

## *Lecture 4*

# Cryptography I

Information & Communication Security  
(WS 2010/11)

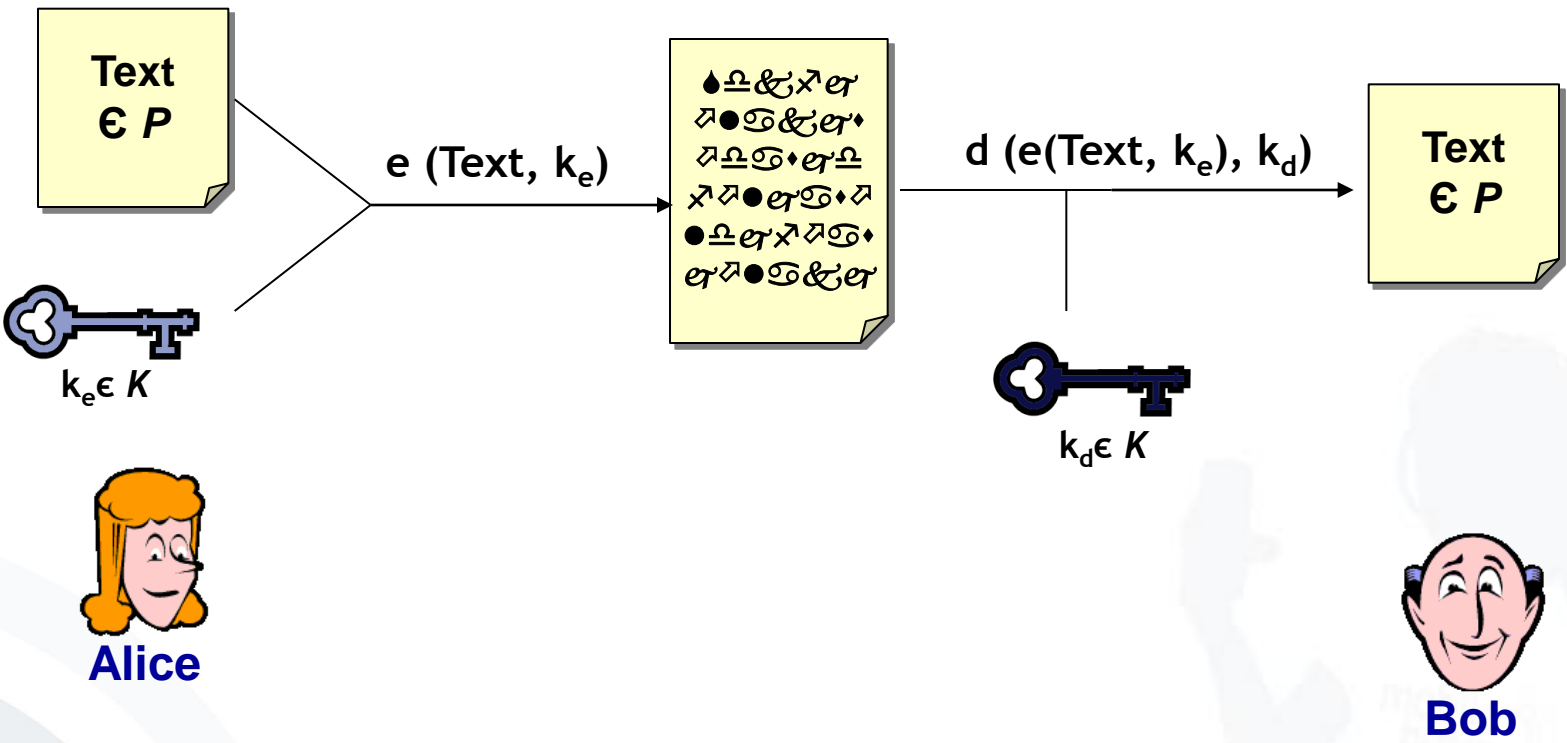
Prof. Dr. Kai Rannenberg

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



- Introduction
- Classical cryptosystems
  - General concept
  - Substitution ciphers
    - Caesar cipher
    - Vigenère cipher
    - One time pad
  - AES
  - Advantages and Problems
- Public key cryptography

- A Cryptosystem is a 5-tuple  $(E, D, P, K, C)$ :
  - A set  $P$  of plaintexts
  - A set  $K$  of keys
  - A set  $C$  of ciphertexts
  - A set  $E$  of enciphering functions, with  $E: P \times K \rightarrow C$
  - A set  $D$  of deciphering functions, with  $D: C \times K \rightarrow P$



- Intention
  - Confidentiality (secrecy of messages):  
**encryption systems**
  - Integrity (protection from undetected manipulation) and accountability:  
**authentication systems** and **digital signature systems**
- Key distribution
  - **Symmetric:**  
Both partners have the same key.
  - **Asymmetric:**  
Different (but related) keys for encryption and decryption
- In practice mostly hybrid systems

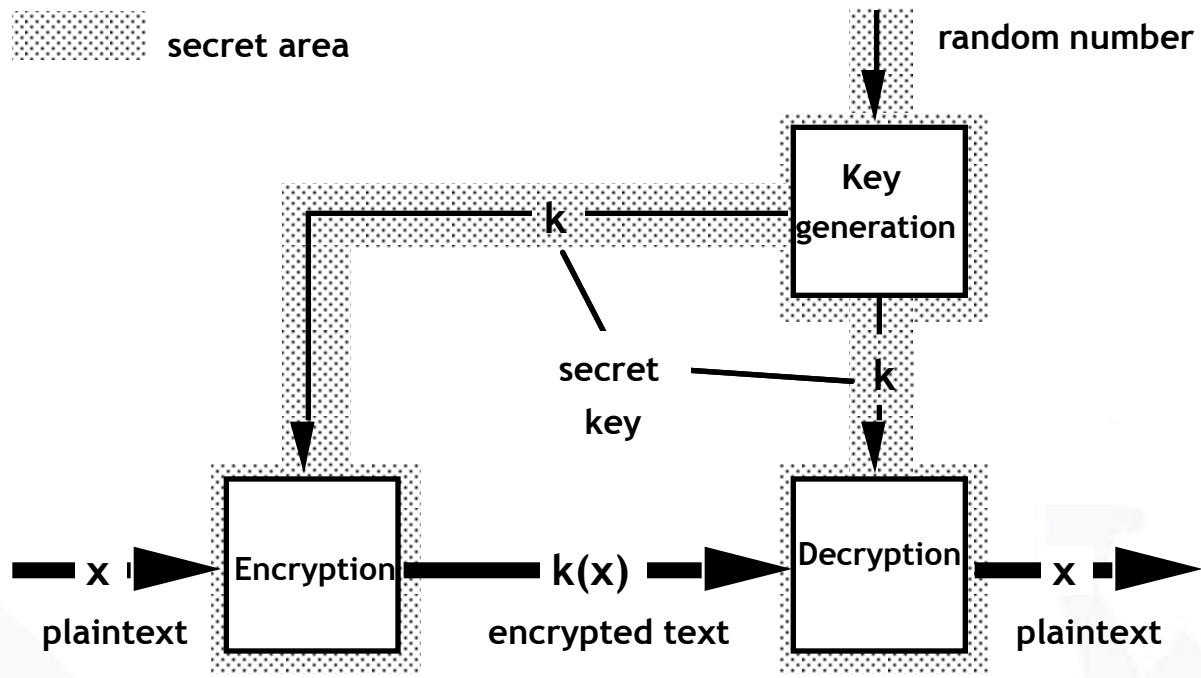
- In a ***ciphertext only*** attack, the adversary has only the ciphertext. Her goal is to find the corresponding plaintext. If possible, she may try to find the key, too.
- In a ***known plaintext*** attack, the adversary has the plaintext and the ciphertext that was enciphered. Her goal is to find the key that was used.
- In a ***chosen plaintext*** attack, the adversary may ask that specific plaintexts be enciphered. She is given the corresponding ciphertexts. Her goal is to find the key that was used.

- Introduction
- Classical cryptosystems
  - General concept
  - Substitution ciphers
    - Caesar cipher
    - Vigenère cipher
    - One time pad
  - AES
  - Advantages and Problems
- Public key cryptography

- Typical applications
  - confidential storage of user data
  - transfer of data between 2 users who negotiate a key via a secure channel
- Examples
  - Vernam-Code (one-time pad, Gilbert Vernam)
    - key length = length of the plaintext (information theoretically secure)
  - DES: Digital Encryption Standard
    - key length 56 bit, so  $2^{56}$  different keys
  - AES: Advanced Encryption Standard (Rijndael, [NIST])
    - 3 alternatives for key length: 128, 192 und 256 bit

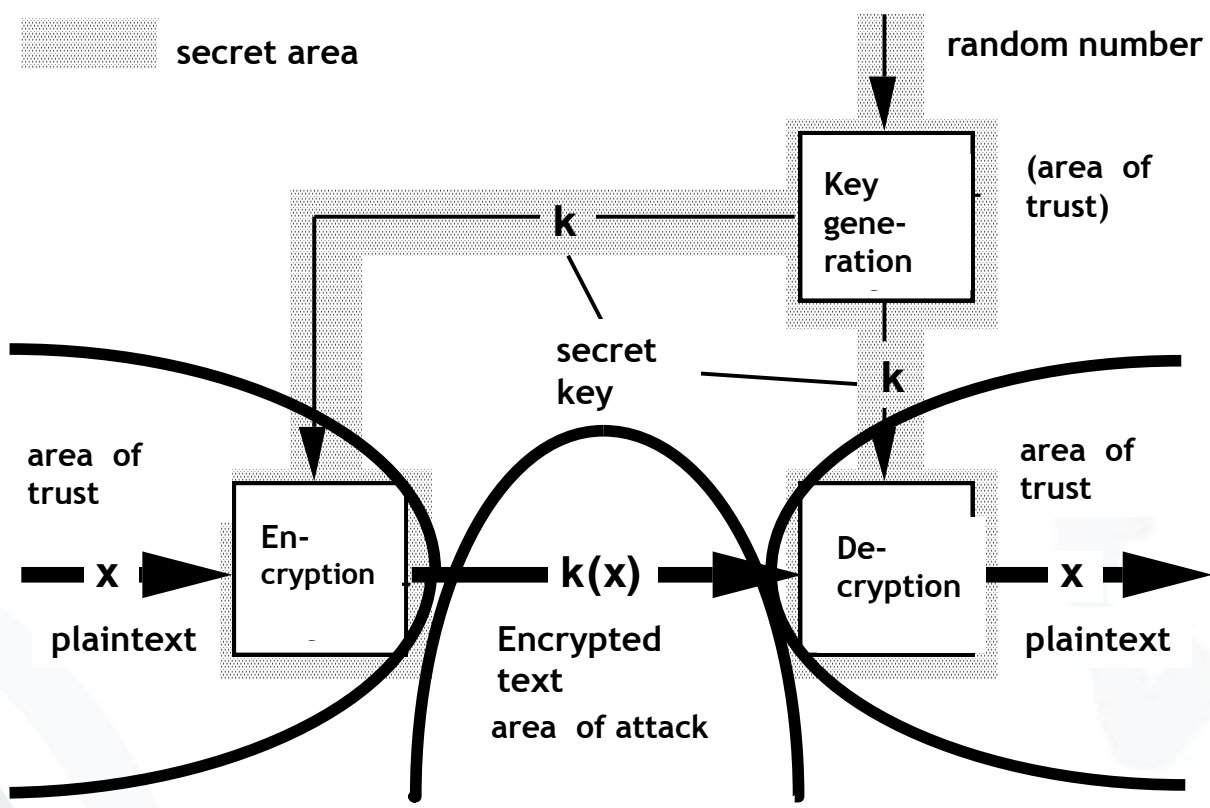
- Introduction
- Classical cryptosystems
  - General concept
  - Substitution ciphers
    - Caesar cipher
    - Vigenère cipher
    - One time pad
  - AES
  - Advantages and Problems
- Public key cryptography

# Symmetric Encryption Systems



*black box with lock, two equal keys*

# Symmetric Encryption Systems



- **Keys have to be kept secret.**  
*(secret key crypto system)*
- It must not be possible to infer on the plaintext or the keys used from the encrypted text (ideally encrypted text is not distinguishable from a numerical random sequence).
- Each key shall be equally probable.
- In principle each system with limited key length is breakable by testing all possible keys.
- **Publication of encoding and decoding functions (algorithms) is considered as good style and is trust-building.**

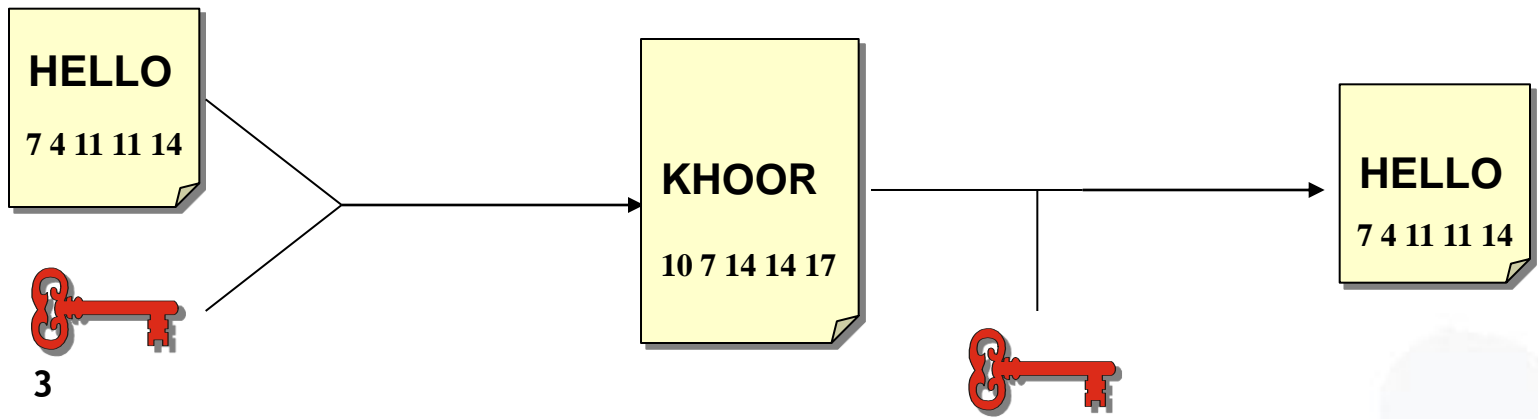
- Introduction
- Classical cryptosystems
  - General concept
  - Substitution ciphers
    - Caesar cipher
    - Vigenère cipher
    - One time pad
  - AES
  - Advantages and Problems
- Public key cryptography

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.

- For  $k \in \{0..25\}$  we have:
- An encryption function  
 $e: x \rightarrow (x+k) \bmod 26$
- A decryption function  
 $d: x \rightarrow (x-k) \bmod 26$
  
- In this case  $k_e = k_d$
- This is not always the case.



- In case of a known plaintext attack it is trivial to get the key used.
- There are only 26 possible keys. This cipher is therefore vulnerable to a brute force attack.
- This cipher is also vulnerable to a statistical ciphertext-only attack.

- Of course this is a 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.

# Can We Make it More Secure?

- Use a permutation of the alphabet as the key.
- Example:

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

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

- “HELLO” -> “ITSSG”

- Use of permutations increases the key space.
- Therefore, a brute force attack becomes more difficult.
- The encryption and decryption are not much harder to compute.
  - Table lookup
- Still vulnerable to a statistical ciphertext-only attack.

# Statistical Ciphertext-only Attack

- Use statistical frequency of occurrence of single characters to figure out the key.
- Language dependent
- Frequencies of character pairs (bigrams) may also be used

<b>E</b>	<b>11.1607%</b>	<b>M</b>	<b>3.0129%</b>
<b>A</b>	<b>8.4966%</b>	<b>H</b>	<b>3.0034%</b>
<b>R</b>	<b>7.5809%</b>	<b>G</b>	<b>2.4705%</b>
<b>I</b>	<b>7.5448%</b>	<b>B</b>	<b>2.0720%</b>
<b>O</b>	<b>7.1635%</b>	<b>F</b>	<b>1.8121%</b>
<b>T</b>	<b>6.9509%</b>	<b>Y</b>	<b>1.7779%</b>
<b>N</b>	<b>6.6544%</b>	<b>W</b>	<b>1.2899%</b>
<b>S</b>	<b>5.7351%</b>	<b>K</b>	<b>1.1016%</b>
<b>L</b>	<b>5.4893%</b>	<b>V</b>	<b>1.0074%</b>
<b>C</b>	<b>4.5388%</b>	<b>X</b>	<b>0.2902%</b>
<b>U</b>	<b>3.6308%</b>	<b>Z</b>	<b>0.2722%</b>
<b>D</b>	<b>3.3844%</b>	<b>J</b>	<b>0.1965%</b>
<b>P</b>	<b>3.1671%</b>	<b>Q</b>	<b>0.1962%</b>

(English)

- Introduction
- Classical cryptosystems
  - General concept
  - Substitution ciphers
    - Caesar cipher
    - Vigenère cipher
    - One time pad
  - AES
  - Advantages and Problems
- Public key cryptography

- 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.

	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

- Let the message be „THE BOY HAS THE BAG“ and let the key be „VIG“:

- Plaintext: THEBOYHASTHEBAG
- Key: VIGVIGVIGVIGVIG
- Ciphertext: OPKWECEIYOPKWIM

- For many years, the Vigenère cipher was considered unbreakable.
- 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.

## Example Vigenère Cipher

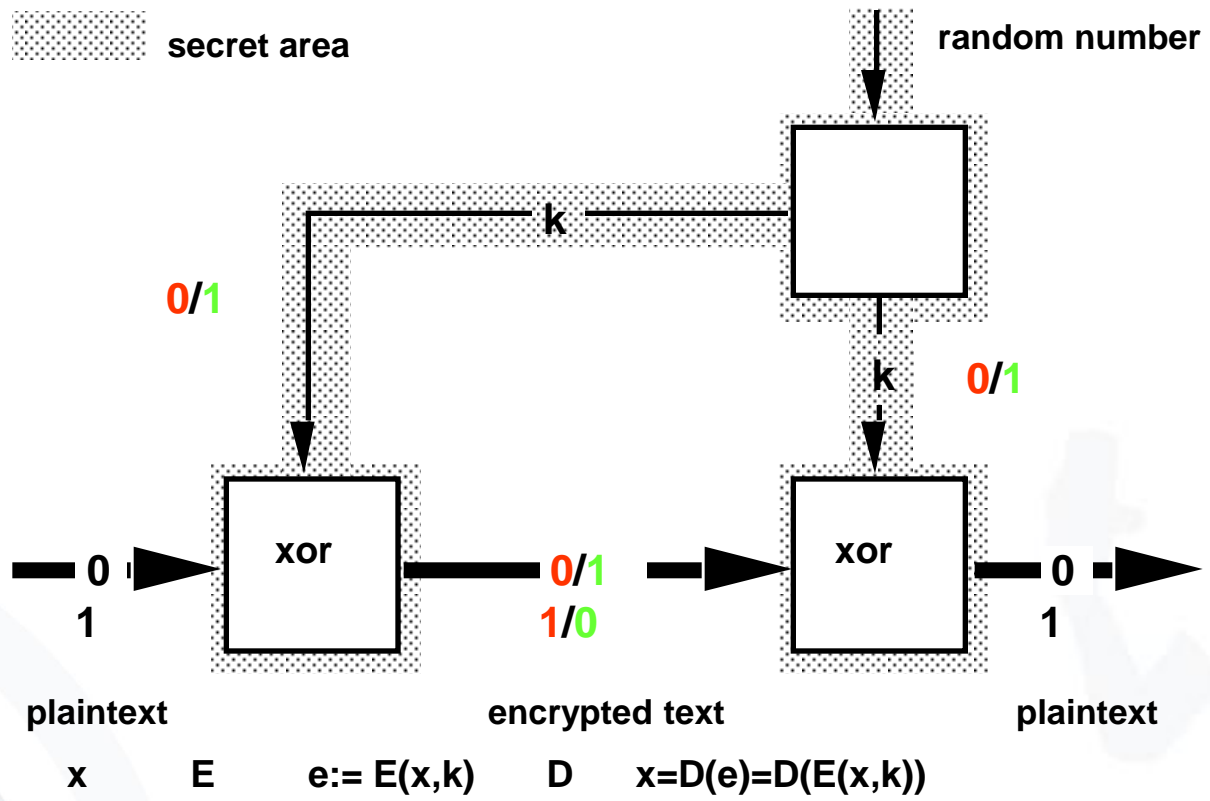
- Let the message be „THE BOY HAS THE BAG“ and let the key be „VIG“:

- Plaintext: THEBOYHASTHEBAG
- Key: VIGVIGVIGVIGVIG
- Ciphertext: OPKWWECIYOPKWIM

- Introduction
- Classical cryptosystems
  - General concept
  - Substitution ciphers
    - Caesar cipher
    - Vigenère cipher
    - One time pad
  - AES
  - Advantages and Problems
- Public key cryptography

- Invented by Gilbert Vernam
- The one-time pad is basically a Vigenère cipher.
- The length of the key is as long as the length of the plaintext.
- Therefore, there are no periodic reoccurrences.
- The key is randomly chosen and only used once.
- Every key has the same probability.

# Example One Time Pad



- The one time pad is unbreakable by ciphertext only attacks.
  - Example: Let the ciphertext be “FGHA”.
  - Since we know the key length is at least 4 and the probability of every possible key is equal, the plaintext can be any 4-letter word possible.
- In a known plaintext attack we can deduct the key.
  - Then we know which key was used to encrypt the message we already know.
  - But the next message is encrypted with a different key, because every key is only used once.
- The same applies to a chosen plaintext attack.
- **The one-time pad is information theoretically secure and provably impossible to break.**

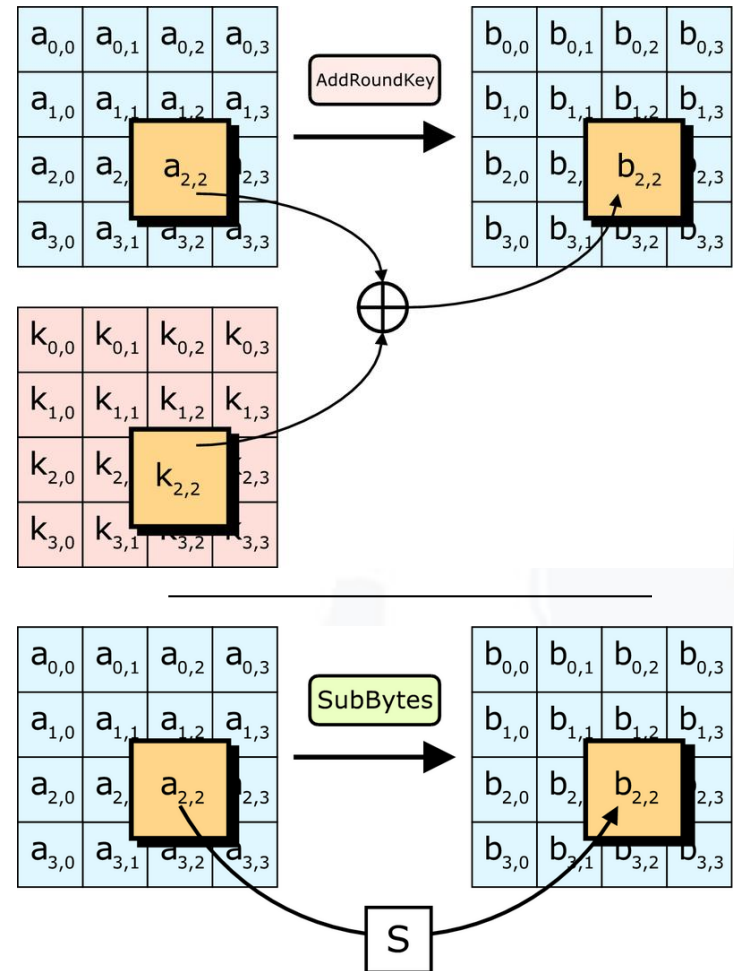
- Introduction
- Classical cryptosystems
  - General concept
  - Substitution ciphers
    - Caesar cipher
    - Vigenère cipher
    - One time pad
  - AES
  - Advantages and Problems
- Public key cryptography

- The Data Encryption Standard (DES) was designed to encipher sensitive but not classified data.
- The standard has been issued in 1977.
- In 1998, a design for a computer system and software that could break any DES-enciphered message within a few days was published.
- By 1999, it was clear that the DES no longer provided the same level of security it had 10 years earlier, and the search was on for a new, stronger cipher.
- This new cipher is called Advanced Encryption Standard (AES).
- AES has been approved for Secret or even Top Secret information by the NSA.

- AES encryption
  - has a variable number of rounds
  - depending on key size.
- To encipher a block of data in AES
  - Initialize (key schedule...)
    - Stretch key data
    - Initialization Round
  - Then several rounds of encryption
    - Shifting and mixing bits
  - Finally, some postprocessing
    - perform a round with the last step omitted

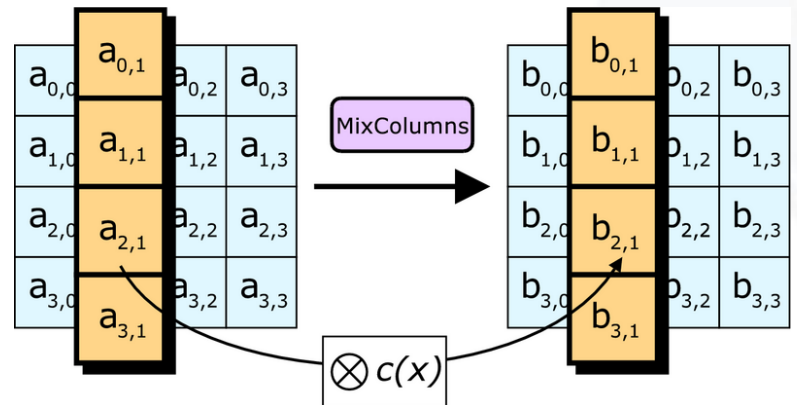
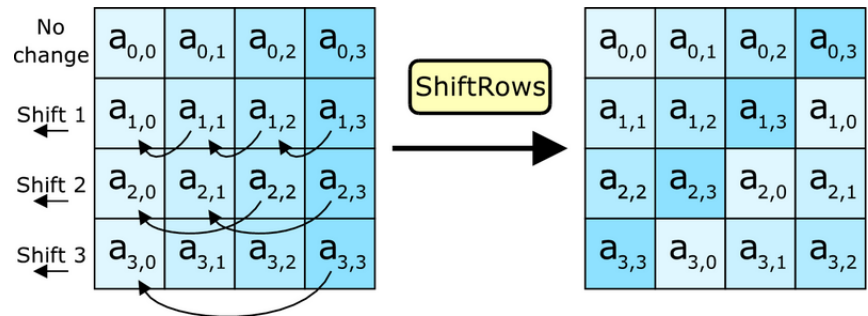
# Encryption Round (1)

- AddRoundKey
  - XOR (mix bits of) current state a and round key
  - Round key k derived using key schedule
- SubBytes
  - Substitution using a lookup table (S-Box)



# Encryption Round (2)

- ShiftRows
  - Shift each row by row index
- MixColumns
  - 4 key bytes combined into each column using polynomial multiplication modulo  $2^8$  [in  $GF(2^8)$ ]



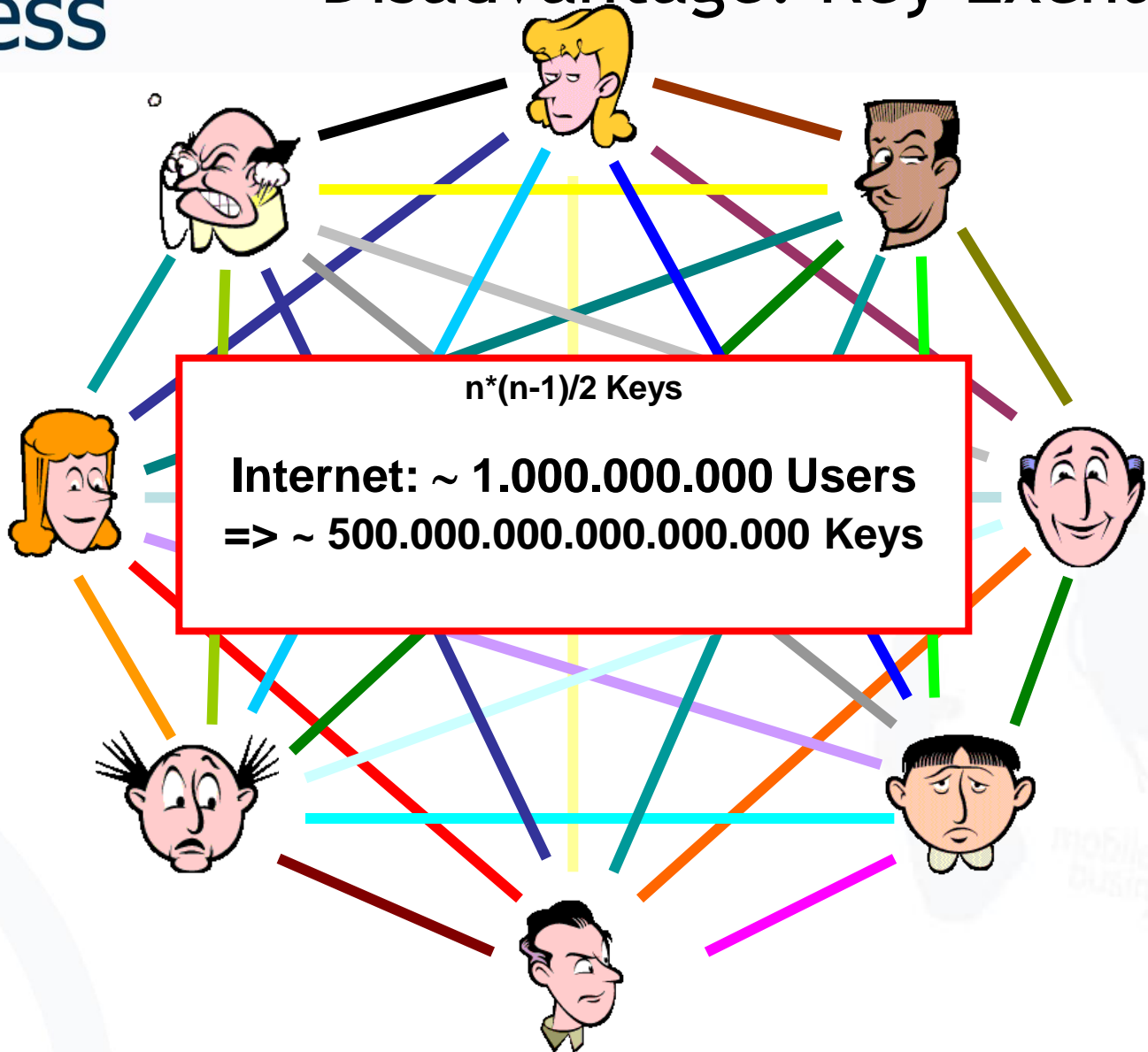
- Introduction
- Classical cryptosystems
  - General concept
  - Substitution ciphers
    - Caesar cipher
    - Vigenère cipher
    - One time pad
  - AES
  - Advantages and Problems
- Public key cryptography

Advantage: Algorithms are very fast

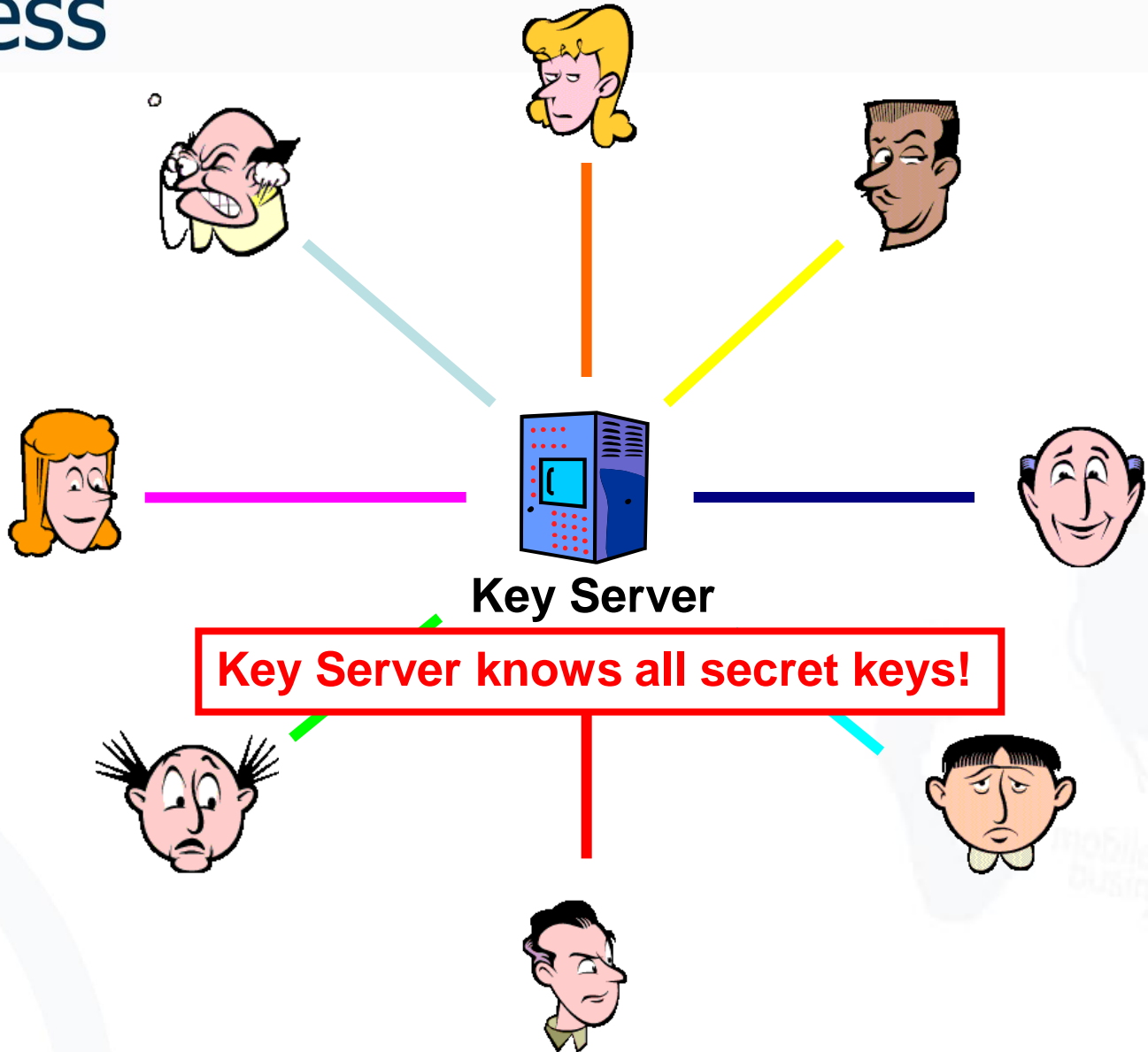
Algorithm	Performance*
RC6	138 ms
AES	173 ms
SERPENT	200 ms
IDEA	288 ms
MARS	394 ms
TWOFISH	697 ms
DES-edc	726 ms

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

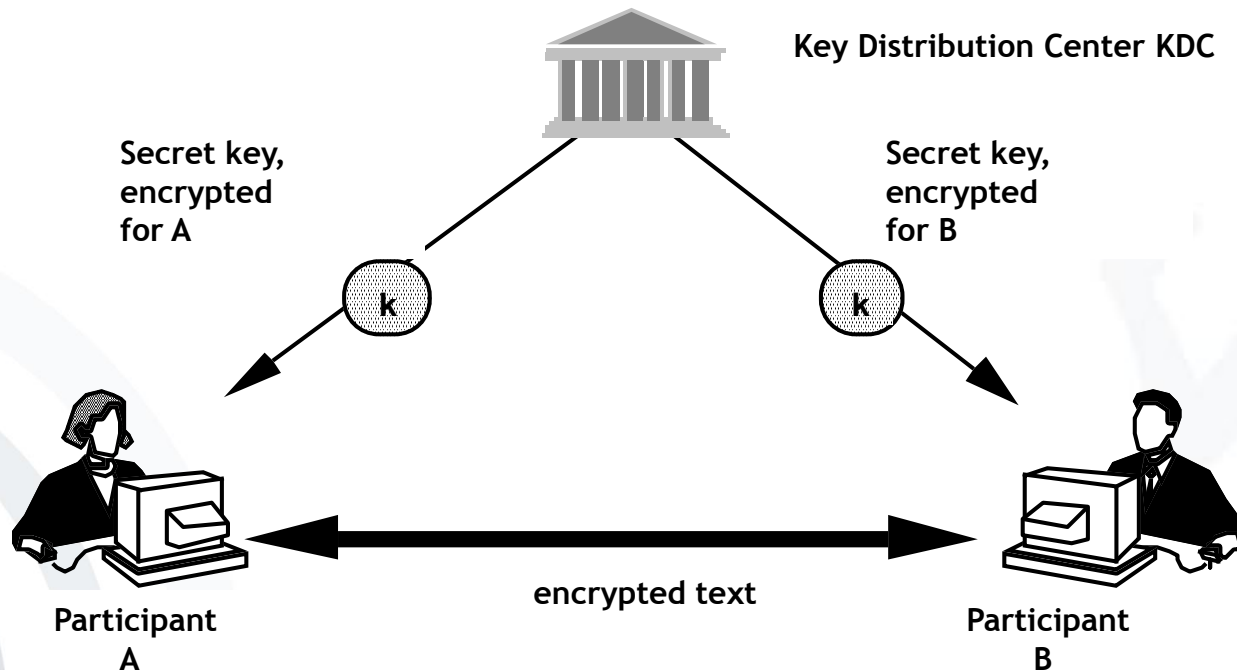
# Disadvantage: Key Exchange



A Possible Solution



- One key per communication pair is necessary.
- Secure agreement and transfer are necessary.
- A center for key distribution is possible but this party then knows all secret keys!



„Anybody who asserts that a problem is readily solved by encryption, understands neither encryption nor the problem.”

(Roger Needham /  
Butler Lampson)



[The Marshall Symposium: Address Roger Needham,  
May 29, 1998, Rackham School of Graduate Studies, University of Michigan  
[www.si.umich.edu/marshall/docs/p201.htm](http://www.si.umich.edu/marshall/docs/p201.htm)]

- **[Bi05] Bishop, Matt.** *Introduction to Computer Security*. Boston: Addison Wesley, 2005. pp. 97-113.