

Exercise 3 - Cryptography

Mobile Business II (SS 2010)

Dipl.-Wirt.-Inf. Markus Tschersich

Dipl.-Kfm. Marvin Hegen

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



Exercise 1: Caesar Cipher

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

JYFWAVNYHWOF

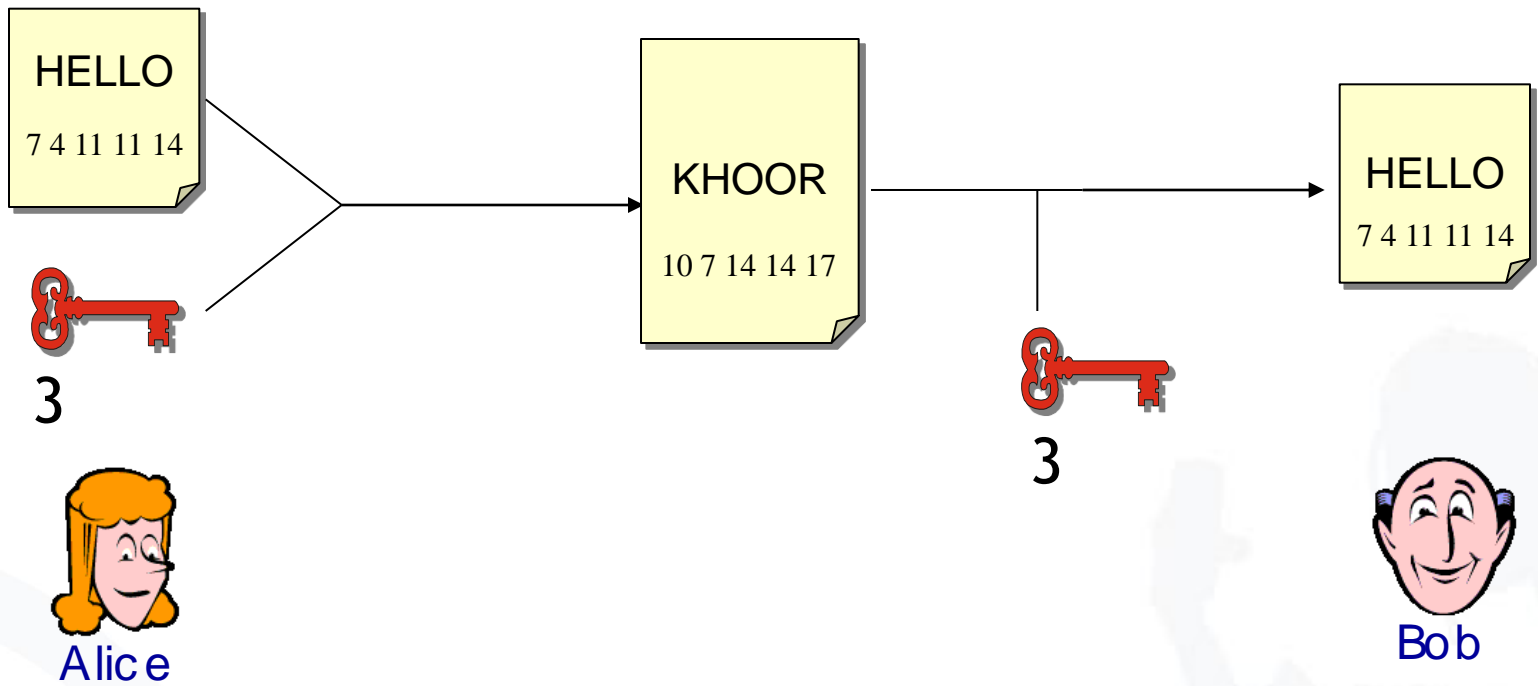
A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

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. $\text{num}(A) = 0$)

Caesar Cipher: Example



- 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 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

- 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

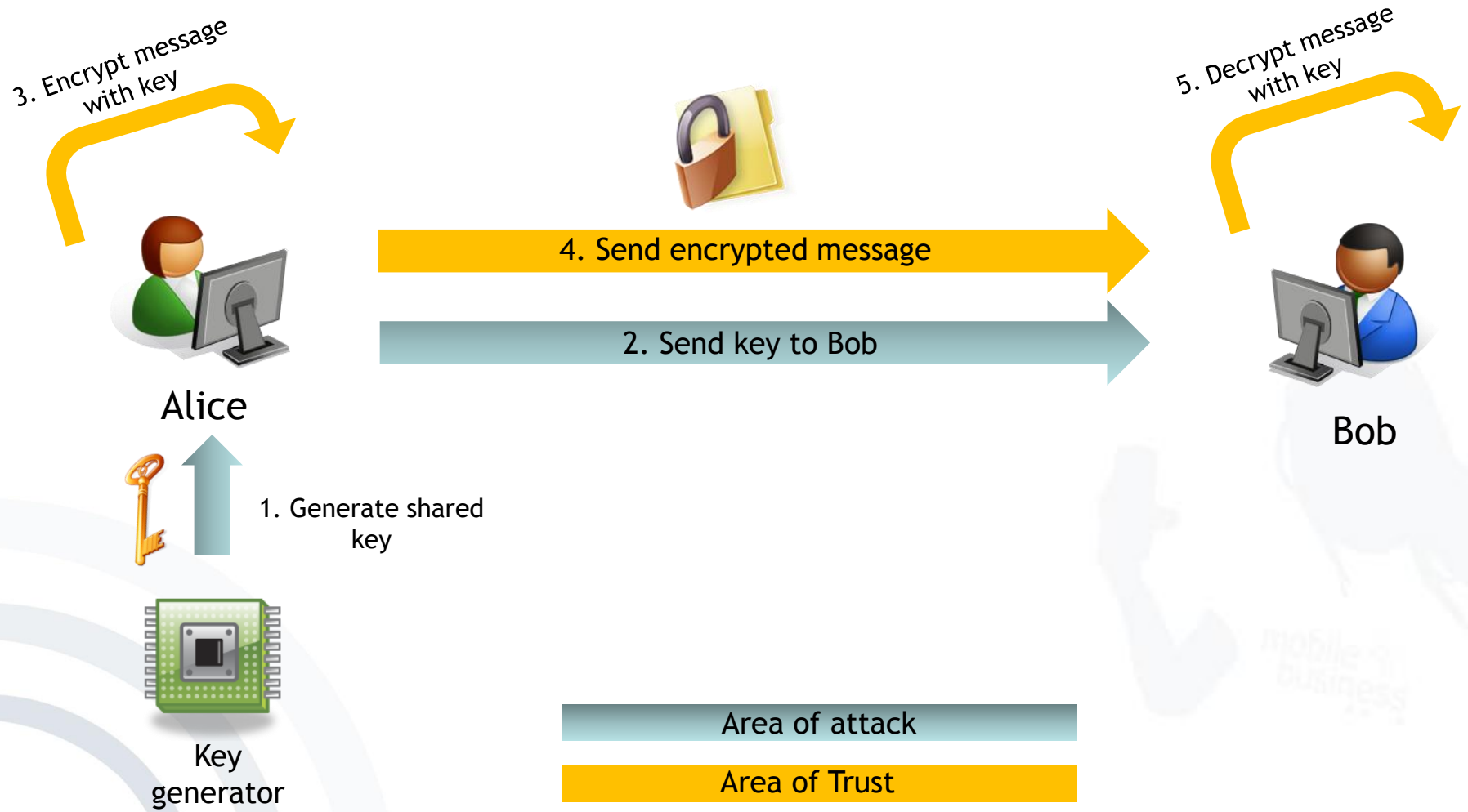
- Very simple form of encryption.
- The encryption and decryption algorithms are very easy and fast to compute.
- It uses a very limited key space ($n=26$)
- Therefore, the encryption is very easy and fast to compromise.

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 3rd parties,...



Exercise 2: Cryptosystems - Symmetric Encryption



b. What are pre-conditions for this approach?

b. What are pre-conditions for this approach?

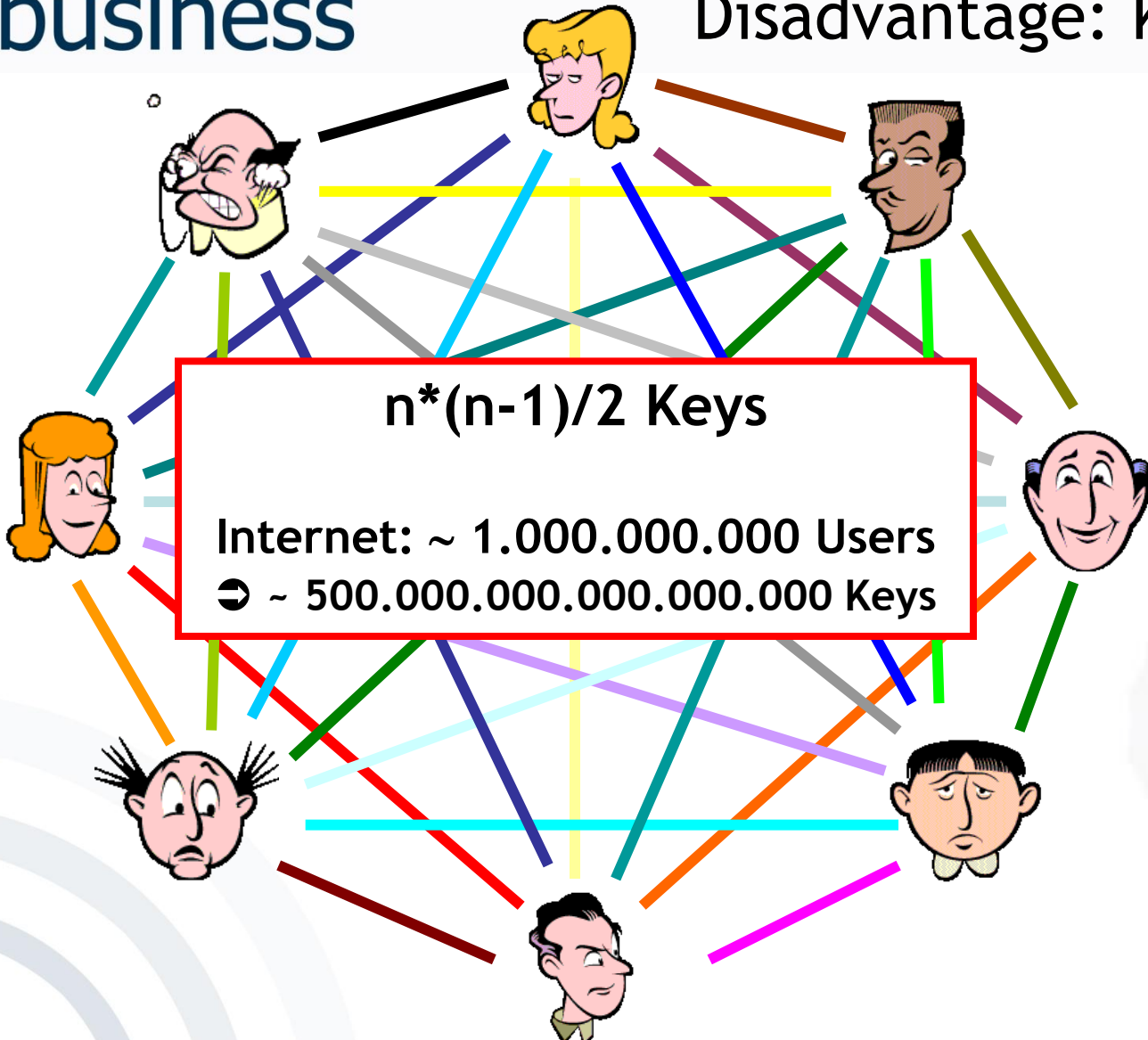
- Generation of shared symmetric key
- Exchange of (secret) shared key
 - Need for secure channel

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

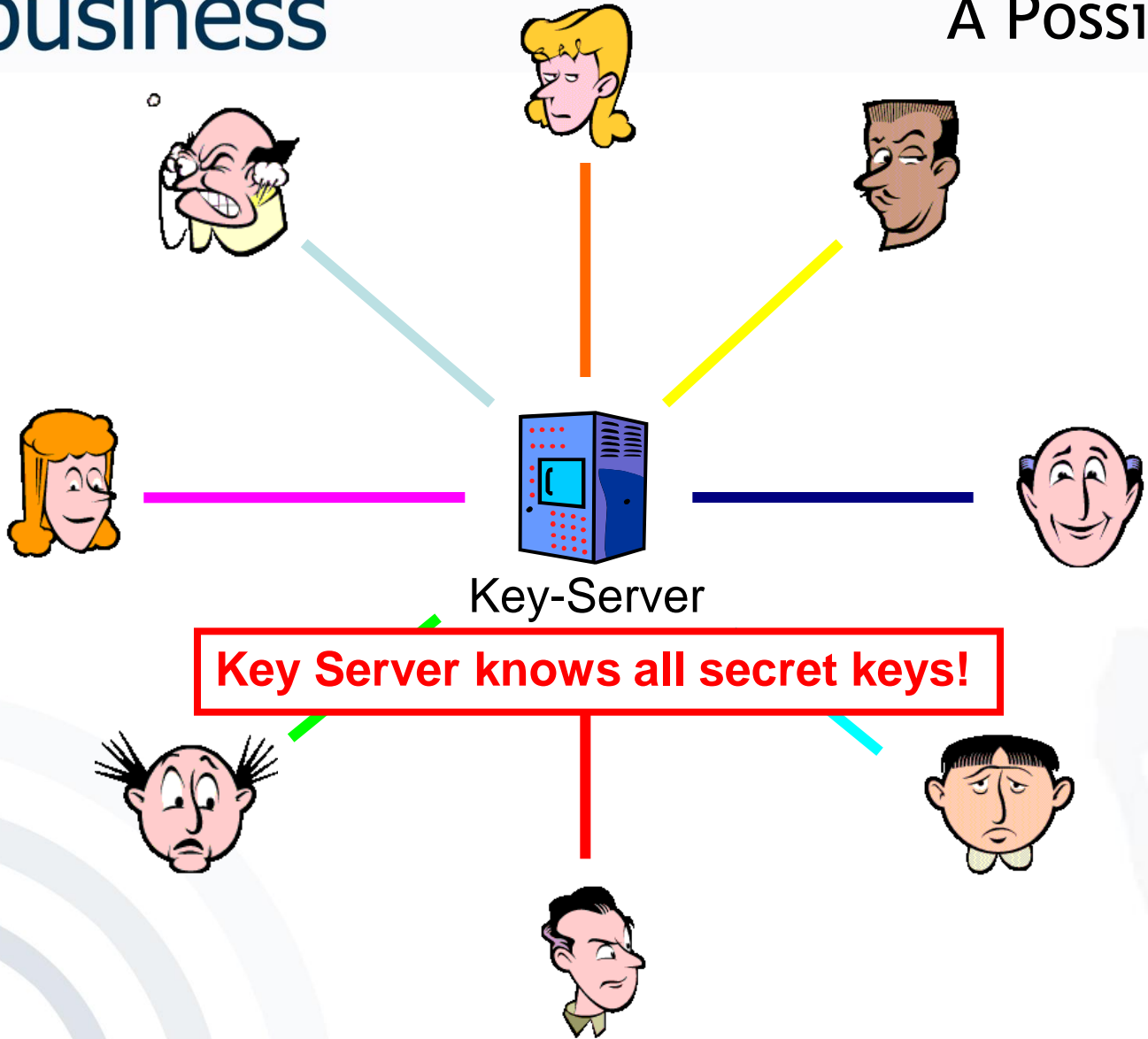
Advantage: Algorithms are very fast

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



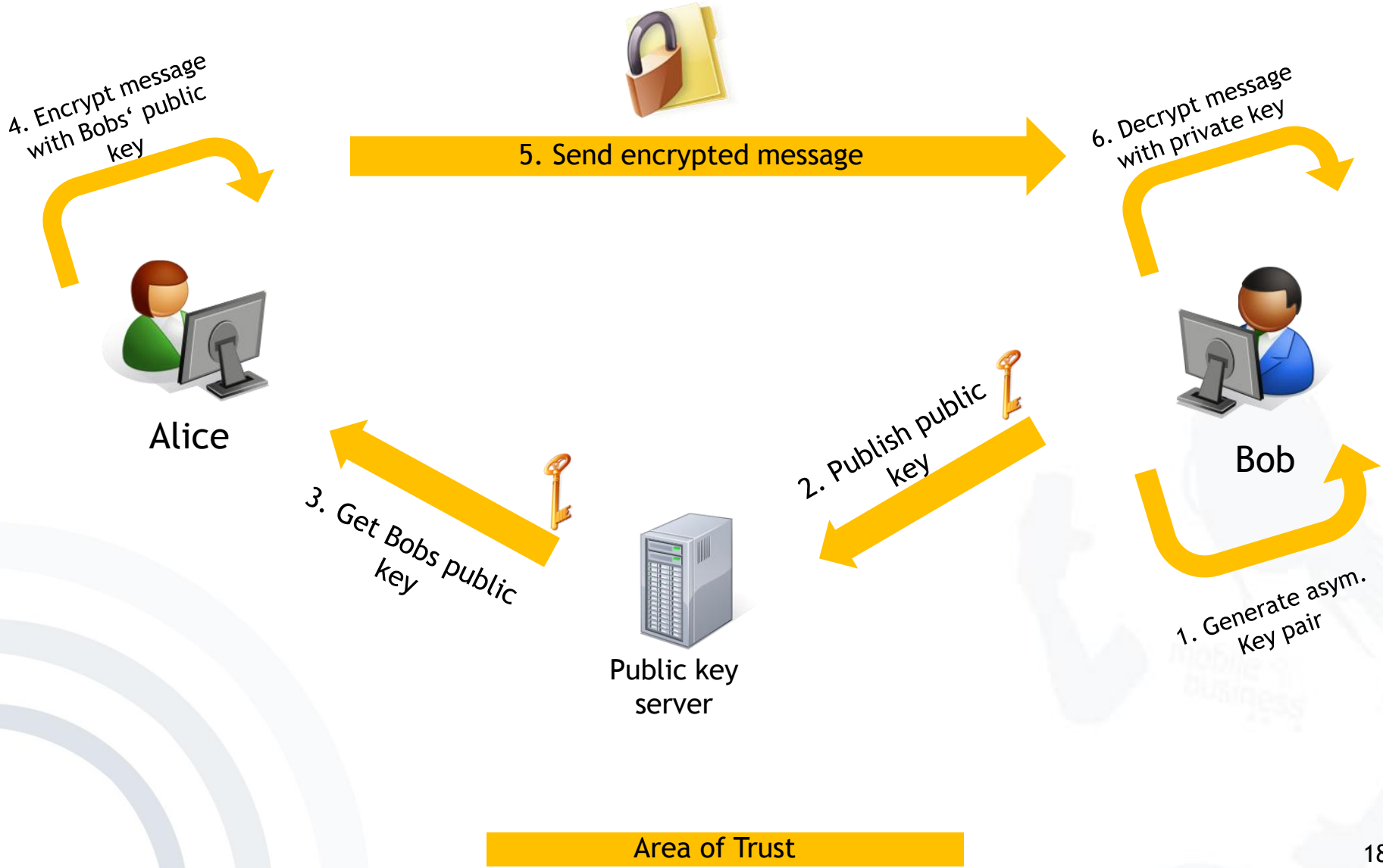
Exercise 2 - Asymmetric Encryption

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 3rd parties,...



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?

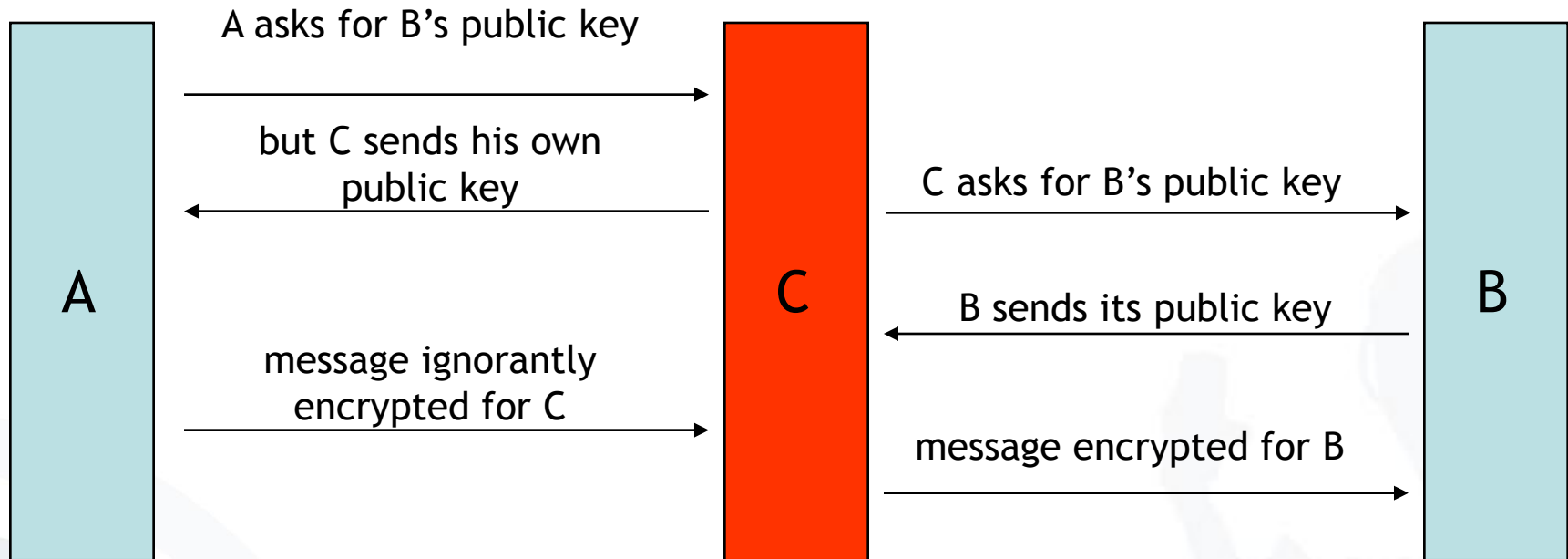
Advantages:

- 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 3rd parties,...



Exercise 2: Cryptosystems - PGP

- 5. Encrypt message with session key
- 6. Encrypt session key with Bobs public key



Contains encrypted session key

- 8. Decrypt session key with private key
- 9. Decrypt message with session key

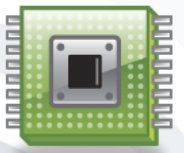
7. Send encrypted message



Alice



4. Generate session key



Key generator

3. Get Bobs public key



Public key server

2. Publish public key



Bob



1. Generate asym. Key pair

Area of attack

Area of Trust

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
- Requires additional software (e.g. GnuPG)

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

- Brute-Force-Attacks on the pass phrase
 - PGPCrack for conventionally encrypted files
- Trojan horses, changed PGP-Code
 - e.g. predictable random numbers, encryption with an additional key
- Attacks on the computer of the user
 - not physically deleted files
 - paged memory
 - keyboard monitoring
- Analysis of electromagnetic radiation
- Non-technical attacks
- Confusion of users [Whitten, Tygar 1999]

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

2. 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