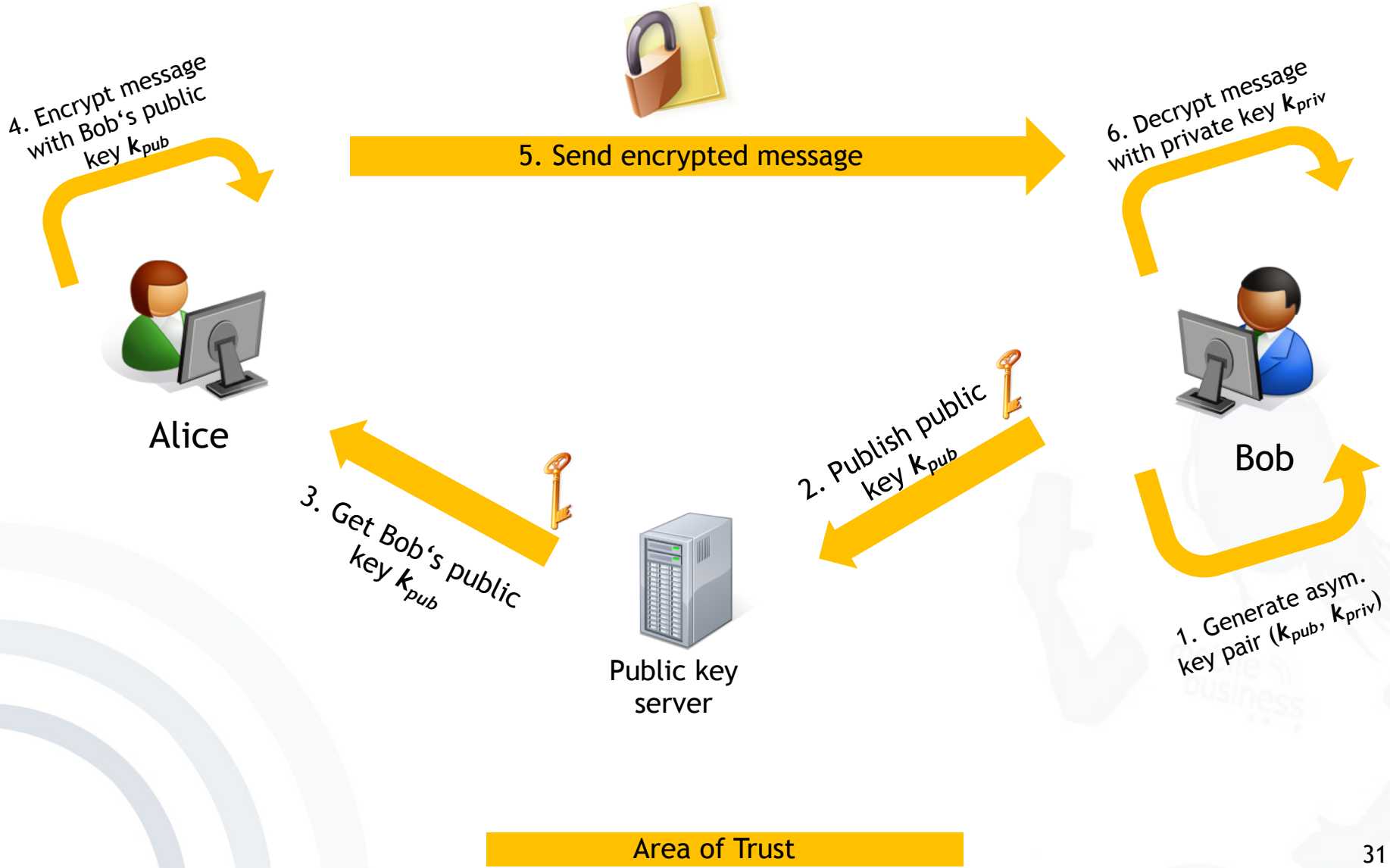


Area of Trust

# Exercise 2: Cryptosystems - Asymmetric Encryption



# Exercise 2: Cryptosystems - Asymmetric Encryption



b. What are pre-conditions for this approach?



b. What are pre-conditions for this approach?

- Generation of asymmetric key pairs
- Publishing public part of key
- Private key must be kept secret (!)

c. What are advantages and disadvantages of asymmetric encryption/decryption?

Algorithm	Performance*
El Gamal	1826 s
RSA	16 s

**Disadvantage:** Complex operations  
with very big numbers

➔ **Algorithms are very slow**

\*) Encryption of 1 MB-blocks with an Athlon 1GHz processor

c. What are advantages and disadvantages of asymmetric encryption/decryption?

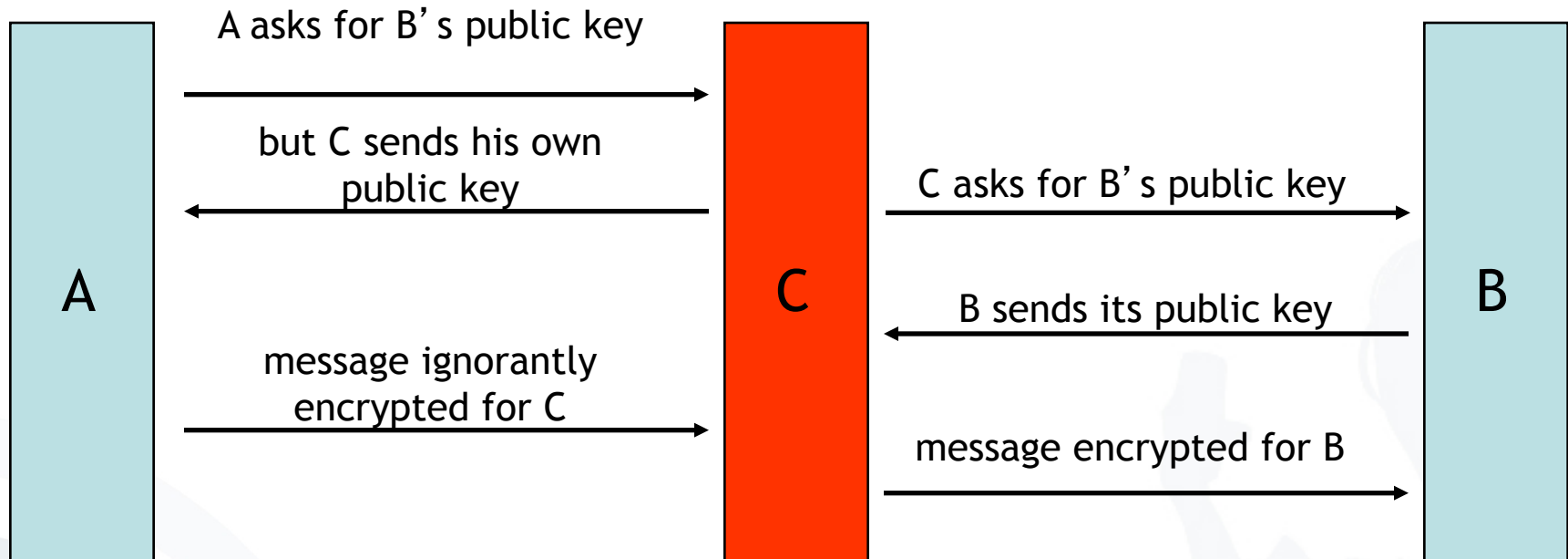
Advantages:

- No secret must be shared
- Only one key per endpoint

Disadvantages:

- Algorithms are very slow
- Man-in-the-middle-attack

## “Man in the middle attack”



- ➔ Keys are certified, that means a third person/institution confirms (with its digital signature) the affiliation of the public key to a person

1.3 Sketch the process by using PGP.

- a. Complete the illustration by highlighting each step and adding all missing elements – such as keys, involved 3<sup>rd</sup> parties,...



# Exercise 2: Cryptosystems - PGP



Alice



Bob



Public key  
server

Area of attack

Area of Trust

# Exercise 2: Cryptosystems - PGP



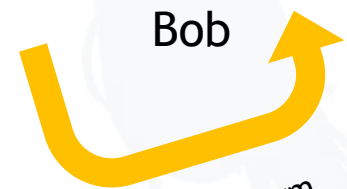
Alice



Bob



Public key  
server



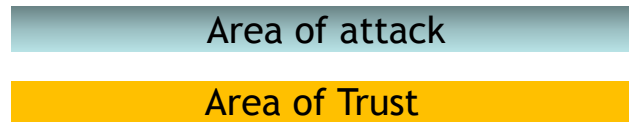
1. Generate asym.  
key pair ( $k_{pub}$ ,  $k_{priv}$ )

Area of attack

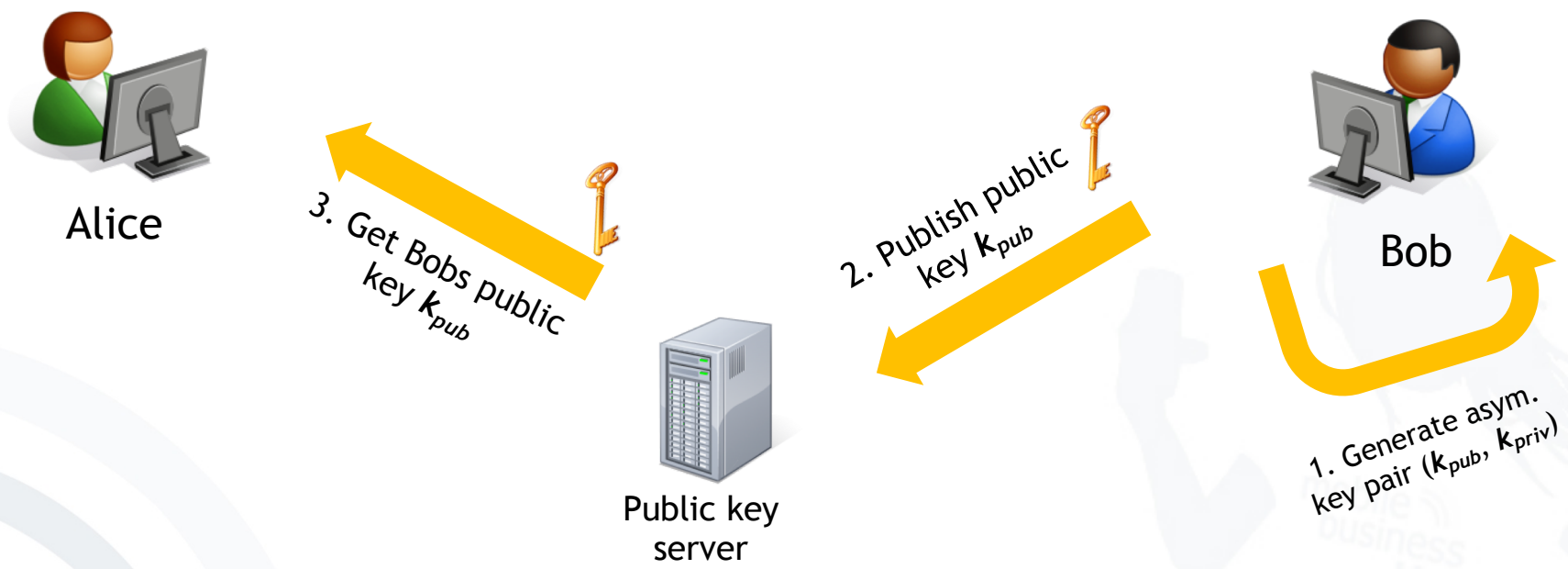
Area of Trust



# Exercise 2: Cryptosystems - PGP



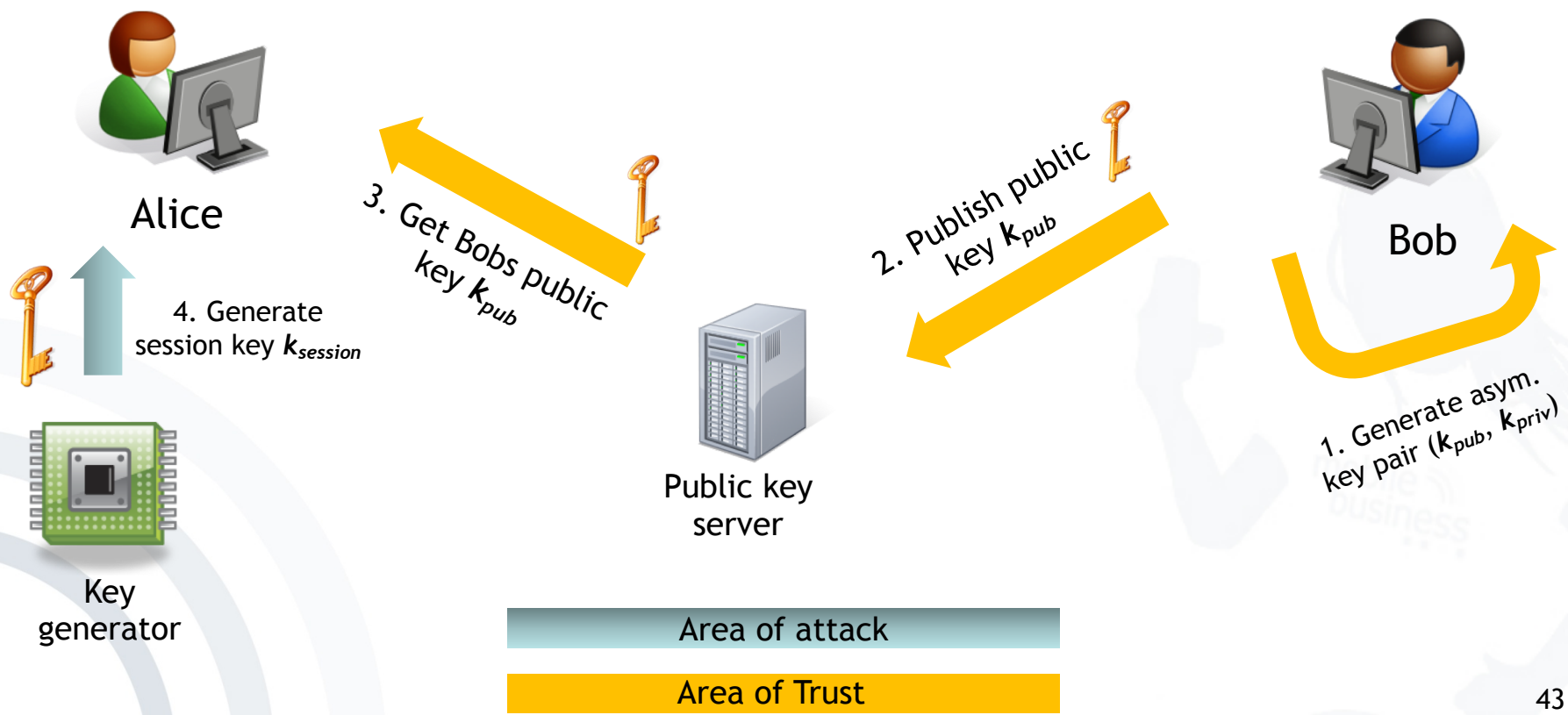
# Exercise 2: Cryptosystems - PGP



Area of attack

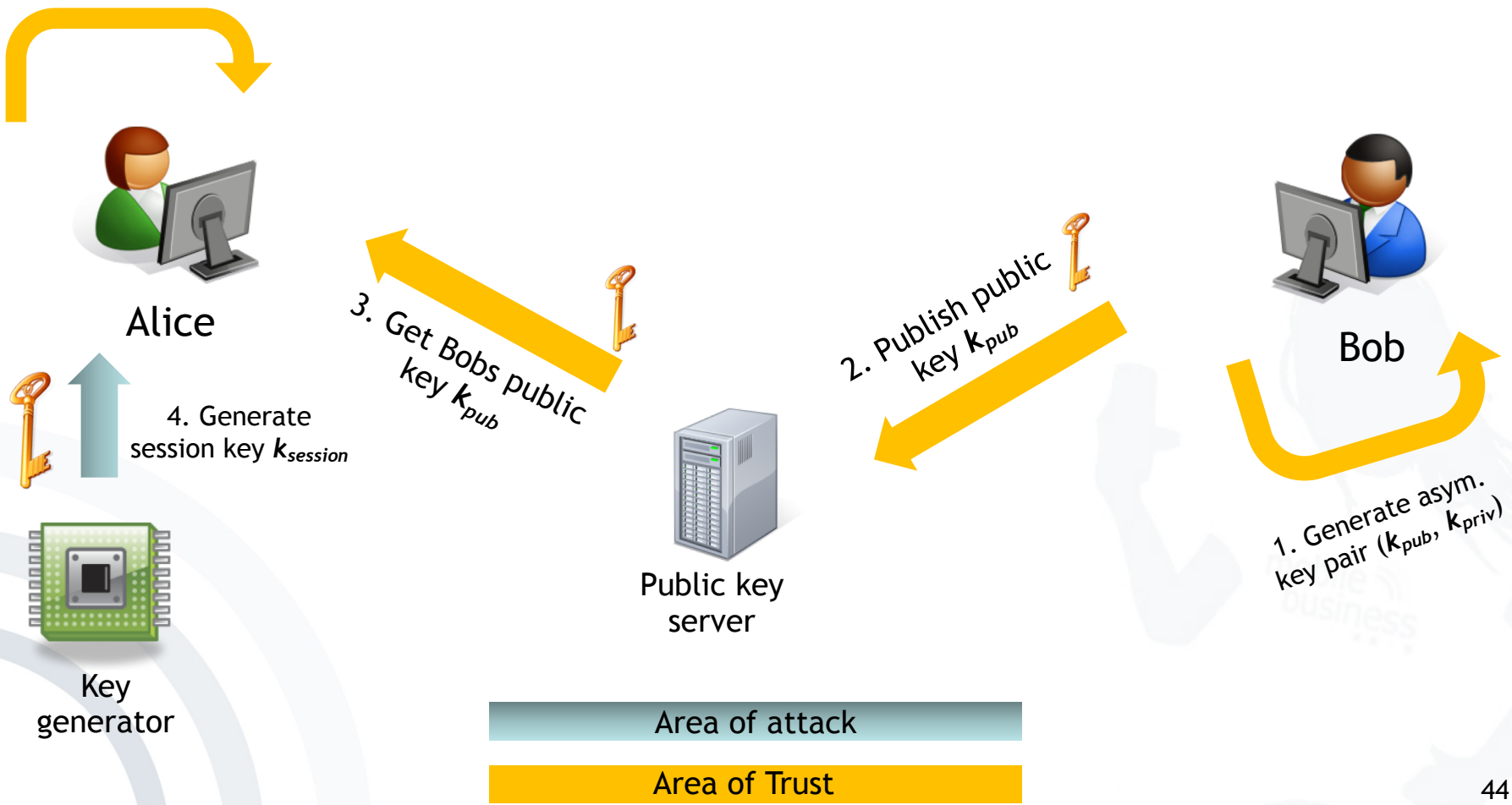
Area of Trust

# Exercise 2: Cryptosystems - PGP



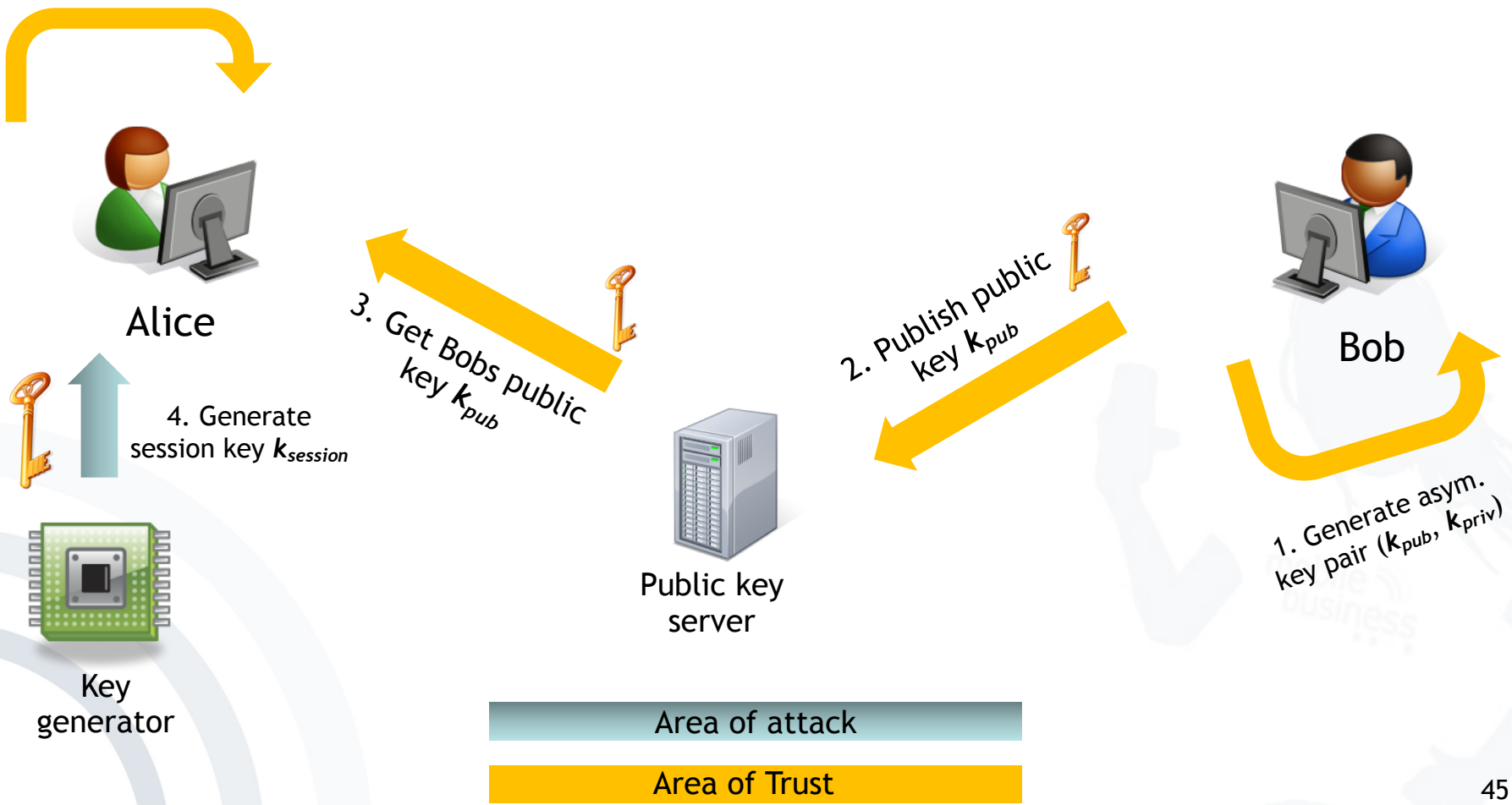
# Exercise 2: Cryptosystems - PGP

5. Encrypt message with session key  $k_{session}$



## Exercise 2: Cryptosystems - PGP

- 5. Encrypt message with session key  $k_{session}$
- 6. Encrypt session key with Bob's public key  $k_{pub}$



## Exercise 2: Cryptosystems - PGP

- 5. Encrypt message with session key  $k_{session}$
- 6. Encrypt session key with Bob's public key  $k_{pub}$



Contains encrypted session key  $k_{session}$

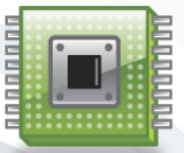
7. Send encrypted message



Alice



4. Generate session key  $k_{session}$



Key generator

3. Get Bobs public key  $k_{pub}$



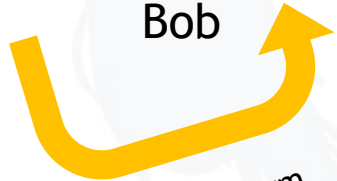
Public key server

2. Publish public key  $k_{pub}$



Bob

1. Generate asym. key pair  $(k_{pub}, k_{priv})$



Area of attack

Area of Trust

## Exercise 2: Cryptosystems - PGP

- 5. Encrypt message with session key  $k_{session}$
- 6. Encrypt session key with Bob's public key  $k_{pub}$



- 8. Decrypt session key with private key  $k_{priv}$

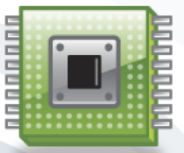
7. Send encrypted message



Alice



- 4. Generate session key  $k_{session}$



Key generator

- 3. Get Bobs public key  $k_{pub}$



Public key server

- 2. Publish public key  $k_{pub}$



Bob

- 1. Generate asym. key pair  $(k_{pub}, k_{priv})$

Area of attack

Area of Trust

# Exercise 2: Cryptosystems - PGP

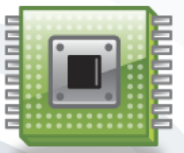
- 5. Encrypt message with session key  $k_{session}$
- 6. Encrypt session key with Bob's public key  $k_{pub}$



Alice



- 4. Generate session key  $k_{session}$



Key generator

- 3. Get Bobs public key  $k_{pub}$



Public key server

- 2. Publish public key  $k_{pub}$



Contains encrypted session key  $k_{session}$



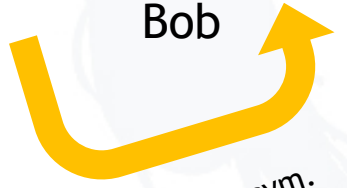
7. Send encrypted message

- 8. Decrypt session key with private key  $k_{priv}$
- 9. Decrypt message with session key  $k_{session}$



Bob

- 1. Generate asym. key pair  $(k_{pub}, k_{priv})$



Area of attack

Area of Trust



## Exercise 2: Cryptosystems

b. What are pre-conditions for this approach?

b. What are pre-conditions for this approach?

- Generation of asymmetric key pairs
- Publishing public part of key
- Private key must be kept secret (!)
- Generation of session key

c. What are advantages and disadvantages of PGP?

c. What are advantages and disadvantages of PGP?

→ **Hybrid encryption**

→ Advantages of both symmetric and asymmetric encryption

## Exercise 3: Cryptosystems

Describe possible ways for distributing keys and discuss advantages as well as disadvantages.

Mention possible ways for distributing keys and discuss advantages as well as disadvantages.

- Manually (e.g. on flash disc)
- Over existing secure channel
- Download from (trusted) key server
- Stored on Smart Card
- Based on certificates
- Key exchange protocols

- Bishop, M. (2005)  
Introduction to Computer Security, Addison Wesley, Boston, pp. 97-116.
- Diffie, W. and Hellman, M. E. (1976)  
New Directions in Cryptography, *IEEE Transactions on Information Theory* (22:6), pp. 644-654.
- Federrath, H. and Pfitzmann, A. (1997)  
Bausteine zur Realisierung mehrseitiger Sicherheit, in: G. Müller and A. Pfitzmann (Eds.): *Mehrseitige Sicherheit in der Kommunikationstechnik*, Boston, Addison Wesley, pp. 83-104.
- Rivest, R. L.; Shamir, A. and Adleman, L. (1978)  
A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM* (21:2), pp. 120-126.
- Whitten, A. and Tygar, J. (1999) *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*. In: Proceedings of the 9th USENIX Security Symposium, August 1999, [www.gaudior.net/alma/johnny.pdf](http://www.gaudior.net/alma/johnny.pdf)