Assignment 3 - Cryptography

Information & Communication Security (SS 2022)

Prof. Dr. Kai Rannenberg
Sascha Löbner (M.Sc.)

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

Agenda

I. Caesar Cipher
II. Stream Ciphers (Vernam code)
III. Vigenère Cipher
IV. Asymmetric Cryptosystems and RSA

Exercise 1 (Caesar Cipher)

A Caesar encryption is given by the following encryption function:

$$e_k: \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \qquad x \to (x+k) \quad mod\ 26$$

, with $k \in \mathbb{Z}_{26}$

a) Encrypt the message "perfect indistinguishability" using e_{10}.
b) What is perfect indistinguishability?
c) Does the condition of perfect indistinguishability hold in general for the Caesar Cipher? Give a two-line explanation.
d) What attacks can be used to break the Caesar Cipher?

Background – Modulo

- Let $a, b \in \mathbb{Z} \setminus \{0\}$. With $\text{remainder}(a, b)$ we denote the remainder, which results from dividing a by b
- $Rest(a, b) \coloneqq \min\{r \in \mathbb{N} : \exists\, m \in \mathbb{Z}\, with\; a = m \cdot b + r\}$
- $Rest(a, b) = \mathrm{a} - \mathrm{m} \cdot b$
- $\boxed{a \equiv b \pmod{m} :\Leftrightarrow remainder(a, m) = remainder(b, m), with\; m \in \mathbb{N} \setminus \{1\}}$

https://sagecell.sagemath.org (Syntax: 6 % 5)

Exercise 1 (Caesar Cipher)

A Caesar encryption is given by the following encryption function:

$$e_k : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}, \qquad x \rightarrow (x + k) \quad mod\ 26$$

, with $k \in \mathbb{Z}_{26}$

a) Encrypt the message "perfect indistinguishability" using e_{10}.
b) What is perfect indistinguishability?
c) Does the condition of perfect indistinguishability hold in general for the Caesar Cipher? Give a two-line explanation.
d) What attacks can be used to break the Caesar Cipher?

Exercise 1 (Caesar Cipher)

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

Exercise 1 (Caesar Cipher)

a) Encrypt the message "perfect indistinguishability" using e_{10}.

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
0	1	2	3	4	5	6	7	8	9	**10**	11	12	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.
- Assign letter with index 10 index 0

Exercise 1 (Caesar Cipher)

a) Encrypt the message "perfect indistinguishability" using e_{10}.

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
0	1	2	3	4	5	6	7	8	9	**10**	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

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
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

"perfect indistinguishability" → "zobpomd sxnscdsxqescrklsvsdi"

- We assign a **number** for every character.
- This enables us to calculate with letters as if they were numbers.
- Assign letter with index 10 index 0

Example for e_k with $k = 10$:
Index of p = 15 (this is x)
$(15 + 10) \bmod 26 = 25$
z has index 25

Exercise 1 (Caesar Cipher)

b) What is perfect indistinguishability?

Exercise 1 (Caesar Cipher)

b) What is perfect indistinguishability?

Solution: An encryption scheme is *perfectly secret* if for all plaintexts $m_0, m_1 \in M$ and all cyphertexts $c \in C$:

$$\Pr[e_k(m_0) = c] = \Pr[e_k(m_1) = c]$$

The condition that all plaintexts have the same probability for a given ciphertext is called perfect indistinguishability. [Kn19]

c) Does the condition of perfect indistinguishability hold in general for the Caesar Cipher? Give a two-line explanation.

c) Does the condition of perfect indistinguishability hold in general for the Caesar Cipher? Give a two-line explanation.

Solution: No. In general, the Caesar Cypher does not fulfil the condition of perfect secrecy. We easily can decrypt the message by trying all 26 possible keys. (We can make the scheme perfectly secret if we use a different key for each letter.)

d) What attacks can be used to break the Caesar Cipher?

d) What attacks can be used to break the Caesar Cipher?

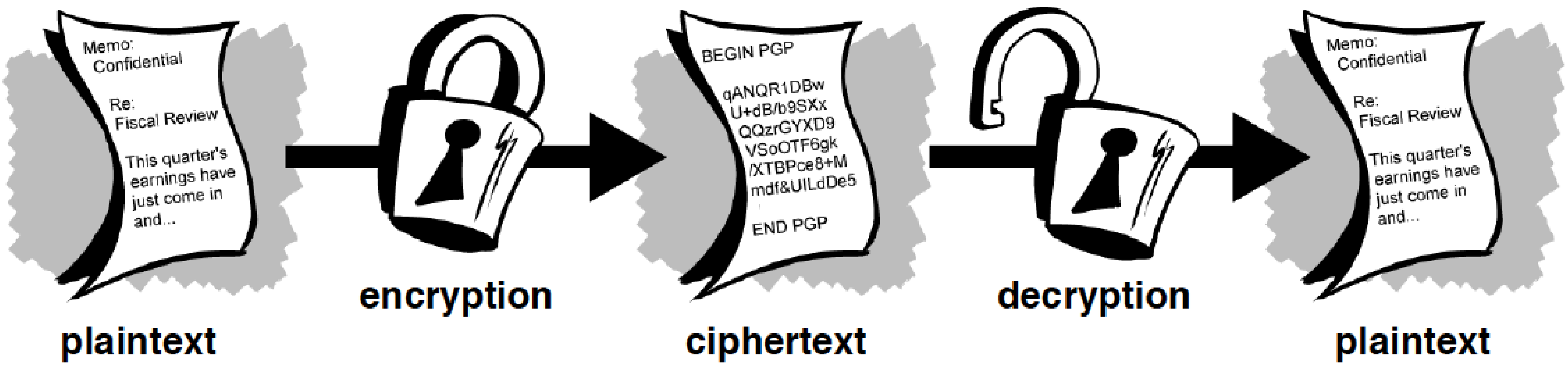
Solution:

- Brute force attack
- Statistical ciphertext-only attack

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.

Encryption - Decryption



http://www.pgpi.org/doc/guide/6.5/en/intro/

Exercise 2 Stream Ciphers (Vernam code)

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

b) Zoe wants to encrypt the letter Z. The letter is given in ASCII code. The ASCII value for Z is $90_{10} = 1111010_2$. Using Vernam-code, which of the following keys are suitable to encrypt this plaintext?

   I. b1) 11100100

   II. b2) 0011101

   III. b3) 101011

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

Exercise 2 Stream Ciphers (Vernam code)

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

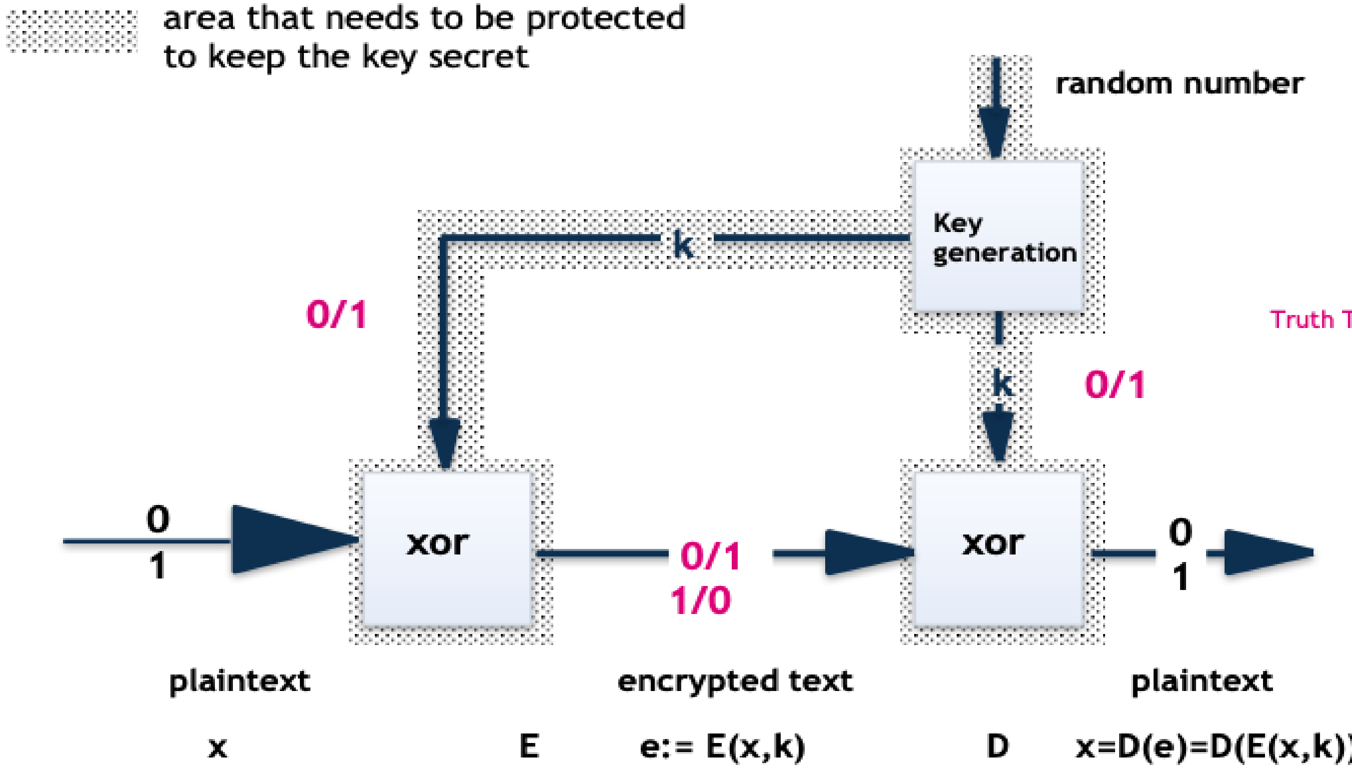
Exercise 2 Stream Ciphers (Vernam code)

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

Solution:

- Invented by Gilbert Vernam
- 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.

Exercise 2 Stream Ciphers (Vernam code)



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 2 Stream Ciphers (Vernam code)

b) Zoe wants to encrypt the letter Z. The letter is given in ASCII code. The ASCII value for Z is $90_{10} = 1111010_2$. Using Vernam-code, which of the following keys are suitable to encrypt this plaintext?

I. b1) 11100100

II. b2) 0011101

III. b3) 101011

Exercise 2 Stream Ciphers (Vernam code)

b) Zoe wants to encrypt the letter Z. The letter is given in ASCII code. The ASCII value for Z is $90_{10} = 1111010_2$. Using Vernam-code, which of the following keys are suitable to encrypt this plaintext?

I. b1) 11100100

II. b2) 0011101

III. b3) 101011

Exercise 2: Stream Ciphers (Vernam code)

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

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

1	1	1	1	0	1	0
0	0	1	1	1	0	1
1	1	0	0	1	1	1

Exercise 3 (Vigenère Cipher)

a) What is the Vigenère Cipher?

b) In the following you are given the key $k = "GOETHE"$ and the cyphertext $c =$ "CSWMLRJWWMOISCWMIIGIXBMYRQEFWYY". Identify the message m using the running key variant as given in the lecture. Show the necessary steps (use the Vigenére tableau below when necessary).

Exercise 3 (Vigenère Cipher)

a) What is the Vigenère Cipher?

Exercise 3 (Vigenère Cipher)

a) What is the Vigenère Cipher?

- The Vigenère cipher chooses a sequence of keys, represented by a string.
- The key letters are applied to successive plaintext characters.
- When the end of the key is reached, the key starts over.
- The length of the key is called the *period* of the cipher.

Exercise 3 (Vigenère Cipher)

b) In the following you are given the key $k =$ "$GOETHE$" and the cyphertext $c =$ "CSWMLRJWWMOISCWMIIGIXBMYRQEFWYY". Identify the message m using the running key variant as given in the lecture. Show the necessary steps (use the Vigenére tableau below when necessary).

c	C	S	W	M	L	R	J	W	W	M	O	I	S	C	W	M	I	I	G	I	X	B	M	Y	R	Q	E	F	W	Y	Y
k	G	O	E	T	H	E	G	O	E	T	H	E	G	O	E	T	H	E	G	O	E	T	H	E	G	O	E	T	H	E	G
m																															

Exercise 3 (Vigenère Tableau)

	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 3 (Vigenère Tableau)

k

		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	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 3 (Vigenère Cipher)

b) In the following you are given the key $k =$ "$GOETHE$" and the cyphertext $c =$ "CSWMLRJWWMOISCWMIIGIXBMYRQEFWYY". Identify the message m using the running key variant as given in the lecture. Show the necessary steps (use the Vigenére tableau below when necessary).

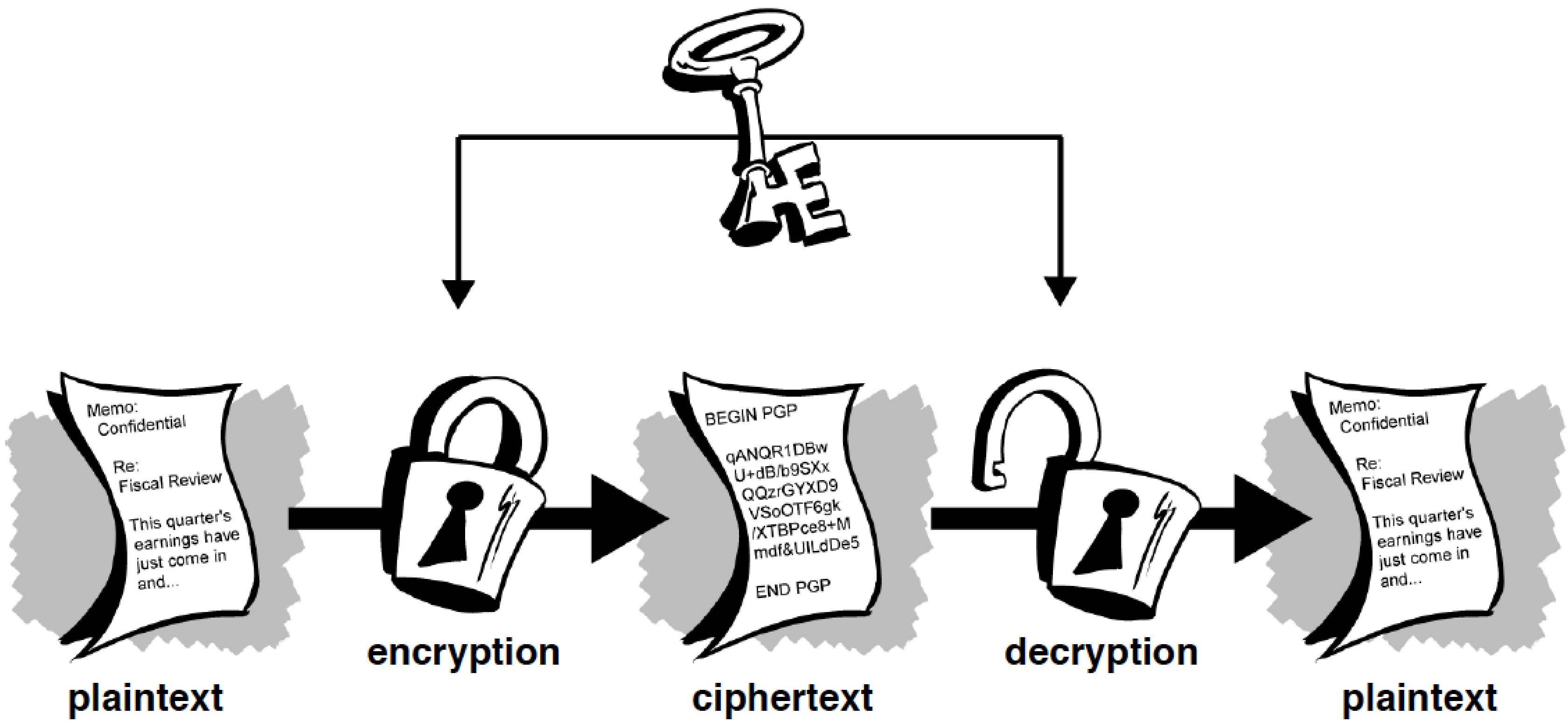
c	C	S	W	M	L	R	J	W	W	M	O	I	S	C	W	M	I	I	G	I	X	B	M	Y	R	Q	E	F	W	Y	Y
k	G	O	E	T	H	E	G	O	E	T	H	E	G	O	E	T	H	E	G	O	E	T	H	E	G	O	E	T	H	E	G
m	W	E	S	T	E	N	D	I	S	T	H	E	M	O	S	T	B	E	A	U	T	I	F	U	L	C	A	M	P	U	S

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 Vigenère cipher is quite easily breakable.
- *Example: The Caesar cipher is a Vigenère cipher with a period of 1.*

[Bi2005]

Guess which crypto system this is



Symmetric or Asymmetric?

Symmetric Encryption

Advantage: Algorithms are very fast

Algorithm	Performance*
RC6	78 ms
SERPENT	95 ms
IDEA	170 ms
MARS	80 ms
TWOFISH	100 ms
DES-ede	250 ms
RIJNDEAL (AES)	65 ms

*** Encryption of 1 MB on a Pentium 2.8 GHz, using the FlexiProvider Java)**

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

Performance of Public Key Algorithms

Algorithm	Performance*	Performance compared to Symmetric encryption (AES)
RSA (1024 bits)	6.6 s	Factor 100 slower
RSA (2048 bits)	11.8 s	Factor 180 slower

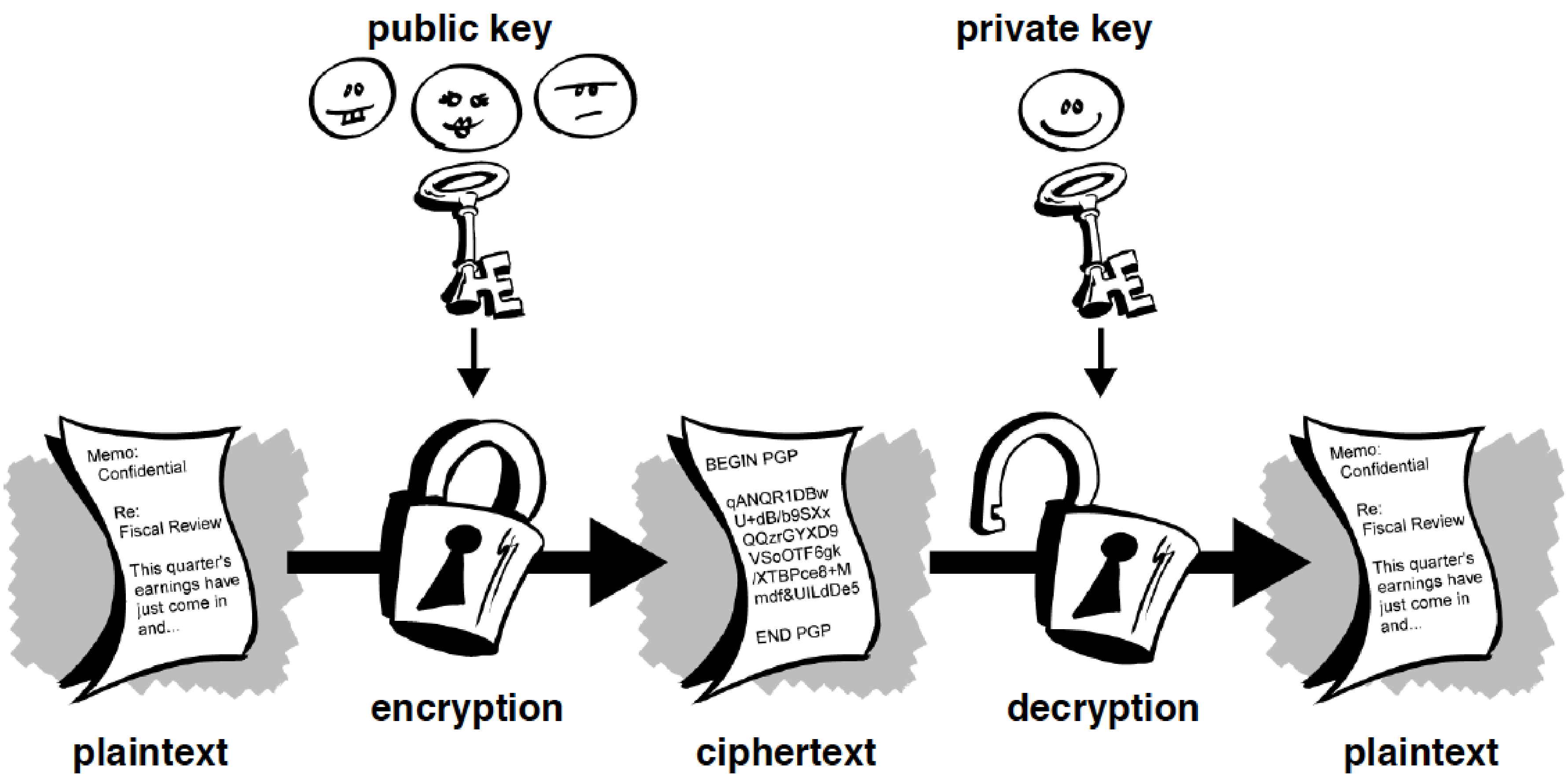
Disadvantage: Complex operations with very big numbers

⇒ **Algorithms are very slow**

*** Encryption of 1 MB on a Pentium 2.8 GHz, using the FlexiProvider (Java)**

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

This crypto system is…?



Symmetric or Asymmetric?

Exercise 4 (Asymmetric Cryptosystems and RSA)

a) Describe differences between symmetric and asymmetric cryptosystems.

b) Alice wants to send a message m to Bob. Because the message is a secret, Alice encrypts the message using RSA. Complete the flow chart below and also show the necessary calculation steps for encryption and decryption. Indicate which information are public or known only by Bob or Alice.

c) Consider a RSA cryptosystem. The following keys were made public: e=5, n=21.
   i. Encrypt the message m=3 using RSA
   ii. Determine p and q.
   iii. Determine the private key d.
   iv. Decrypt the cyphertext and check that the result is m=3
   v. What is the problem with the chosen keys?

d) Decrypt the message c = 7 using RSA. The private key of the receiver is $d = 4$ and $n = 13$.

e) Why is it possible to break RSA with Post-Quantum Cryptography?

Exercise 4 (Asymmetric Cryptosystems and RSA)

a) Describe differences between symmetric and asymmetric cryptosystems.

Exercise 4 (Asymmetric Cryptosystems and RSA)

a) Describe differences between symmetric and asymmetric cryptosystems.

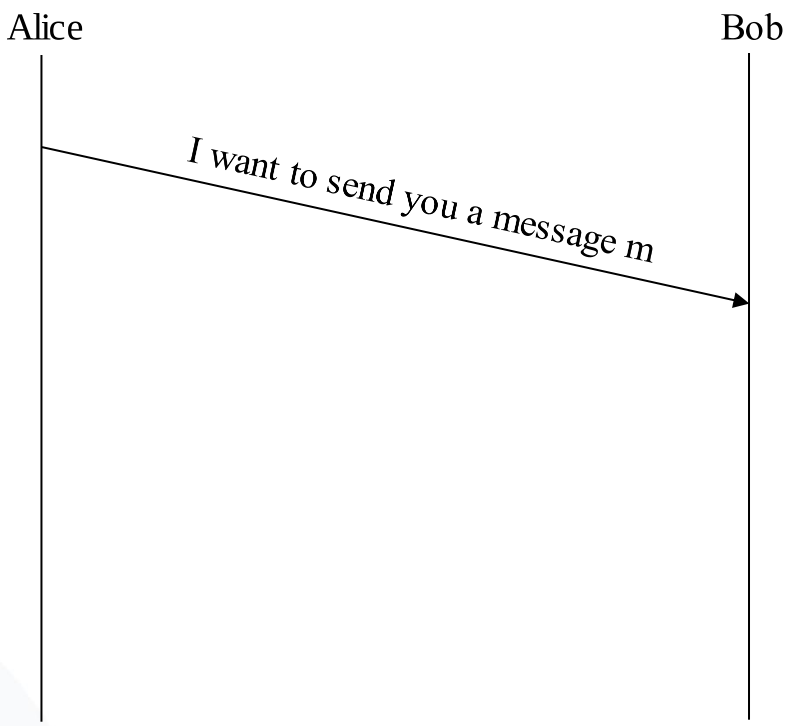
Symmetric	Asymmetric
Both encryption and decryption are done with the same key.	Encryption with public key, decryption with private key.
One key per communication pair is necessary.	Does not require a secure communication channel. Public key can be freely distributed.
Efficient in terms of performance	Less efficient
Keys have to be kept secret	Only keep own private key secret
Secure agreement and transfer are necessary.	Does not require agreement on a shared key.
A centre for key distribution is possible but this party then knows all secret keys!	A centre for key distribution is possible and this party does not know the secret keys.

Exercise 4 (Asymmetric Cryptosystems and RSA)

b) Alice wants to send a message *m* to Bob. Because the message is a secret, Alice encrypts the message using RSA. Complete the flow chart below and also show the necessary calculation steps for encryption and decryption. Indicate which information are public or known only by Bob or Alice.

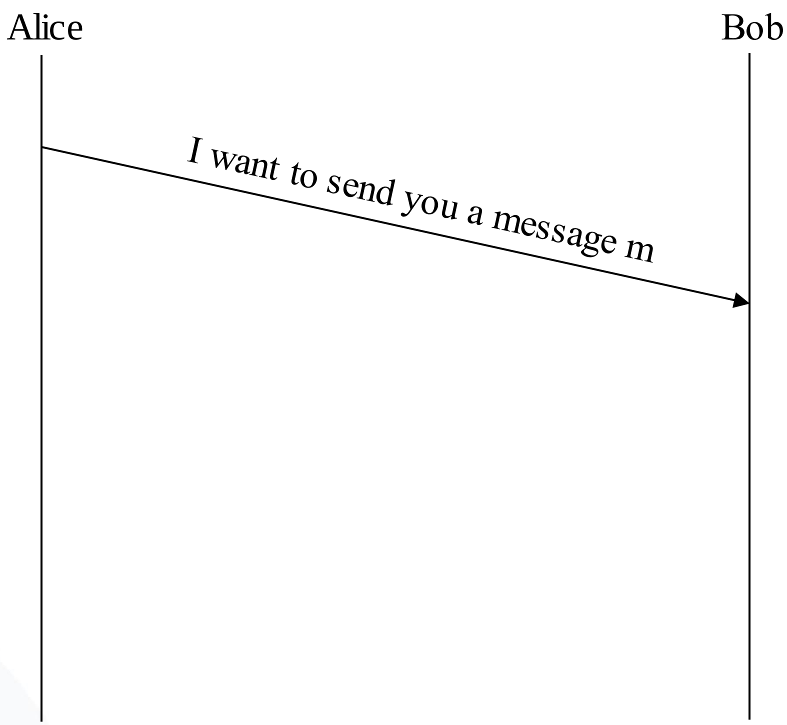
Exercise 4 (Asymmetric Cryptosystems and RSA)

- Alice has a message m



Exercise 4 (Asymmetric Cryptosystems and RSA)

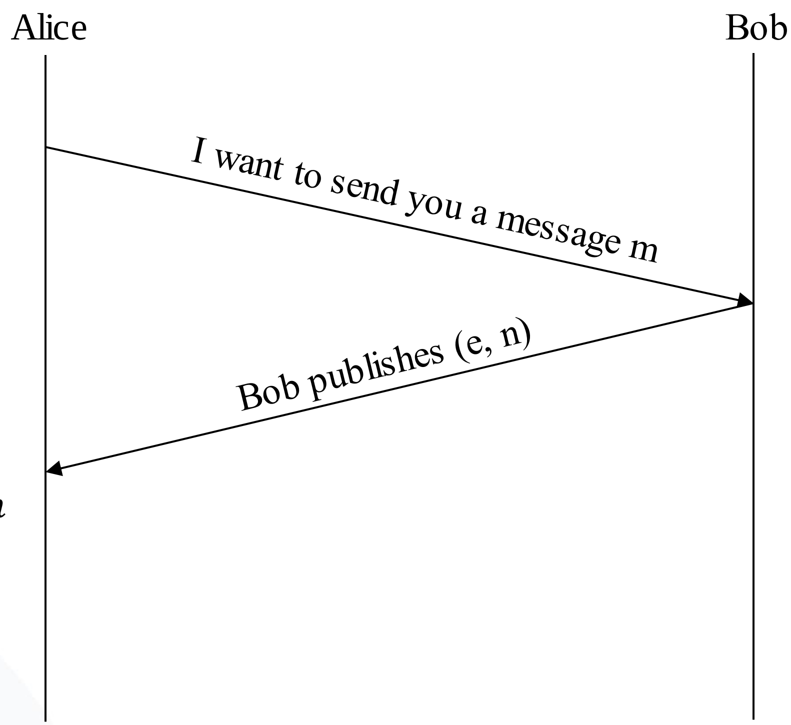
- Alice has a message m



- Bob chooses p, q
- Bob calculates $n = p * q$
- Bob chooses public key e that $1 < e < (p-1)(q-1)$ and $\gcd\big(e, (p-1)(q-1)\big) = 1$
- Computes a modular inverse d that: $1 < d < (p-1)(q-1)$ and $ed \equiv 1 \bmod (p-1)(q-1)$

Exercise 4 (Asymmetric Cryptosystems and RSA)

- Alice has a message m

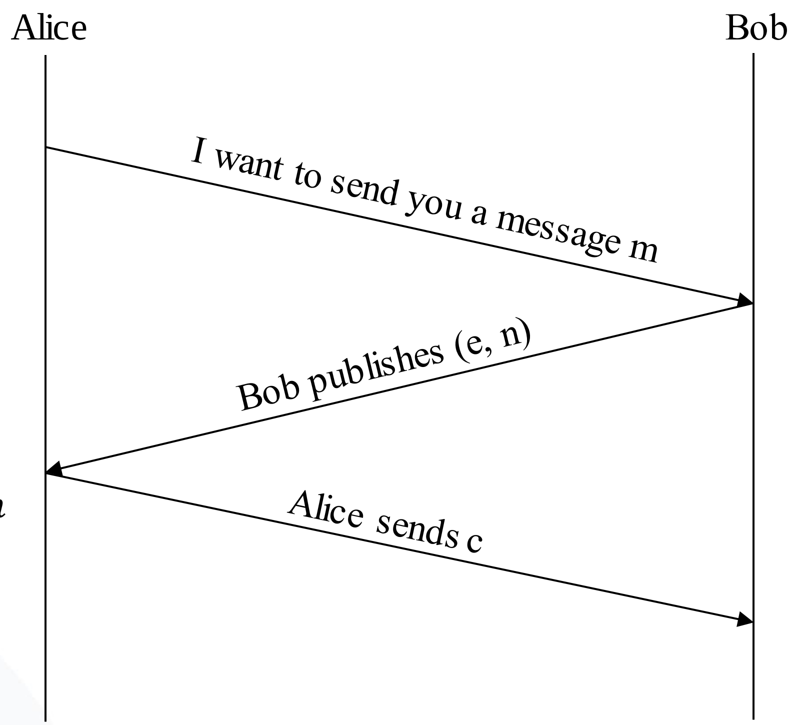


- Bob chooses p, q
- Bob calculates $n = p * q$
- Bob chooses public key e that $1 < e < (p-1)(q-1)$ and $\gcd\big(e, (p-1)(q-1)\big) = 1$
- Computes a modular inverse d that: $1 < d < (p-1)(q-1)$ and $ed \equiv 1 \bmod (p-1)(q-1)$

- Alice calculates $c = m^e \mod n$

Exercise 4 (Asymmetric Cryptosystems and RSA)

- Alice has a message m
- Alice calculates $c = m^e \mod n$



- Bob chooses p, q
- Bob calculates $n = p * q$
- Bob chooses public key e that $1 < e < (p-1)(q-1)$ and $\gcd\big(e, (p-1)(q-1)\big) = 1$
- Computes a modular inverse d that: $1 < d < (p-1)(q-1)$ and $ed \equiv 1 \bmod (p-1)(q-1)$
- Bob computes $m = c^d \mod n$ and can now read the message

Exercise 4 (Asymmetric Cryptosystems and RSA)

c) Consider a RSA cryptosystem. The following keys were made public: $e = 5$, $n = 21$.

   i. Encrypt the message $m = 3$ using RSA
   ii. Determine p and q.
   iii. Determine the private key d.
   iv. Decrypt the cyphertext and check that the result is $m = 3$
   v. What is the problem with the chosen keys?

Exercise 4 (Asymmetric Cryptosystems and RSA)

c.i Encrypt the message $m = 3$ using RSA. The following keys were made public: $e = 5$, $n = 21$.

Solution: $c = m^e \mod n$

$c = 3^5 \mod 21$

$c = 243 \mod 21$

$c = 12$

c.ii Determine p and q (Factorize n).

mobile business

Exercise 4 (Fermat‘s Factorization)

- Let p, q be prime and $n = pq$. Fermat’s factoring represents *N* as a difference of 2 squares:
- $\boldsymbol{n = x^2 - y^2 = (x + y)(x - y))}$.
- First, we start with x = $\lceil \sqrt{n} \rceil$ and then increase x by 1 until $x^2 - n$ is square (so that we can derive y) so that $\boldsymbol{n} = x^2 - y^2$ holds.
- This method works because we can represent n as a difference of 2 squares:
- $pq = (\frac{1}{2}(p + q)^2 - (\frac{1}{2}(p - q)^2)^2 = x^2 - y^2$.
- You will find this explanation with more details in Knospe 2019, p. 178 f.

c.ii Determine p and q (Factorize n).

- Let $n = 21$; then we first set $x \approx \sqrt{n}$. We obtain $x = ???$ and derive $x^2 - n = ???$. Because 4 is square we know that $y = ???$. From above we know that $pq = (x + y)(x - y)$ so we receive $??? = ??? \cdot ???$.

Exercise 4 (Asymmetric Cryptosystems and RSA)

c.ii Determine p and q (Factorize n).

- Let $n = 21$; then we first set $x \approx \sqrt{n}$. We obtain $x = 5$ and derive $x^2 - n = 4$. Because 4 is square we know that $y =$???. From above we know that $pq = (x + y)(x - y)$ so we receive $21 = ??? \cdot ???$.

c.ii Determine p and q (Factorize n).

- Let $n = 21$; then we first set $x \approx \sqrt{n}$. We obtain $x = 5$ and derive $x^2 - n = 4$. Because 4 is square we know that $y = 2$. From above we know that $pq = (x + y)(x - y)$ so we receive $21 = ???\cdot???$.

Exercise 4 (Asymmetric Cryptosystems and RSA)

c.ii Determine p and q (Factorize n).

- Let $n = 21$; then we first set $x \approx \sqrt{n}$. We obtain $x = 5$ and derive $x^2 - n = 4$. Because 4 is square we know that $y = 2$. From above we know that $pq = (x + y)(x - y)$ so we receive $21 = 7 \cdot 3$.

Exercise 4 (Asymmetric Cryptosystems and RSA)

c.iii Determine d.

c.iii Determine d.

Solution:

$\phi(n) = (p-1)(q-1)$

$\phi(n) = 12$

$d \cdot e \equiv 1 \, mod \, \phi(n) \; and \; 1 < d < \phi(n)$

$d \cdot 5 \equiv 1 \, mod \, 12$

$d \cdot 5 \equiv 1 \, mod \, 12$

$d = 5$

$1 < 5 < 12$ ✓

$12 \rightarrow +1 \rightarrow 13$

$24 \rightarrow +1 \rightarrow 25$

c.iv Decrypt the cyphertext and check that the result is $m = 3$

Exercise 4 (Asymmetric Cryptosystems and RSA)

c.iv Decrypt the cyphertext and check that the result is m = 3

Solution: $m = c^d \bmod n$

$m = 12^5 \bmod 21$

$m = 248832 \bmod 21$

$m = 3$ ✓

Simple Way

2 4 8 8 3 2 : 2 1 = 1 1 8 9

```
2 1
---
  3 8
  2 1
  -----
  1 7 8
  1 6 8
  -----
    1 0 3
      8 4
    -----
      1 9 2
      1 8 9
      -----
          3
```

Only for small exponents

Excursus - Modular exponentiation

1	2	3	4	5	6
21	42	63	84	105	126

$m = \; 12^5 \mod 21$

$12 \equiv 12 \mod 21$

$12^2 \equiv 144 \mod 21 \equiv 18$

$12^4 \equiv 12^2 \cdot 12^2 \equiv 18 \cdot 18 \equiv 18^2 \mod 21 \equiv 9$

$12^5 \equiv 12^4 \cdot 12 \equiv 9 \cdot 12 \mod 21$

$m = 108 \mod 21$

$m = 3$

c.v What is the problem with the chosen keys?

Solution:

- Too short, a modulus with up to around 1000 bits can be factored (in 2019).

Exercise 4 (Asymmetric Cryptosystems and RSA)

d) Decrypt the message c = 2 using RSA. The private key of the receiver is $d = 3$ and $n = 15$.

Exercise 4 (Asymmetric Cryptosystems and RSA)

d) Decrypt the message c = 2 using RSA. The private key of the receiver is $d = 3$ and $n = 15$.

Solution: $m = c^d \mod n$

$8 = 2^3 \mod 15$

Exercise 4 (Asymmetric Cryptosystems and RSA)

e) Let $n = 221$. Use Fermat's factorization to factorize n. (Hint: $n = x^2 - y^2 = (x + y)(x - y)$)

Exercise 4 (Asymmetric Cryptosystems and RSA)

e) Let $n = 221$. Use Fermat's factorization to factorize n.
(Hint: $n = x^2 - y^2 = (x+y)(x-y)$)

Solution: $n = x^2 - y^2$
$\sqrt{221} \approx 14.87$

Start with $x = 15$
$x^2 - n = y^2$, *put in the numbers*
$225 - 221 = 4$, *this is a square. We receive*
$y = 2$ *(If we do not receive a square we try* $x = 16 \ldots$*)*

$n = (x+y)(x-y) = (15+2)(15-2) = 17 \cdot 13$

(Only efficient if prime factors are close)

Exercise 4 (Asymmetric Cryptosystems and RSA)

f) Why can Post-Quantum Cryptography break RSA?

Exercise 4 (Asymmetric Cryptosystems and RSA)

f) Why can Post-Quantum Cryptography break RSA?

Solution: RSA is based on the difficulty to solve a factoring problem. “Shor’s factoring algorithm leverages the Quantum Fourier Transform to solve factoring problems in polynomial time.” [Kn19]

Assessment of RSA

- “RSA [currently] considered as secure against non quantum computers”
  - Prime factors randomly chosen
  - Prime factors more than 1000 bits longs

[Kn19, p. 182]

Thank you!

Questions: security@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.
- **[Kn19]** Knospe, Heiko. A Course in Cryptography. Vol. 40. American Mathematical Soc., 2019. https://ebookcentral.proquest.com/lib/senc/reader.action?docID=5962876
- **[Bi05]** Bishop, Matt: *Introduction to Computer Security*. Boston: Addison Wesley, 2005. pp. 113-116.