Assignment 3 - Cryptography

Information & Communication Security
(WS 2016/17)

Ahmed S. Yeusf, M.Sc.

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

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)

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

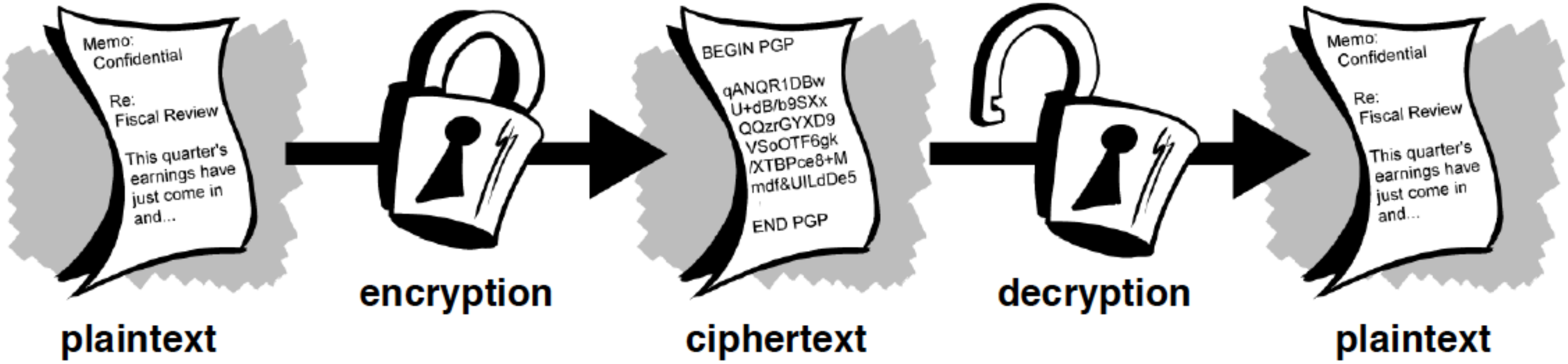
- The key is 8
- The plain text is:

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.

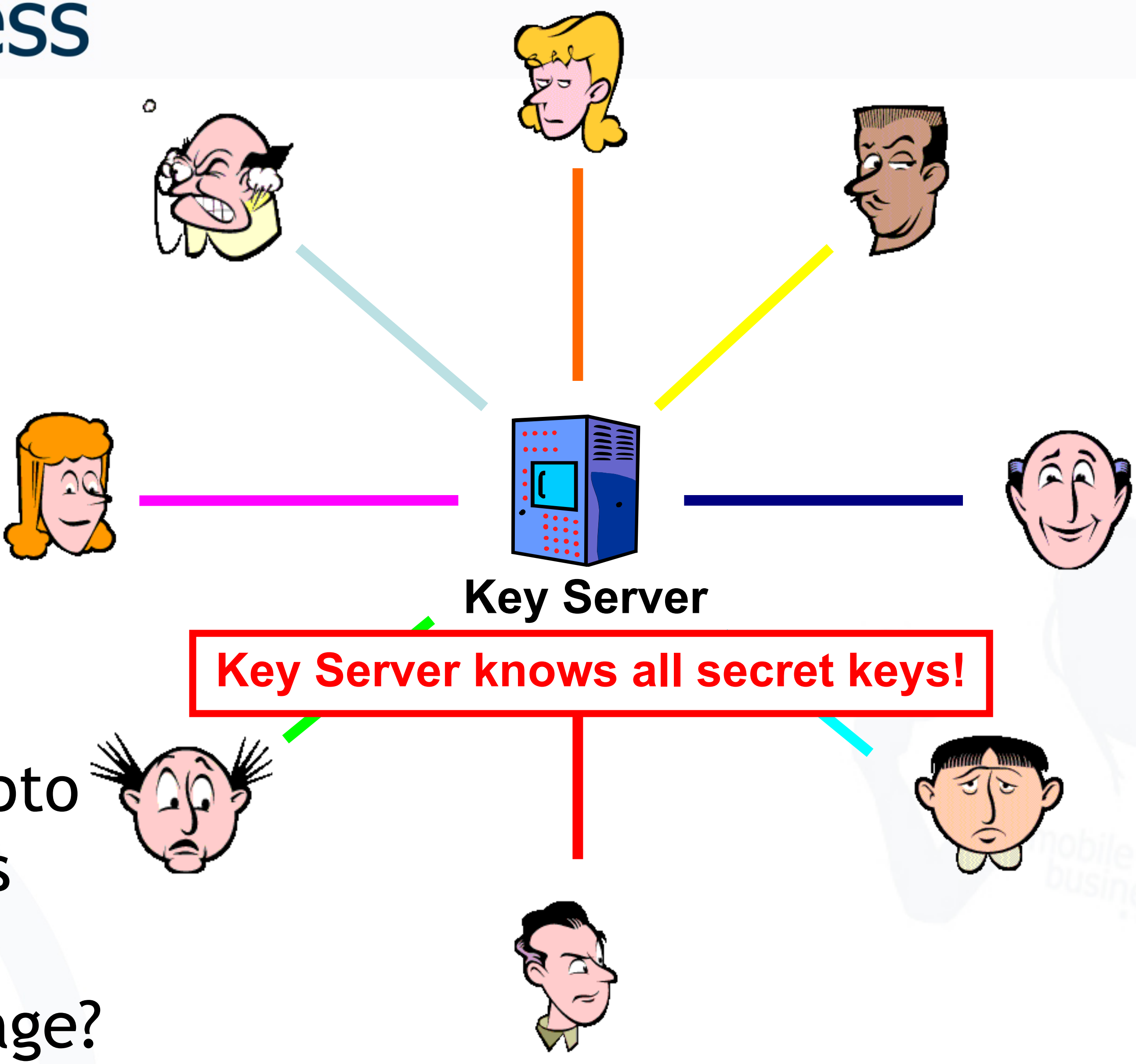
Encryption - Decryption



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

Exercise 2: Symmetric vs. asymmetric crypto

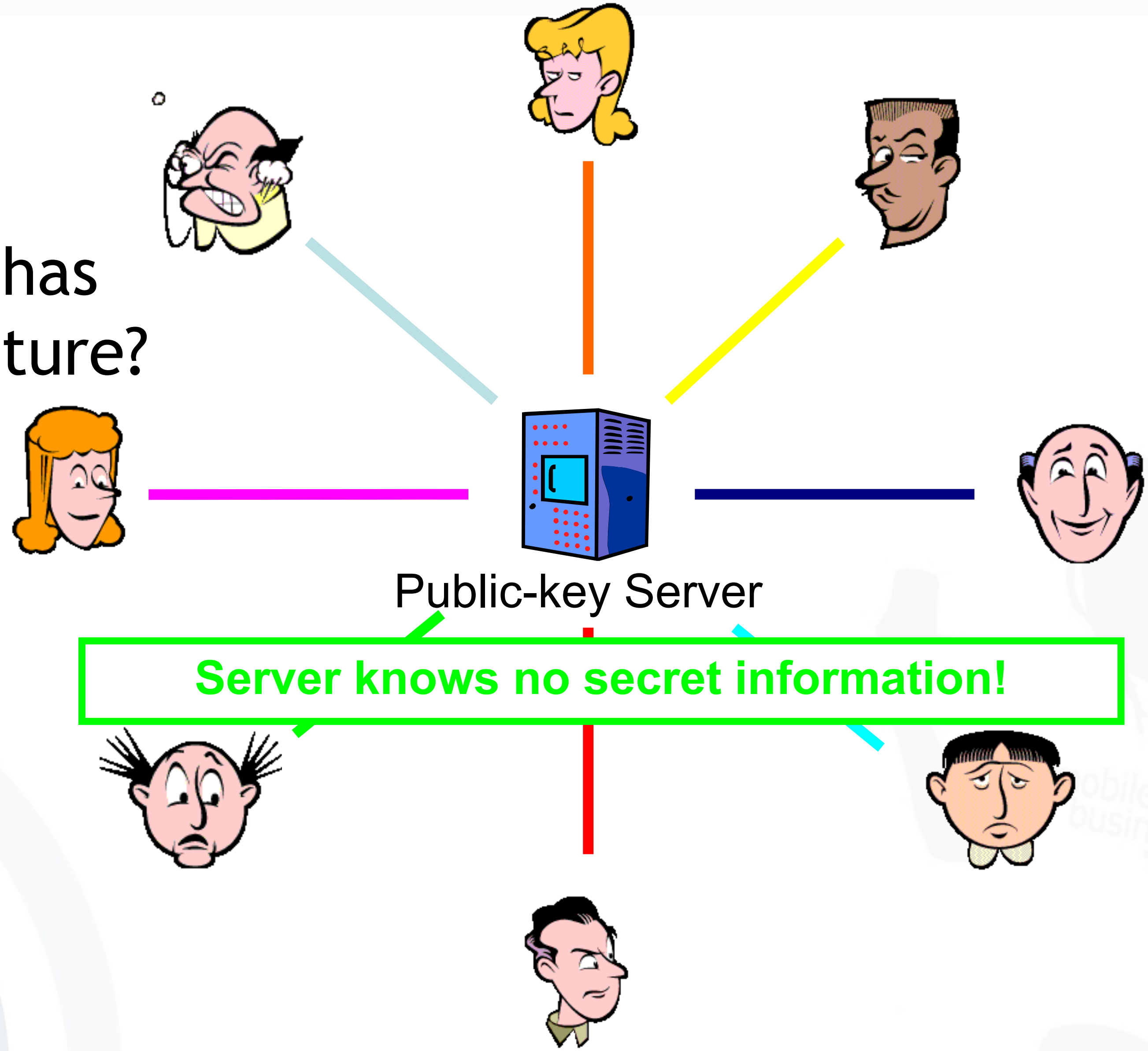
What is the difference between symmetric and asymmetric crypto systems?



Key Server knows all secret keys!

Which crypto system has this disadvantage?

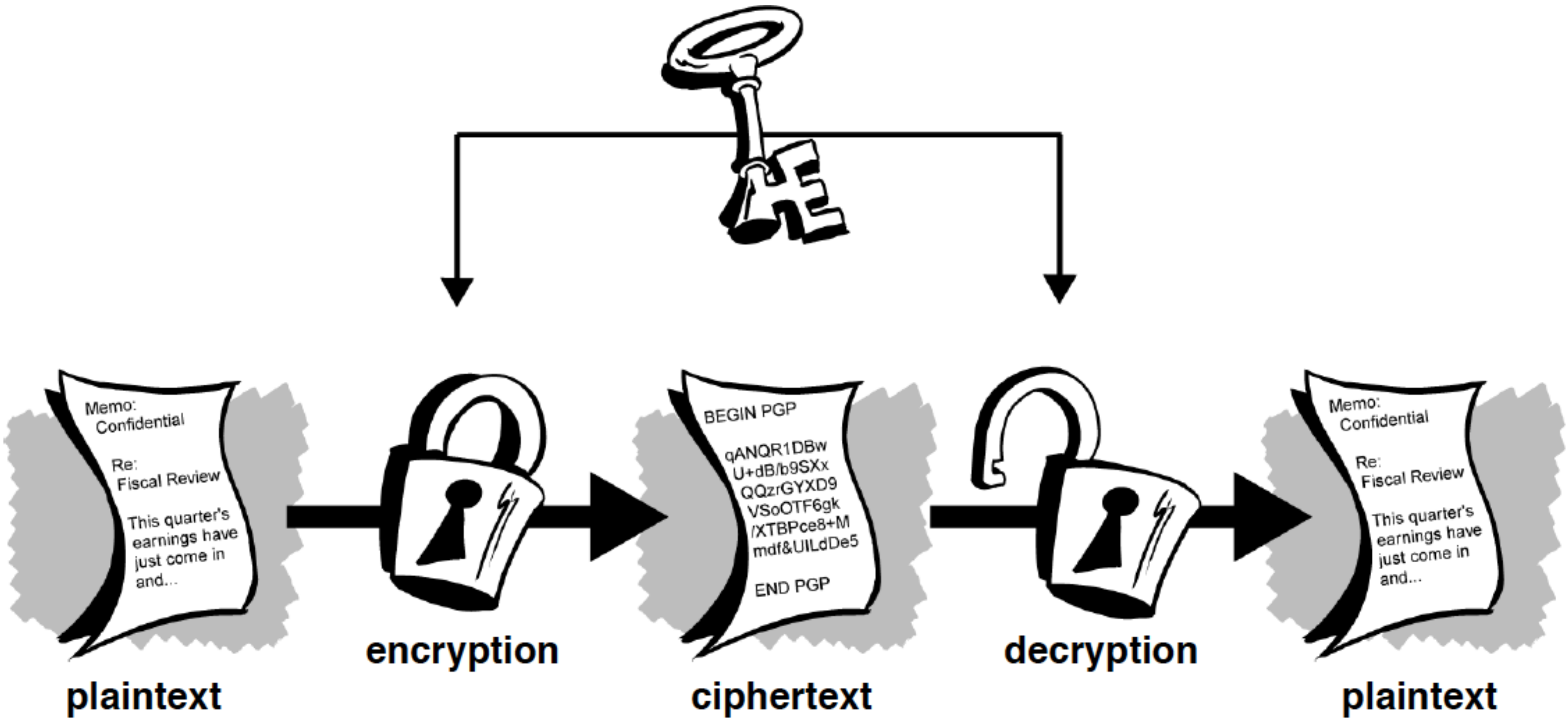
Which crypto system has this feature?



Public-key Server

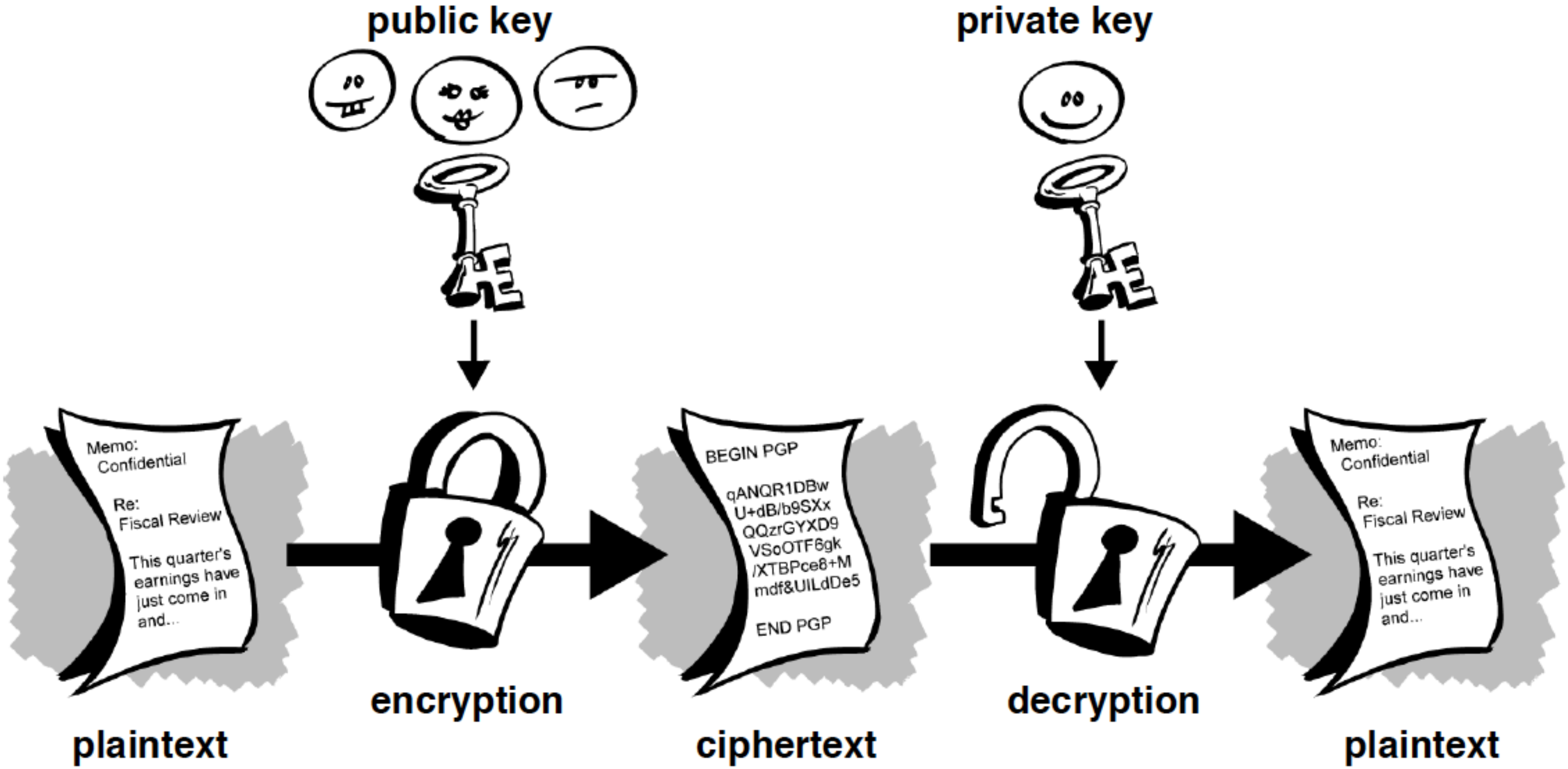
Server knows no secret information!

Guess which crypto system this is



Symmetric or Asymmetric?

This crypto system 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]

Summary

Differences between symmetric and asymmetric cryptosystems.

Symmetric	Asymmetric
Both encryption and decryption is 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 center for key distribution is possible but this party then knows all secret keys!	A center for key distribution is possible and this party does not know the secret keys.

Exercise 3: Stream ciphers

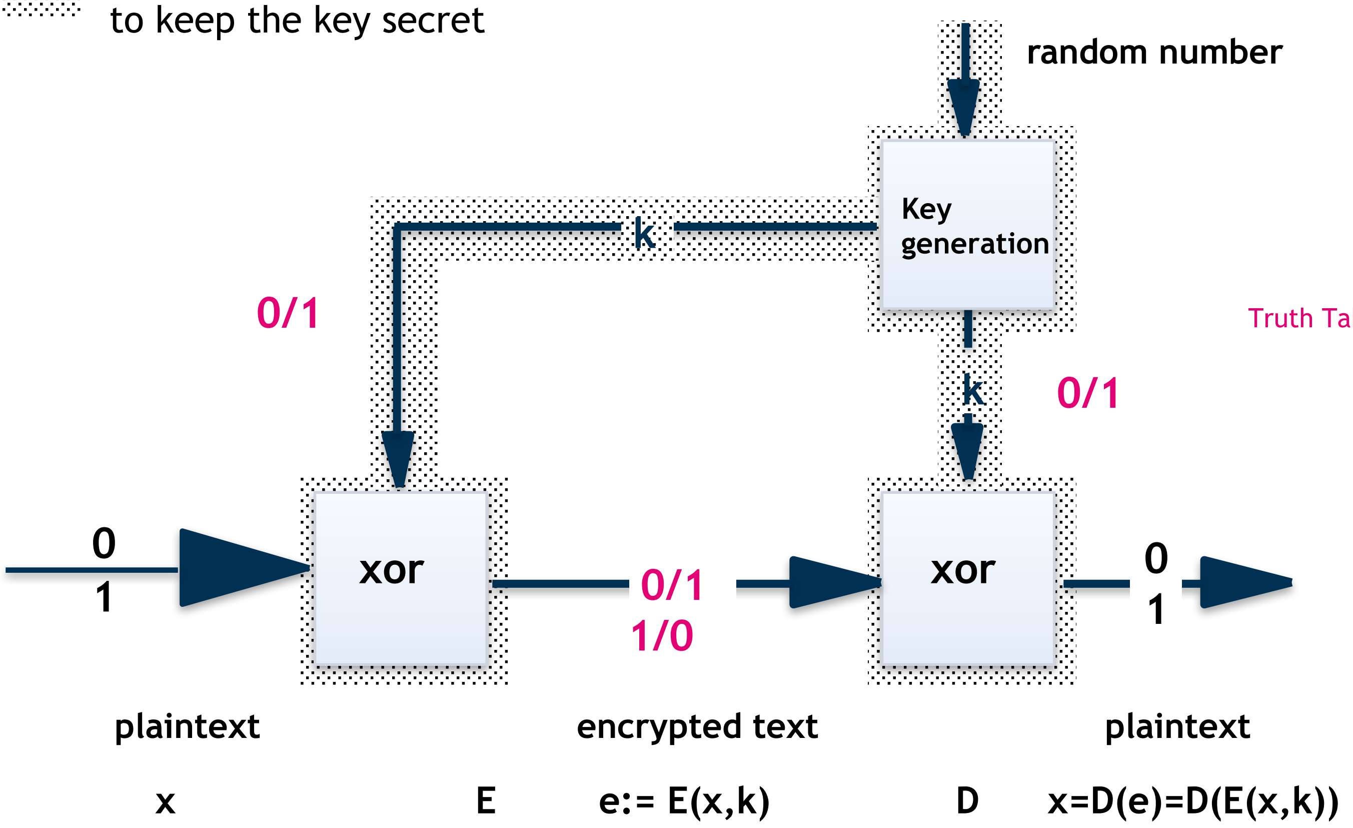
a) What is a one-time pad (Vernam-code)?

One Time Pad

- 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.

Example One Time Pad

▨ 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

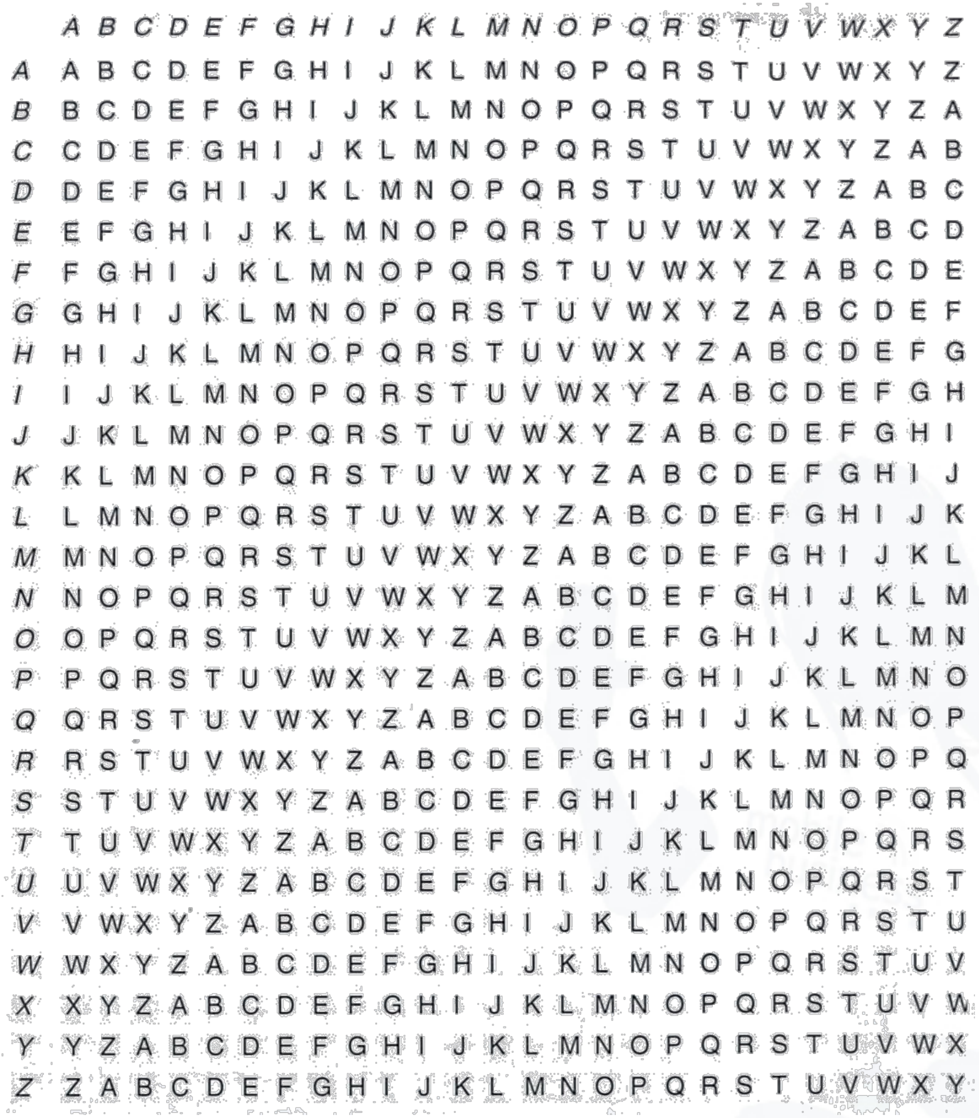
X_i	S_i	Y_i
0	0	0
0	1	1
1	0	1
1	1	0

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 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 4(a): Vigenére Cipher

- The Vigenére 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.

[Bi2005]

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]

Thank you!

Questions: sec@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.