Assignment 3 - Cryptography

Information & Communication Security
(WS 2018/19)

Abtin Shahkarami, M.Sc.

Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe-University Frankfurt a. M.

mobile business

Agenda

- Caesar cipher
- Symmetric vs. asymmetric ciphers
- Stream ciphers (Vernam code)
- Vigenére Cipher

Exercise 1: Caesar Cipher

- Break the following ciphertext, given that the Caesar cipher was used to produce it is:

  NZIVSNCZB QA QV OMZUIVG

- (Hint: Start by a permutation of the alphabet by 1, then 2, … until the result makes sense in English)

- It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

Caesar Cipher

Ciphertext: **NZIVSNCZB QA QV OMZUIVG**

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.

Caesar Cipher

- For k ϵ {0..25} we have:
  - An encryption function:
    - e: x -> (x+k) mod 26
  - A decryption function:
    - d: x -> (x-k) mod 26
  - In this case $k_e = k_d$

Caesar Cipher

- Let‘s try:

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

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

The plaintext

- The key is 8
- The plain text is:

FRANKFURT IS IN GERMANY

Assessment of Caesar Cipher

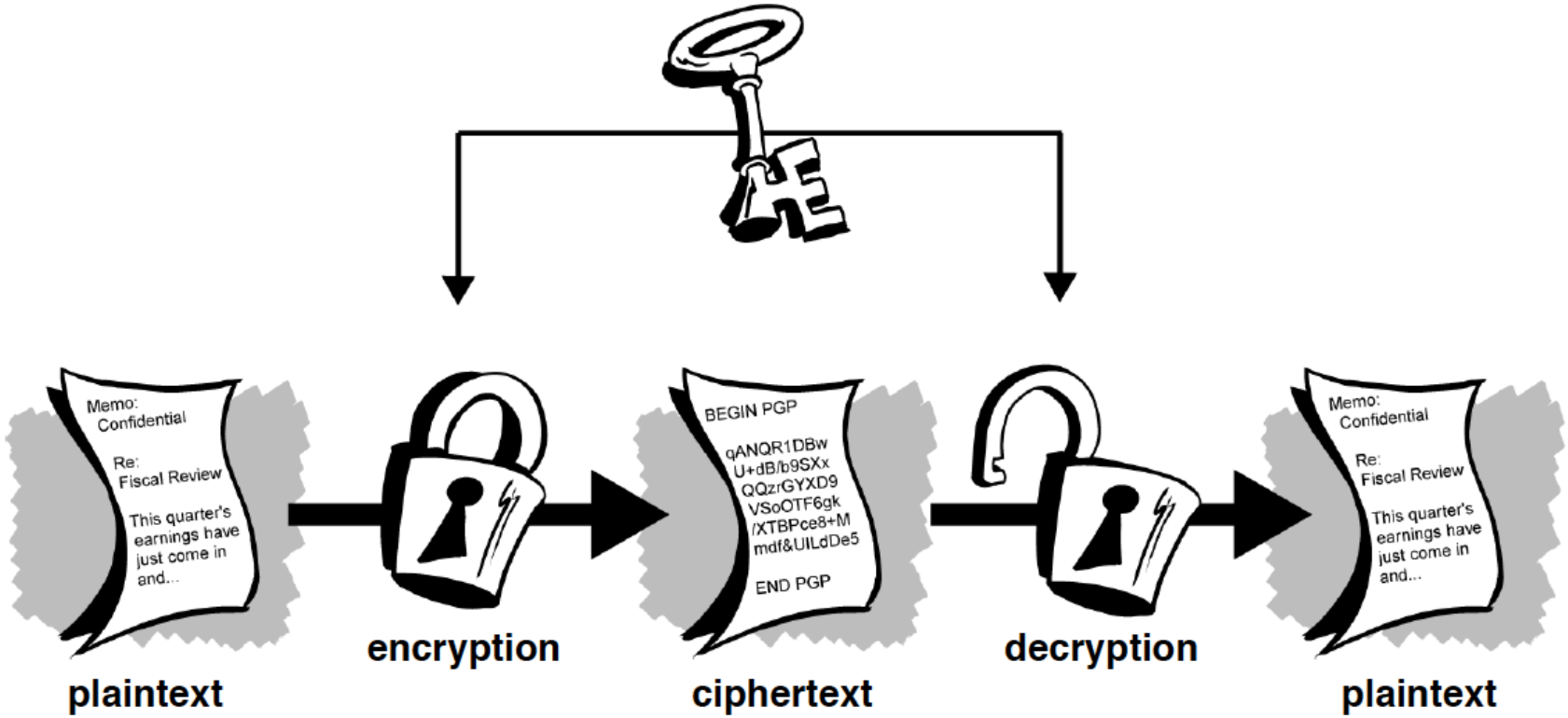
- Very simple form of encryption.
- The encryption and decryption algorithms are very easy and fast to compute.
- It uses a very limited key space (n=26)
- Therefore, the encryption is very easy and fast to compromise.

Exercise 2: Symmetric vs. asymmetric crypto

What is the difference between symmetric and asymmetric crypto systems?

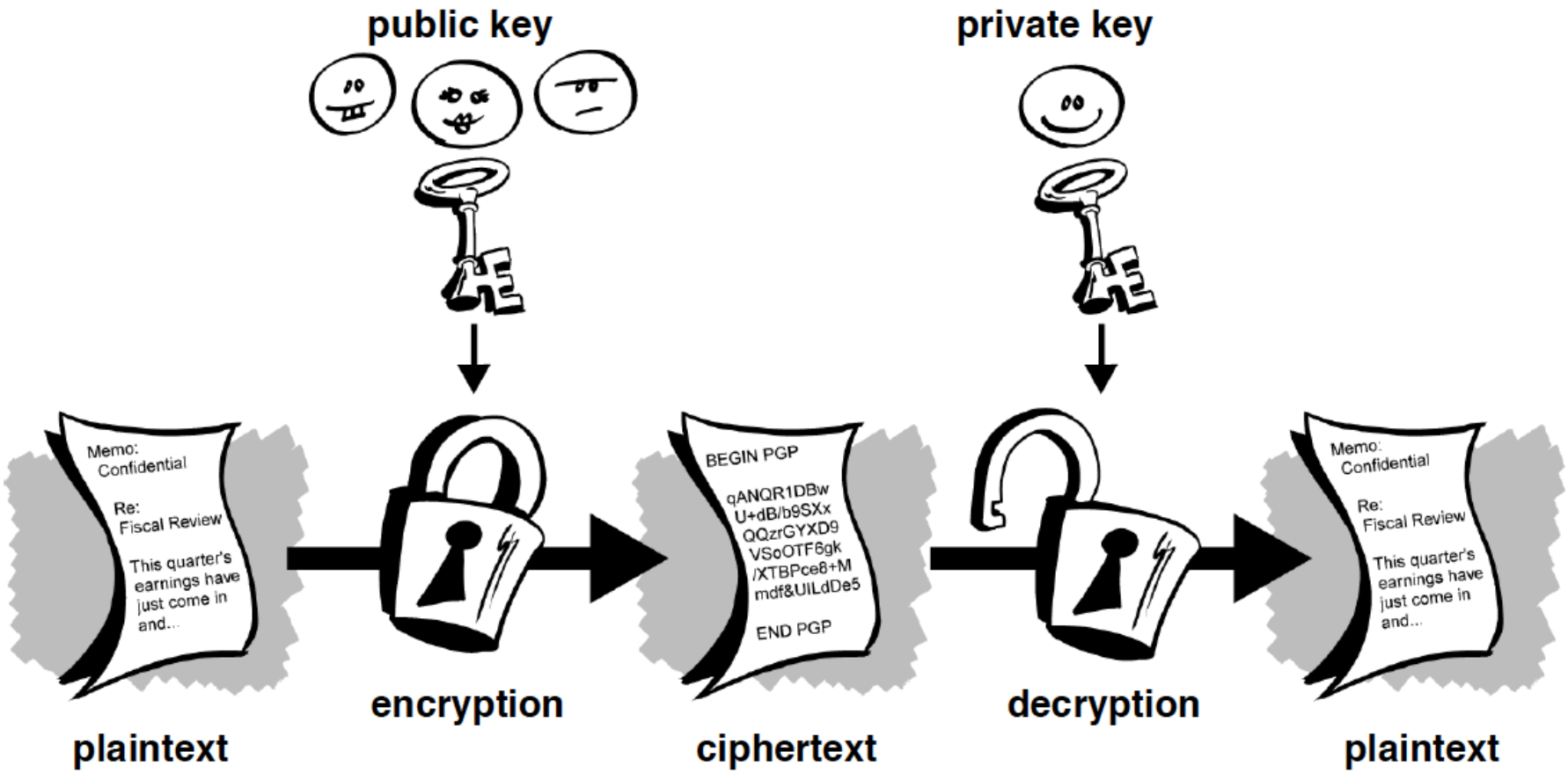
- symmetric algorithms: (also called “secret key”) use the same key for both encryption and decryption;
- asymmetric algorithms: (also called “public key”) use different keys for encryption and decryption.

Guess which crypto system this is



Symmetric or Asymmetric?

This crypto system is…?



Symmetric or Asymmetric?

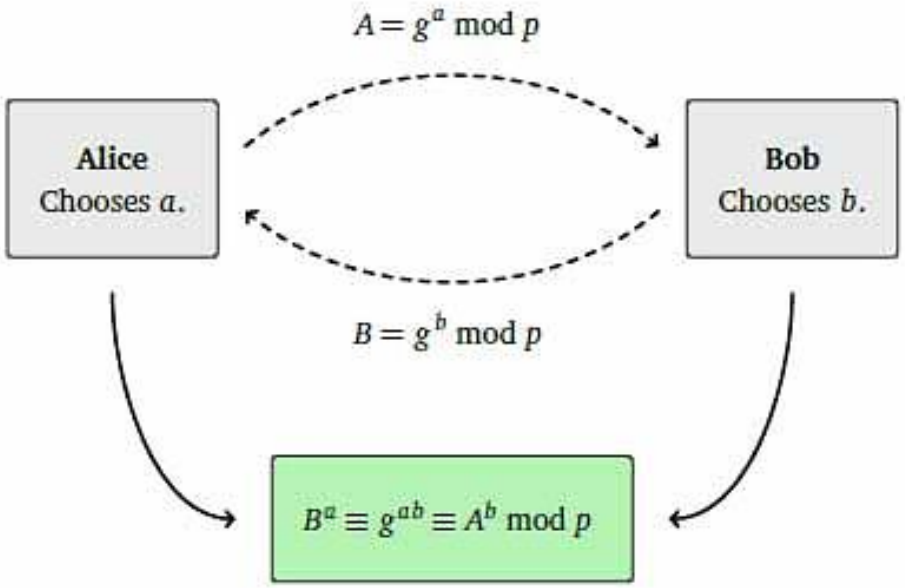


Figure 1.2: Diffie-Hellman Key Exchange

a) Alice and Bob agree publicly on a cyclic group, e.g. $G = \langle g \rangle$, $G = \mathbb{F}_p^*$.

b) Alice chooses randomly some $0 \leq a < |G|$ and computes $A := g^a$. Bob chooses randomly some $0 \leq b < |G|$ and computes $B := g^b$.

c) Alice sends Bob A. Bob sends Alice B.

d) Alice computes $S := B^a = (g^b)^a = g^{ab}$. Bob computes $S := B^a = (g^a)^b = g^{ab}$.

e) Now Alice and Bob can use S as their secret key to encrypt and decrypt messages.

Exercise 3: Stream ciphers

a) What is a one-time pad (Vernam-code)?

Vernam Code

- Invented by Gilbert Vernam
- is based on the principle that each plaintext character from a message is 'mixed' with one character from a key stream
- The length of the key is as long as the length of the plaintext.
- The key is randomly chosen and only used once.
- Every key has the same probability.

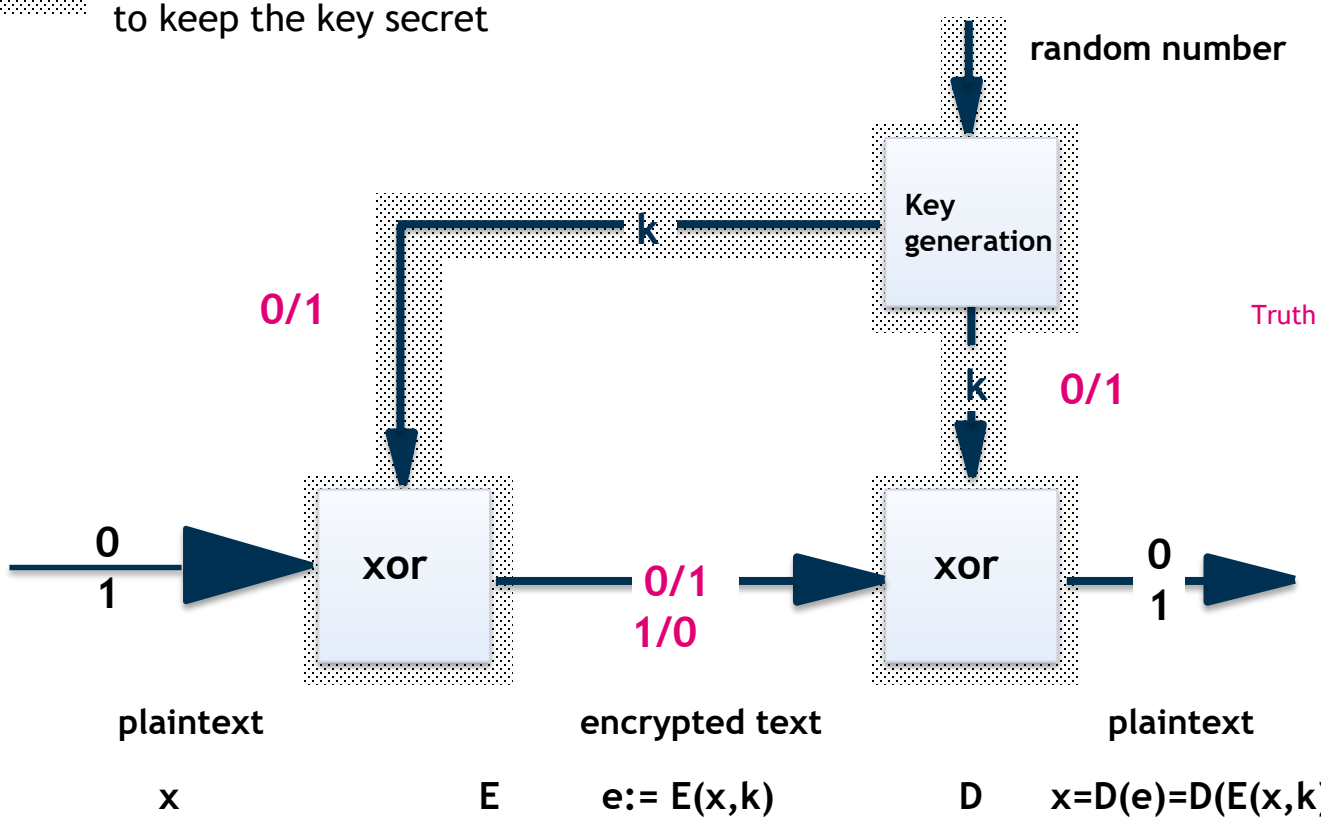
Vernam Code

- If a truly random key stream is used, the result will be a truly 'random' ciphertext which bears no relation to the original plaintext

http://www.cryptomuseum.com/crypto/vernam.htm

Example Vernam Code

area that needs to be protected to keep the key secret



X_i	S_i	Y_i
0	0	0
0	1	1
1	0	1
1	1	0

Truth Table of the XOR operation

[based on Federrath and Pfitzmann 1997]

Exercise 3: Stream ciphers

- b) Alice wants to encrypt the letter A, where the letter is given in ASCII code. The ASCII value for A is $65_{10} = 1000001_2$. Using Vernam-code, which of the following keys are suitable to encrypt this plaintext:
  - b1) 10100110
  - b2) 0011111
  - b3) 101010

X_i	S_i	Y_i
0	0	0
0	1	1
1	0	1
1	1	0

Truth Table of the XOR operation

Exercise 3: Stream ciphers

- c) Encrypt the message using Vernam code and using XOR as an encryption function and the key in b).

Plaintext (A)	1000001
Key (B)	0011111
Ciphertext (A xor B)	1011110

X_i	S_i	Y_i
0	0	0
0	1	1
1	0	1
1	1	0

Truth Table of the XOR operation

Exercise 4: Vigenére Cipher

- a) What is a Vigenére Cipher?
- b)You want to encrypt the message "**I am studying in Frankfurt**" to your friend living in Berlin. What will be your cypher text encrypted using the key "**Berlin**"? Show the necessary steps (Use the Vigenére tableau below when necessary).

Vigenére Cipher

https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Exercise 4(b):

b)You want to encrypt the message

“I am studying in Frankfurt”

to your friend living in Berlin. What will be your cypher text encrypted using

the key “**Berlin**”?

Show the necessary steps (Use the Vigenére tableau below when necessary).

- The plain text

  “I am studying in Frankfurt”
- The key

  “Berlin”

Plain text	I	A	M	S	T	U	D	Y	I	N	G	I	N	F	R	A	N	K	F	U	R	T
Key	B	E	R	L	I	N	B	E	R	L	I	N	B	E	R	L	I	N	B	E	R	L
Cypher text	j	e	d	d	b	h	e	c	z	y	o	v	o	j	i	l	v	x	g	y	i	e

Assessment Vigenére Cipher

- Then a Prussian cavalry officer named Kasiski noticed that repetitions occur when characters of the key appear over the same characters in the plaintext.
- The number of characters between successive repetitions is a multiple of the period (key length).
- Given this information and a short period the Vigenére cipher is quite easily breakable.
- *Example: The Caesar cipher is a Vigenére cipher with a period of 1.*

[Bi2005]

mobile business

Thank you!

Questions:

security@m-chair.de

abtin.shahkarami@m-chair.de

References

- [Federrath Pfitzmann 1997] Hannes Federrath, Andreas Pfitzmann: Bausteine zur Realisierung mehrseitiger Sicherheit. in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-

  Longman1997, 83-104.